Ref. Ares(2018)6249614 - 05/12/2018

Advanced Cyber-Threat Intelligence, Detection, and Mitigation Platform for a Trusted Internet of Things

Grant Agreement: 786698

D2.3 Cyber-Trust Use Case Scenarios

Work Package 2: Cyber-threat landscape and end-user requirements

Document Dissemination Level

PU	Public	X
CO	Confidential, only for members of the Consortium (including the Commission Services)	

Document Due Date: 31/10/2018

Document Submission Date: 05/12/2018

Co-funded by the Horizon 2020 Framework Programme of the European Union

Document Information

Deliverable number:	**D2.3**
Deliverable title:	Use case scenarios
Deliverable version:	0.5
Work Package number:	WP2
Work Package title:	Cyber-threat landscape and end-user requirements
Due Date of delivery:	31/10/2018
Actual date of delivery:	05/12/2018
Dissemination level:	PU
Editor(s):	Stavros Shiaeles (CSCAN)
Contributor(s):	Abdulrahman Alruban, Hussam Mohammed, Julian Ludlow, Stavros Shiaeles, Salam Ketab (CSCAN) Christos Tryfonopoulos, Christos-Minas Mathas, Costas Vassilakis, Konstantinos Limniotis, Konstantinos Ntemos, Nicholas Kalouptsidis, Nicholas Kolokotronis, Sotirios Brotsis, Paris Koloveas, Spiros Skiadopoulos (UOP) Clément Pavué (SCORECHAIN) Dimitrios Kavallieros, Vasiliki-Georgia Bilali, George Kokkinis (KEMEA) Emanuele Bellini (MATH) Liza Charalambous, Nectarios Efstathiou (ADITESS) Olga Gkotsopoulou, Paul Quinn (VUB)
Reviewer(s):	George Kokkinis (KEMEA) Liza Charalambous (ADITESS)
Project name:	Advanced Cyber-Threat Intelligence, Detection, and Mitigation Platform for a Trusted Internet of Things
Project Acronym	Cyber-Trust
Project starting date:	01/05/2018
Project duration:	36 months
Rights:	Cyber-Trust Consortium

Cyber-Trust Consortium. All rights reserved.

Version History

Version	Date	Beneficiary	Description
0.10	27/08/2018	CSCAN	Proposed outline
0.1	03/09/2018	All	UCs proposed
0.2	10/10/2018	All	Scenarios added from partners
0.3	19/10/2018	All	UCs added from partners
0.4	21/10/2018	All	UCs and Components mapping from partners
0.5	20/11/2018	KEMEA, ADITESS	Review deliverable
06	29/11/2019	KEMEA	Review deliverable
0.7	04/12/2018	CSCAN	Address reviewers' comments
1.0	05/12/2018	KEMEA	Final submission

Cyber-Trust Consortium. All rights reserved.

Acronyms

ACRONYM	EXPLANATION
AMI	Advanced Metering Infrastructure
API	Application Programming Interface
CERT	Computer Emergency Response Team
CISO	Chief Information Security Officer
CSIRT	Computer Security Incident Response Teams
CTI	Cyber-Threat Intelligence
CVE	Common Vulnerabilities and Exposures
CVRF	Common Vulnerability Reporting Framework
CVSS	Common Vulnerability Scoring System
CWE	Common Weakness Enumeration
CWSS	Common Weakness Scoring System
DDoS	Distributed Denial of Service
DGA	Domain Generation Algorithm
DLT	Distributed Ledger Technology
DNS	Domain Name Server
DPI	Deep Packet Inspection
DVR	Digital Video Recorder
eVDB	Enriched Vulnerability Database
FTP	File Transfer Protocol
HIDS	Host-based Intrusion Detection System
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ICS	Industrial control systems
IDS	Intrusion Detection System
iIRS	Intelligent Intrusion Response System
IoC	Indicator of Compromise
IoT	Internet of Things
IPS	Intrusion Prevention System
IR	Incident Response
LEA	Law Enforcement Agency
NFV	Network Function Virtualisation
NTP	Network Time Protocol
OMCE	Oracle Mobile Cloud Enterprise
OMCP	Online Middleware/Component Provider

Cyber-Trust Consortium. All rights reserved.

OS	Operating System
PII	Personally Identifiable Information
SaaS	Software as a Service
SDN	Software Defined Networking
SIEM	Security Information and Event Management
SOC	Security Operations Center
SQL	Structured Query Language
SSH	Secure Shell
TIP	Threat Intelligence Platform
TTPs	Tactics, Techniques and Procedures
UI	User Interface
UMP	Universal Media framework Plugin

Cyber-Trust Consortium. All rights reserved.

Table of contents

Cyber-Trust Consortium. All rights reserved.

Cyber-Trust Consortium. All rights reserved.

Cyber-Trust Consortium. All rights reserved.

List of figures

Cyber-Trust Consortium. All rights reserved.

List of tables

Cyber-Trust Consortium. All rights reserved.

Executive summary

This report is a contractual deliverable within the Horizon 2020 Project Cyber-Trust: Advanced Cyber-Threat Intelligence, Detection, and Mitigation Platform for a Trusted Internet of Things. It provides the Use Cases and example implementations of the capabilities.

Set against the threat landscape established in D2.1 (Threat Landscape: trends and methods), which highlighted the prescient attacks against networks, Industrial control systems (ICS)/Internet of Things (IoT) devices and networks, two principle Domains of the IoT have been chosen: smart home and mobile devices. Within the context of the two Domains, five categories were developed covering the fundamental capabilities offered by Cyber-Trust: namely (a) cyber-threat Intelligence discovery and sharing, (b) monitoring and vulnerability assessment, (c) network-level attacks, (d) device-level attacks, and (e) forensic evidence collection, as well as mitigation and remediation actions. Within the five fundamental capabilities in the two Domains, Use Cases are applied to describe the system functionality under either normal operation or attack conditions.

The attack conditions for both domains were centered on botnet exploits, a serious yet common challenge for IoT, given the fundamental security issues within embedded devices (common passwords, ports and communication protocols) coupled to power and memory resource constraints. These scenarios and the Use Cases align to the proposed system, to include key proactive technologies and cyber-threat intelligence, advanced cyber-attack detection and mitigation, and distributed ledger technology.

The general use cases and common actors designed, which are applicable across all the scenarios, are described as part of the taxonomy section. The methodology section tries to introduce reader to the common Cyber-Trust operation that will be followed for both domains.

It is also worth mentioning that alignment with the General Data Protection Regulation (GDPR) was taken into account to ensure that capabilities within the Cyber-Trust solution do not deviate from established data protection legislation and regulations within member states.

Cyber-Trust Consortium. All rights reserved.

1 Introduction

The grand vision of the Internet of Things (IoT) is to establish a whole new ecosystem comprised of heterogeneous connected devices - computers, laptops, smartphones and tablets as well as embedded devices and sensors - that communicate to deliver capabilities making our living, cities, transport, energy, and many other areas more intelligent. However, only 26% of company-based IoT initiatives are successful (MIPS,2017), and factors such as time to completion, quality of data, internal expertise, IoT integration and budget overruns are commonly listed as reasons why IoT implementation fails. Cyber-Trust aims to provide the necessary security, software and support enabled IoT hardware to offset these failure factors, and deliver secure, scalable IoT via an enhanced blockchain ledger. The project also deals with network and device data, device profiles and vulnerabilities supporting complex visualization and enabling rapid decision making and mitigation actions during enhanced threat and delivering efficient remediation post attack.

The IoT aim, whilst laudable, presents an exponential increase in the complexity of the network, and in terms of cyber-security, creates a more vulnerable topology as a result of the increased complexity, principally due to security problems arising from embedded devices and other legacy hardware (Living Map, 2018). This vulnerability challenge is what Cyber-Trust aims to address, to both support the growth of IoT whilst mitigating the effects of complexity and vulnerability when protecting IoT devices. The setup described in this document has its roots to the *Technical Objectives* (TO) which are the fundamental aims of the project, underpinning the scenarios and use cases. All system fundamentals can be traced back to one or more of these TOs (1-7) and collectively aims to achieve TO8.

TO1: Protect the hardware and software configurations of IoT devices;
TO2: Develop an inventory of authorized (and unauthorized) software;
TO3: Manage network hardware devices so that compromised devices are denied access;
TO4: Build a framework for efficient continuous vulnerability assessment and remediation;
TO5: Trustworthy IoT operation, verify the behaviour of IoT devices against security policies;
TO6: Increase the resistance of IoT networks against DDoS attacks;
TO7: Tools and methods for protecting sensitive data and users' privacy;
TO8: development of a cyber-security platform that goes beyond the state-of-the-art

Work Packages have been developed to deliver the above objectives, focusing on specific capabilities such as network attack, which are underpinned by the Use Cases detailing specific system functionality. To highlight the core system functionality within the Work Packages, this document, develops a malicious software (malware) attack scenario. Moreover, it provides a series of IoT domains such as smart home (these domains, have within them scenarios which detail how work-package produce subsystems and subsystems hold capabilities in order all subsystems to work together and compose the Cyber-Trust solution Figure 1.1, in response to the attack scenario), consuming actors, the Domain, the attack and use cases to do so.

Cyber-Trust Consortium. All rights reserved.

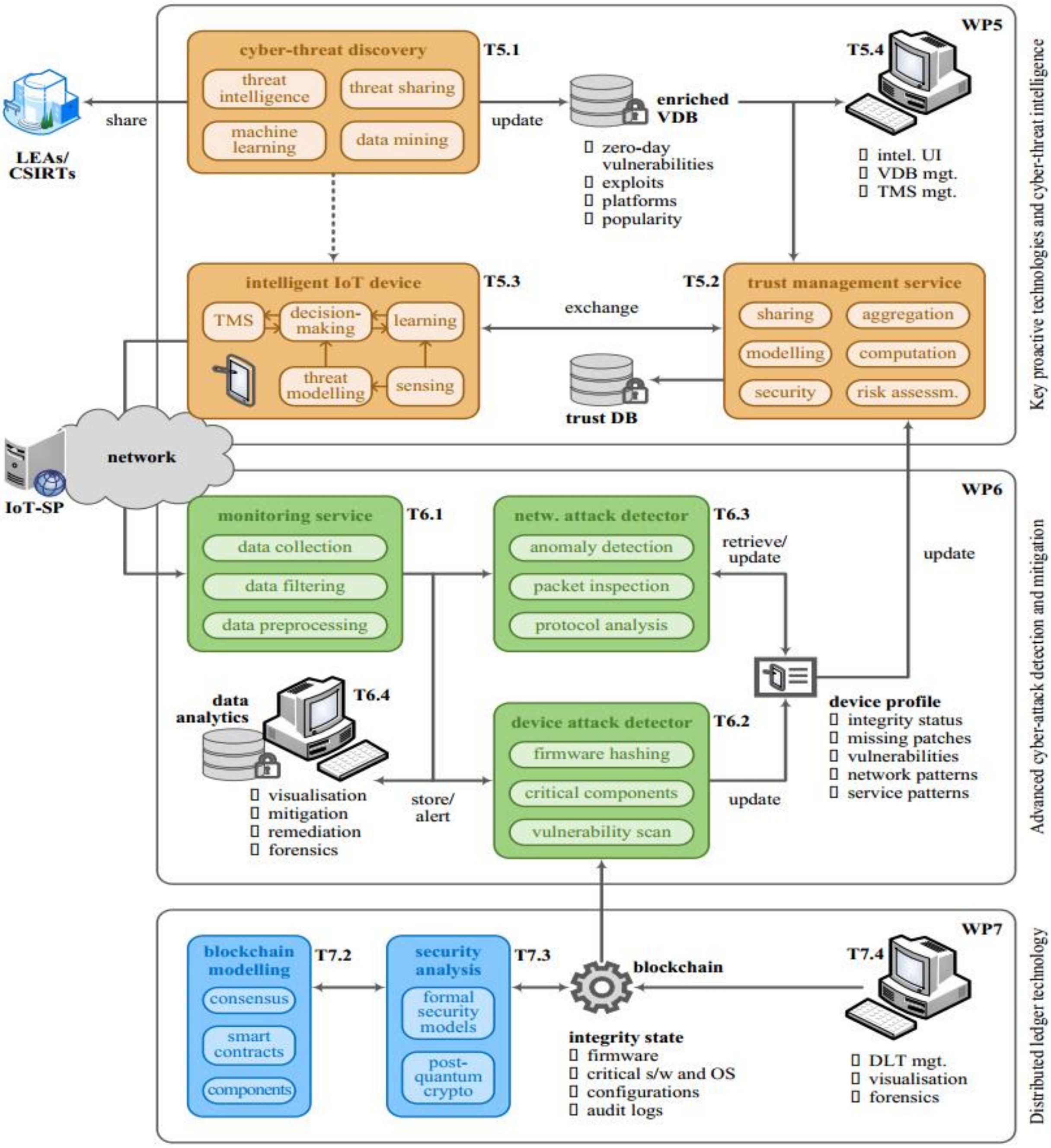

Figure 1.1: Detailed overview of Cyber-Trust's research work packages

1.1 Purpose of the document

The purpose of this document is to describe how the Cyber-Trust platform's components work to detect and mitigate attacks, as shown in Figure 1.1, when operating within the context of a Domain. As a deliverable, it describes the value of Cyber-Trust as a system through it. In this context we will utilize two domains: smart homes and mobile devices in cellular carrier context.

Cyber-Trust Consortium. All rights reserved.

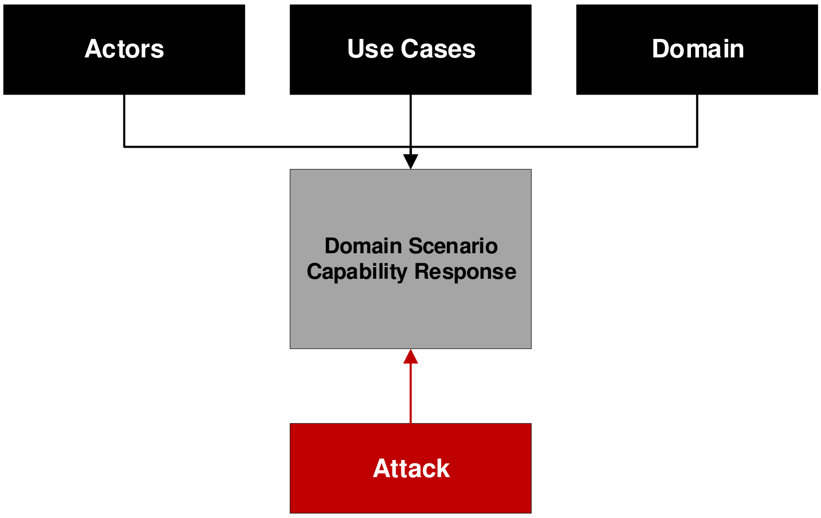

Figure 1.2: D2.3 Structure and Logic

1.2 Relations to other activities in the project

The document will help to derive the Cyber-Trust reference architecture in WP4 as well as the development of detailed scenarios to be used for the demonstration of the platform as well as the creation of evaluation plans (WP8).

1.3 Structure of the document

The Description of Methodology describes how the elements of Figure 1.2 above work together to describe the system functionality both under normal operation and under attack conditions. The general domain structure then applies environmental elements to the use cases so as to describe how the system operates in such different cases.

Individual scenarios then map Use Cases to the Domain so as to show at a suitable level the system functions under normal operations and attack mitigation so as to highlight the nature of the system that Cyber-Trust delivers. Remediation actions then serve as a summary to the individual scenarios and their attack mitigation actions to highlight how post-mitigation 'return to normal' remediation actions occur to either permanently remove a device from the environment or return it to normal operation as a trusted component of the Cyber-Trust system.

Cyber-Trust Consortium. All rights reserved.

2 Description of taxonomy

To derive accurate scenarios and use cases, a system engineering approach has been used whereby actors have been derived and will be used throughout the use cases. Table 2.1 illustrates the main actors in the cyber-trust system.

Table 2.1: Common Person-Class Actors

ID	Description
P1	A smart home owner
P2	A smart device owner
P3	Cyber-attacker

Actors such as ISP employees, security operators, LEA officials will be local in-scenario instantiations of Table 2.2 Actors, i.e. O1 is Bob, a Cyber-Trust Service Provider CISO.

Table 2.2: Common Organization-Class Actors

ID	Description
O1	Cyber-Trust Service Provider
O2	ISP: Internet Service Provider and network operator
O3	LEA: Law Enforcement Agency, either national or inter-national (i.e. Europol)
O4	IoT-SP: IoT Service Provider
O5	Smart Device Security Company
O6	Smart Device Manufacturer

In Table 2.3 are the 6 categories of data collected. As Cyber-Trust deals with different categories of data we also devoted Section 7 to data protection legislation which will be further analysed in WP3.

Table 2.3: Common Data-Class Actors

ID	Description
D1	**Registration/subscription data:** reflects the data relating to natural persons who register/subscribe to the platform.
D2	**Forensic data:** reflects the collection, processing and storage of information that may contain evidentiary material.
D3	**Other personal data**

Cyber-Trust Consortium. All rights reserved.

D4	**Network Data:** reflects the basic data of the network, *that may include personal and non-personal data* and are categorized as normal traffic. Examples include packet captures (pcaps).
D5	**Device Data:** reflects the basic data of the devices, *that may include personal and non-personal data*.
D6	**Anonymised data:** reflects the processing of personal data which went through anonymisation. The anonymised data is used for activities such as analytics and forensic analysis. Examples include log files, IP addresses, packet payloads.

Because it is necessary to link the elements to corresponding Use Cases, Table 2.4 places current envisioned components into actor roles:

Table 2.4: Common Asset-Class Actors

ID	Description	Description
A01	Visualization Portal	All related to the Visualization component (e.g. health status of devices, incident alerts, DLT exploration, etc.)
A02	DLT Service	All related to the DLT component's operation, such as storage of forensic evidence, validation of the transactions, consensus, etc.
A03	Monitoring Service	All related to monitoring components that are responsible for the gathering of data from the network and the devices
A04	Cyber-defense Service	This is covering the detection and mitigation of Cyber-Attacks on networks and device level.
A05	Trust Management System	All related to the trust management, such as trust computation/sharing, device vulnerability assessment, etc.
A06	Cyber-Trust Registration Module	This is part of the Admin Portal which is responsible for the registration of the various actors (users, devices, organizations).
A07	eVDB Admin Module	The database maintaining enriched data about vulnerabilities, exploits, etc., that are collected through Threat Intelligence techniques.
A08	TrustDB Admin Module	Database of Trust based on the vulnerabilities assessment and other metric.
A09	eVDB Sharing Service	All related on disseminating meaningful results for vulnerabilities, exploits, cyber-attacks, etc., to other affiliate members.

Cyber-Trust Consortium. All rights reserved.

A10	Crawling Service	All methods of harvesting the data available on the surface/deep/dark web and store them for further analysis.
A11	Smart Gateway Agent	Cyber-Trust component running on network gateway
A12	Smart Device Agent	Cyber-Trust component running on devices
A13	Smart Gateway iIRS app	Cyber-Trust app running on Android and iOS powered gateways
A14	Smart Device iIRS app	Cyber-Trust app running on Android and iOS powered devices
A15	DLT Admin Module	The administrative part of the DLT service that resides at the Cyber-Trust service provider
A16	Network architecture and assets repository	This is a set of tools allowing to get information on a network's architecture (including the topology and the security defenses deployed therein), assets and their values, etc.
A17	Profiling Service	Device and Network profiling services.

The common actors in the preceding Table 2.1, Table 2.2, Table 2.3 and Table 2.4 used within the two domain scenarios. Table 2.4 ensures that use case assets can be mapped to the Assets Class Actors. In addition to the above, several assumptions are made about the core functionality of the Cyber-Trust platform. Such assumptions are important to understand so as to develop the correct use cases.

Cyber-Trust Consortium. All rights reserved.

3 Description of methodology

In section 2 we presented the taxonomy that will be used across the two domains and Use Cases of this document. The purpose of this section is to provide a brief description of the methodology that will be utilised as required by the scenarios to describe the system functionality in two domains.

3.1 System Operation

The general description of the Cyber-Trust system is one of an architecture split between local device-based capabilities and service-provider-wide capabilities (e.g. ISP, IoT service operator, etc.), supported by global cloud-based capabilities. The local device is the focal element of the architecture – besides providing the required functionality, it may encompass a number of vulnerabilities, some of which have not been identified or/and made public to the wider community or/and cannot be patched or/end cannot be mitigated; while it cannot be relied upon for performing all tasks, the expectation is that it may run a number of basic tasks, including a level of DPI or comparison with an IDS database. Rather than relying on the traditional vulnerability discovery and patching process, the system uses early discovery sources, based in the dark web and hacking communities, to form a faster, more dynamic source of information, including a range of solutions from patching to attack signatures. As part of its process, the system crawls the dark web to identify such new vulnerabilities and exploits, which are processed and loaded in a database. Through the distribution agents, information from the database is used to either patch the affected systems, mitigate their impact on the network in case of infection, or isolate them to avoid any impact or further infection. To improve its resilience, information is stored using a distributed ledger. From a system interaction perspective, Cyber-Trust can be modelled as a SaaS to consumers (industrial, government, commercial and individuals), leveraging the strength of Software-Defined Networking (SDN) to allow a more granular control of traffic, with the potential for Network Functions Virtualization (NFV), where required by the processing needs, in order to maximize efficiency in terms of resource and power consumption. The following description breaks down the cloud and device-based elements, drawn from Table 4, based on the architecture and conceptual operational model.

To illustrate typical environments and associated threats, the project will focus on two domains: smart homes and mobile devices in cellular carrier context. While sharing some of the IoT principles, the two domains are very different in terms of connectivity, perimeter, and processing capabilities. With the domain in mind, appropriate scenarios, capabilities, and actors were designed as part of the scenarios to illustrate a typical attack and how the Cyber-trust environment will identify, isolate, and mitigate or eliminate the threat. One important point is that actions taken by each actor depend on its capabilities, hence the scenarios included the necessary flexibility to.

Starting with the device-based capabilities, these can range from observational and communication for low-powered, low-computation IoT devices to analysis and decisional for high-computation devices. For example, a mobile terminal may perform some analysis and parsing of the data to be analysed by other actors but cannot be expected to run a full IDS or DPI due to power restrictions. Along the same lines, a smart home meter may have sufficient power for communication, but will include no computational power for any analysis, hence relying exclusively on an external or perimeter device for analysis.

At a minimum, an IoT device included within the Cyber-Trust environment includes an embedded agent to report, monitor, and alert upon detecting a system or network behaviour change. Changes or anomalies in firmware or software, using the DLT-assured baseline, and in behaviours on the network (port use, traffic profile etc.) would be first detected by the device agent and reported to other actors. Should the device also

Cyber-Trust Consortium. All rights reserved.

include tangible processing capabilities, the system can rely on it to also perform a first level of analysis or negotiate distribution of tasks with the other entities.

Once the device signals an issue, the cloud-based remote services evaluate the risks and, after comparing with the existing data, may decide to either further analyse the data or take response/isolation/mitigation action against the device. Two critical aspects are required in order for this process to succeed – a comprehensive vulnerabilities/attack databases and an infrastructure that allows for communication with the device and isolation if necessary, as well as processing power sufficient to analyse the data provided by IoT devices. The Cyber-trust environment encompasses an *enriched vulnerability database* (eVDB) [A07] which contributes to the ability of the system to respond dynamically to threats by enabling an accurate calculation of device risk on a per-vulnerability basis.

From a communication perspective, the Cyber-Trust architecture enables a scalable platform that facilitates the exchange of data between the IoT device and the vulnerabilities databases, allows optimisation of CPU and GPU processing, and communicates with the existing network infrastructure to control the IoT device access to network and information.

This allows satisfying different operational demands and easily shifts from normal operation to response of situational changes, such as attacks. As stated in the introduction, the core security, storage, and data action require substantial computing power, but also demand which varies with the state of the system variable. In this context, normal operations would be low demand whereas situations such as processing new threats to create signatures to train machine learning algorithms, or conducting attack mitigation by running DPI, would result in processor and memory spikes that the can be accommodated by the cloud.

In the context of the ledger which is an implicit underpinning capability driving the system architecture, the majority of the high-memory, high-processing demand or high memory footprint related tasks are cloud-based. Such tasks/services would include monitoring services, enhanced gateway-fed intrusion detection systems (IDSs), and embedded device agents that may collect, filter and pre-process (where appropriate) the network traffic. The aim of the analysis is to identify anomalous network traffic or protocol behaviour via the dedicated network and device attack detection and mitigation agents, as provided by the ISP or an equivalent organisation.

3.1.1 Trust and the Cyber-Trust Cloud

As previously discussed, Cyber-Trust devices vary widely by computing power, networking capability, storage space, access to electricity, and mobility, whilst vulnerability analysis utilises trust as an entity in determining device-based risk. Cyber-Trust devices will be part of an ecosystems that requires continuously evolving levels of trust. This, in turn, enables the development of intra-device trust scores that adds a layer of threat detection to further enhance the TrustDB. As more transactions occur between peer devices, trust will evolve between them. What starts as an interaction between two trustless peers can over time become a semi-trusted or even a trusted relationship. So the extent of transaction verification required between devices depends on many factors: the kind of device, nature of the interaction, kind of relationship between the devices and also the constraints imposed by device owners on what the devices can and cannot do in specific circumstances.

Different Cyber-Trust devices support different degrees of functionality, depending on their performance and storage capabilities. At the lowest end are level 1 devices such as wearables, smart plugs and light switches that perform basic IoT functions like messaging. At the other end of the device spectrum, devices may contribute to peer exchanges to enable more complex transactions as peer services. As these devices become

Cyber-Trust Consortium. All rights reserved.

peers of a decentralized network, it is essential that each can identify itself uniquely to peers in a verifiable manner, retain details on its relationship when intetacting with other peers and identify peers unambiguously across protocols. These actions can be achieved by means of a secure peer list which holds the peer-level trust metrics.

3.1.2 Device-Based

The cloud-based capabilities described above are beneficial but would be challenged in their delivery of a dynamic protection capability should the support of low-power, low-resource blockchain-enabled device agents be missing. When an IoT device is included within the Cyber-Trust environment, it means that a device-suitable agent or iIRS is embedded to provide advanced monitoring and alerts upon detecting a system or network behaviour change. Changes or anomalies in firmware or software, using the DLT-assured baseline, and in behaviours on the network (port use, traffic profile etc.) would be detected by the device agent first – they are the alert point for the system, and as such critical to the system being able to respond correctly in an acceptable time, as mitigation (trust, threat, profile as vulnerabilities) and remediation (forensic storage and restoration) actions will be centered on the device and the affected elements.

3.1.3 Domain Foundations

The Domain scenario is based on a wide range of equipment, including mobile devices, SCADA, PLC, Smart Meters, DVRs, as well as generic IoT devices. The choice of devices leads to utilize 'real-world' environments in their domain scenarios. It is important to note that exploits within the scenarios, as it is the case in the real-world, are designed to attack specific architectures and firmware, and so device architectures and firmware are metrics used in the calculation of device risk and trust under normal and attack conditions.

The Actors and Processes are integrated in the scenarios via the Use Cases. Within the context of the two Domains, five categories were developed covering the fundamental capabilities offered by Cyber-Trust (Figure 3.2): namely (a) cyber-threat Intelligence discovery and sharing, (b) monitoring and vulnerability assessment, (c) network-level attacks, (d) device-level attacks, and (e) forensic evidence collection, as well as mitigation and remediation actions. The capabilities shown in Figure 3.2 correspond to the Sections 4.1-4.5 and 5.1-5.5 of Domain 1 and Domain 2 respectively based on the five categories aforementioned. Within the five fundamental capabilities in the two Domains, Use Cases are applied to describe the system functionality under either normal operation or attack conditions. When a service capability calls on another service capability, it should be via Actors and Processes to allow for the development of accurate inter-dependency mapping. The sum of this approach is that the system response to specific threats can be modelled and described, allowing Cyber-Trust to communicate how its unique approach will protect service customers and the providers during service provisioning.

The registration process is the trigger function by which the Cyber-Trust map within a consumer's domain is developed, or in the case of an existing user the map being updated per new device: the map simply being the registered devices and gateway. Scenarios will assume the registration process has occurred.

The trigger function for the activation of the registration process is a new user application or an existing user adding or removing a registered device from the service. Two cases are considered regarding the security coverage offered by the Cyber-Trust platform.

The Figure 3.1 below demonstrates the approach to be followed for the two domains of interest.

Cyber-Trust Consortium. All rights reserved.

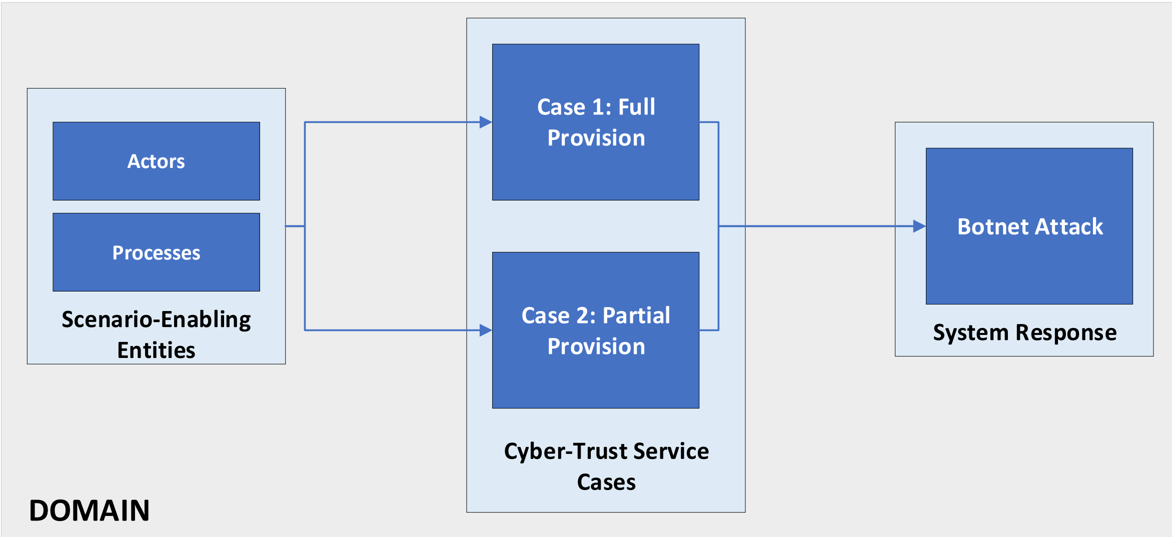

Figure 3.1: Common Use Case approach under the two Domains

1. **Full Provision:** covers the gateway and devices, so all devices present within the consumer's domain are in-effect cyber-trust registered, enabling full protection coverage.
2. **Partial Provision:** covers the gateway and some devices as selected by the user. This provides partial cover within the consumer's domain whilst maintaining a level of protection for the wider Cyber-Trust system.

To effectively develop the Use Cases and cross-capability interdependency, this document will define a main scenario, which will then be detailed with the attack vector(s). The individual capabilities will then develop and shape the associated Use Cases, according to the main scenario, and the service cases to describe how their capability element will respond to the threat vectors described below.

3.2 Main Attack Scenario

The Cyber-Trust capable smart IoT devices can have admin passwords, firmware, OS and security patches managed centrally by Cyber-Trust, which actively monitors them as a matter of course, whereas users are responsible for maintaining OS updates on their own edge devices, i.e. via Windows/iOS/Android scheduled updates from hardware/OS providers. The Cyber-Trust system is capable, once installed on edge devices as a root service, to be able to check the status of updates via passive monitoring and provide an alert to users if patches or updates have not been installed or the device profile deviates from the held version.

The Domain-Specific attack scenarios are described in the Domain descriptions below, however as an introduction the following attacks will be used:

Domain 1 Attack Vector: ARM Botnet Exploit on ANKO Products DVR.

Domain 2 Attack Vector: RottenSys Android exploit.

As previously discussed and highlighted in the overall Cyber-Trust environment in Figure 1.1, the scenario defines the attack context, including domain specific details; in turn, this encompasses possible device attack detection options. The scenario, context, and attack are enacted through use cases and actors, functionality, and attack conditions.

The Actors and Processes are consumed in the scenarios via the Use Cases. When a service capability calls on another service capability, it should be via Actors and Processes to allow for the development of accurate inter-dependency mapping. The essence of this approach is that the system response to specific threats can

Cyber-Trust Consortium. All rights reserved.

be modelled and described, allowing Cyber-Trust to communicate how its unique approach will protect service customers across the two potential service offerings (full or partial coverage).

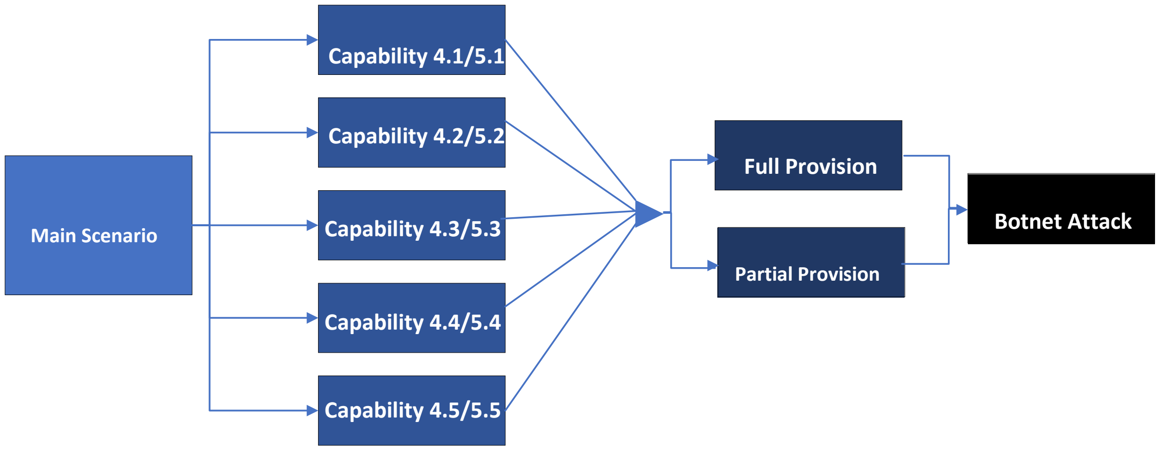

Figure 3.2: Sub-scenario Taxonomy

To effectively develop the Use Cases and cross-capability interdependency, this document will define a main scenario, which will detail the attack vectors as per Figure 3.2 above. To this extent, the scenarios will explore an incident where a Linux-based smart device, such as a home surveillance system, was compromised and the software binary of an unknown [until now] malicious bot was installed. This bot is listening for commands through HTTP and HTTPS and can execute three different types of attacks. These attacks are a) DDoS b) Eavesdropping c) Spamming. Currently, the bot is trying to replicate itself over the network using telnet/FTP/SSH default logins; however, it can also update itself from C&C server with exploits that can attack more devices with firmware vulnerabilities. In order to understand the lifecycle of a botnet displaying in Figure 3.3. we will analyse each phase below thoroughly.

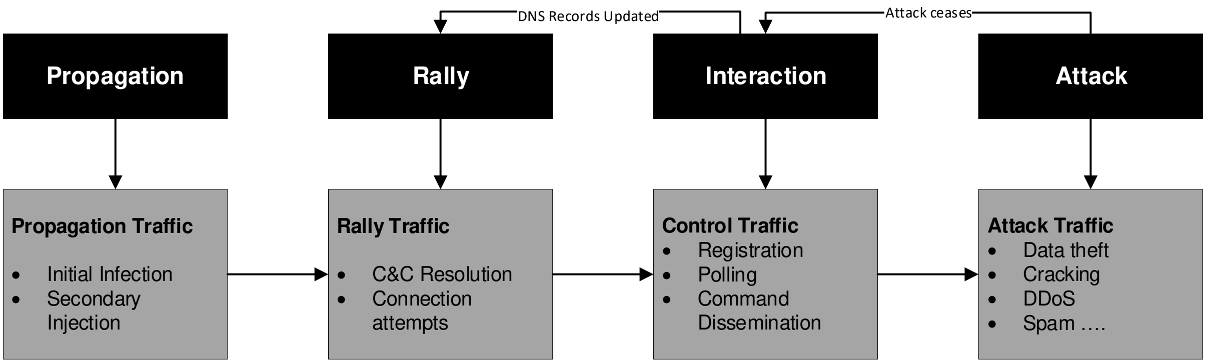

Figure 3.3: Botnet Life-cycle (de Siva et al, 2013)

Propagation: On initial infection, a DVR device becomes infected with a bot net. Initial infection is successful (and so DNS back-scatter does not occur), and a secondary injection occurs via SHELL_INJECTION commands, where the infected device runs a program to search and download malware binaries via an application layer protocol (i.e. HTTP) to update and establish its configuration. Bot1 scans local network in order to identify more vulnerable devices and to propagate further by making use of techniques such as buffer overflow vulnerabilities in processing NTP servers' information, in particular configuration files: a vulnerable host will run the injected command, which includes a retrieval method (e.g. wget or tftp)

Cyber-Trust Consortium. All rights reserved.

to the attacker's IP address. An unpatched router with a vulnerability (for instance TR-064), which might be obtained via scanning, can be exploited in this fashion.

Rallying: At the rallying stage the bot now contacts the Command and Control (C&C) server via HTTP, and query for updates or instructions. This phase restarts every time the host is booted, and is when the main configuration files are downloaded to the bot. The bot and botmaster have a common seeded Domain Generation Algorithm (DGA) which generates pseudo-random domain names, and domain fluxing is in use.

Interaction: HTTP botmasters employ a pull approach, so Bot1 must initiate contact with the C&C server and request instructions, and then regularly poll for updates utilising ports 80 and 443. This allows perimeter controls to be bypassed, and a natural obfuscation via hiding communications (with a low signal-to-noise ratio) in regular web traffic. As well as polling, Bot1 can return domain-based 'user' data to the C&C server, as well as download updated config files or attack instructions.

Attack: HTTP Botnets can conduct a variety of attacks (DDoS, man-in-the-middle, SQL injections), all of which varies the traffic seen.

Problem Description: The underlying problem is one of characterization and identification of HTTP-based botnet traffic. Within the context of the lifecycle the problems are one of identifying rallying traffic, interaction traffic and attack traffic against a background of normal web traffic.

Cyber-Trust Consortium. All rights reserved.

4 Domain 1 - Smart Home

A smart home is an ubiquitous computing environment that involves adding intelligence into residences so as to increase comfort, safety, security, and energy conservation. An important aspect of smart homes is the ability to remotely control the various components by using a diverse range of communication and web technologies.

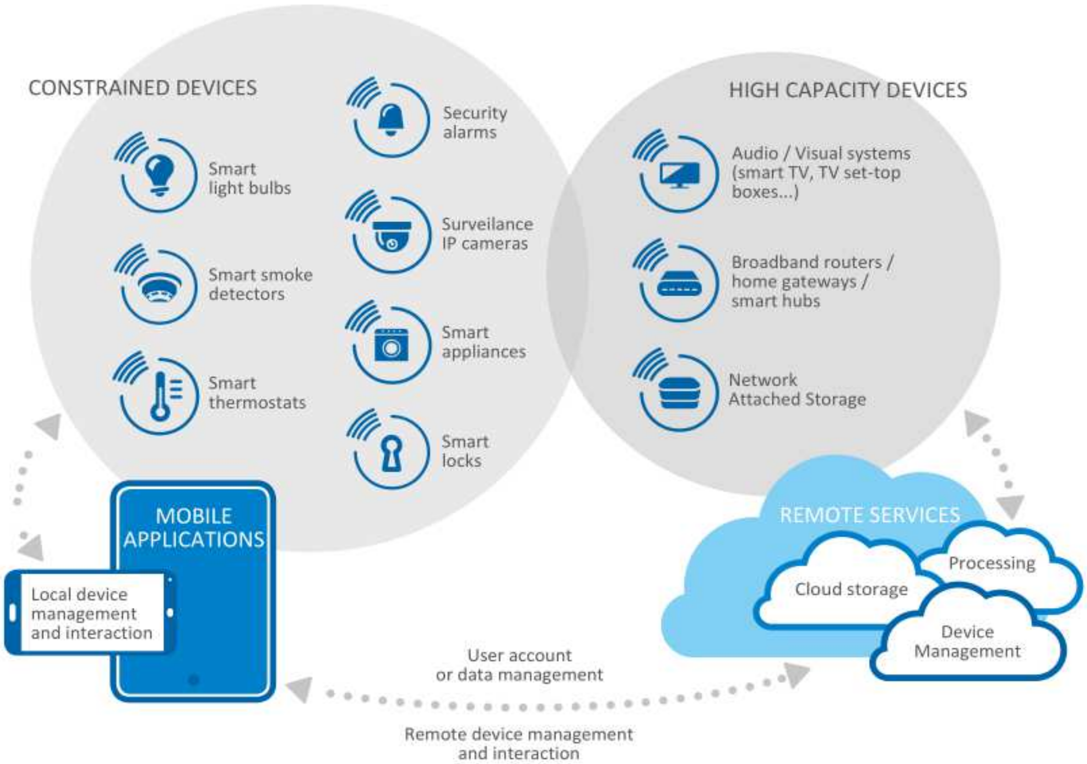

Figure 4.1: Common smart devices and IoT components

Smart homes offer a better quality of life by introducing automated appliance control and assistive services. They optimize user comfort by using context awareness and predefined constraints based on the conditions of the home environment. A user can control home appliances and devices remotely, which enables him or her to execute tasks before arriving home. Based on the Cyber-Trust Deliverable 2.1, smart devices can generally be classified in two categories as shown in Figure 4.1:

1. Resource-constrained devices, such as: smart home appliances (refrigerators, lights, etc.); alarm systems, smart locks and cameras; smart meters and thermostats; environmental detectors (motion, smoke, fire, etc.)
   i. Class 0 devices: << 10 KB RAM, << 100 KB Memory Storage Capacity; may not be possible to implement security measures.
   ii. Class 1 devices: ~ 10 KB RAM, ~ 100 KB Memory Storage Capacity; may be using some security protocols but implementation of standard security measures may not be possible.
   iii. Class 2 devices: ~ 50 KB RAM, ~ 250 KB Memory Storage Capacity; implementation of most standard security measures is possible.

Cyber-Trust Consortium. All rights reserved.

2. High-capacity devices, such as: smart TVs and media centers; gateways, routers and other network equipment.
   - >> 50 KB RAM, >> 250 KB Memory Storage Capacity; may provide additional security measures (ex. network scans).

This limitation of resources leads to a lack of security mechanisms as well as the fact that smart devices are set-up for ease of use. Moreover, traditional security practices may not be applicable or easily followed by users of smart devices and also the installation of software updates may be hard or impossible due to embedded system powering device complexity or the manufacturer may not be supporting the device any more. In terms of connectivity smart devices can be connected:

1. On a *local area network* (LAN), directly to the home router/gateway or on a secondary hub dedicated to the smart devices (to deal with incompatibilities between the existing home infrastructure). Using either high speed networks (e.g. WiFi), or personal area networks (ex. Bluetooth, Zigbee).
2. On a *wide area network* (WAN), usually with access to the Internet. Using a high-speed connection (through the existing home connection to an ISP or through a mobile network connection), or a low power wide area network (LP-WAN) (e.g. LoRaWAN, Sigfox).
3. On a *dedicated network* (ex. *advanced metering infrastructure* (AMI) in the case of smart energy meters).

Connectivity, on the other hand, raises more issues as smart devices are usually connected to the already existing home infrastructure which makes generalized security solutions hard and also use of multiple communications protocols, as shown in Figure 4.2.

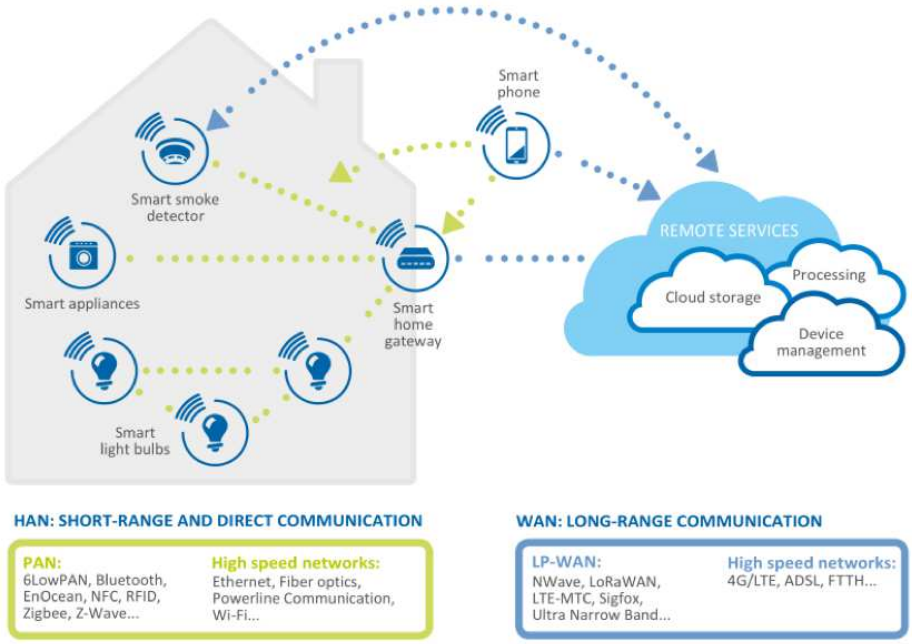

Figure 4.2: Devices in Smart Homes

Attackers show an increasing interest on controlling our Smart Home devices, and recent examples like the Mirai botnet highlight this fact.

Cyber-Trust Consortium. All rights reserved.

Cyber-Trust exploits existing network infrastructure(s) to enable enhanced IoT device safety. Domain represented in the following scenario, collectively show how Cyber-Trust operates effectively as a two-state system, delivering passive monitoring and active mitigation and remediation, to protect IoT devices.

4.1 Cyber-threat intelligence discovery and sharing

Mary, a smart home owner [P1], has been informed about Cyber-Trust from her ISP [O2] that also provides all the smart home services. Mary [P1] is registered in the Cyber-Trust platform [UCG-02] where she can monitor [UCG-05] her devices' health status [UCG-05, UCG-10]. The ISP is also registered in the Cyber-Trust platform [UCG-02] and accesses to the 2D Operator Monitoring [A03] and Control Panel - OMCP [UCG-05] in order to monitor the network of smart homes [UCG-05], and detect misbehaving devices, along with its own infrastructure [UCG-05]. As such, Mary [P1] relies on the Cyber-Trust platform to ensure that her home network, and the devices she registers [UCG-05] are protected and will indeed remain secure across the existing LAN, WAN, AMI networks within the property.

Mary [P1] buys a new smart device (e.g., a smart plug); before even physically installing it in her home, she decides to register the new device [UCG-02] into the Cyber-Trust platform to safeguard it. This allows Mary to provide information about the device (e.g., name, version of firmware and operating system, etc.) and use Cyber-Trust's eVDB [A07] to get information for any security issues [UCG-05] that pertain to her newly acquired device [UCG-06]; at the moment, nothing comes up. She decides to subscribe to the publish/subscribe service that is offered by the Cyber-Trust platform to be promptly notified about any updates and security-related issues that may rise in the future [UCG-02]. Mary is able to tune the information she would like to receive [UCG-02] from Cyber-Trust platform (e.g., type of updates/alerts, desired level of alert confidence, desired impact threshold) [UCG-05]. As Mary is not a security analyst, she decides to be notified only for high confidence/high impact alerts [UCG-14].

Tom is a security officer [O2] working at a Smart Home operator and wants to search, uncover, [UCG-06] and be notified about possible attacks [UCG-14] that are likely to pose a risk to the Smart Home devices his company supports. He also wants to identify and prioritize these cyber-threats [UCG-16] with the highest potential for negative impact on the supported devices by resorting to gathered cyber-threat intelligence. To do so, he registers the supported devices with the Cyber-Trust platform [UCG-02] and subscribes to its publish/subscribe service [UCG-02]; the system stores the devices' profiles [A17] and matches them [UCG-14] against the contents of the eVDB [A07] to determine possible exploits and attacks that have been collected from the clear, deep, and dark web. The system then communicates the matched vulnerabilities and exploits to the security officer through an appropriate intelligent UI [UCG-14], indicating also issues that are pivotal or of high priority.

Since Tom is particularly interested in protecting the devices from certain types of attacks he augments his subscription with keywords related to the attacks he is interested in being notified for [UCG-02]. Moreover, to stay on the safe side regarding new threats that may affect the devices his company supports, he sets the confidence level of receiving alerts to the lowest possible [UCG-02]. This means that a continuous query for the registered devices is created, allowing him to receive notifications for all newly discovered vulnerabilities and exploits [UCG-14] that are inserted into the eVDB [A07] (even without verification) and be presented with a summary of the eVDB [A07] vulnerabilities affecting the Smart Home operator's devices [UCG-11]. The difference in the Cyber-Trust usage between Mary (a technology aware person [P1]) and Tom (a security officer [O2]) lies not only on the number of devices they control, but also on the attack mitigation options they may apply [UCG-14]; for instance, Tom [O2] has access to a wider variety of devices and gateways.

Cyber-Trust Consortium. All rights reserved.

Meanwhile, the cyber-threat discovery module of Cyber-Trust is already bootstrapped and since then is continuously crawling popular social media streams [A10], popular security-related websites and deep/dark web forums and marketplaces [UCG-16]. Cyber-Trust searches for cyber-threat information including zero-day vulnerabilities and exploits, signatures, executables, and other related information. To this end, it uses an ensemble of state-of-the-art data and knowledge processing and machine learning techniques to identify the (clear/deep/dark) web pages that should be crawled and to extract and contextualize all relevant threat information [UCG-16]. The collected data may refer to a new threat that has to be inserted into the eVDB [A07], or new information about known threats (e.g., exploits) that will update the eVDB [A07] entries and enrich the stored intelligence [UCG-16]. New information is initially added to the eVDB [A07] with a low level of confidence in the existence of the vulnerability (as it has possibly not been validated yet by security experts) and the credibility of the known technical details [UCG-06]. The function of the cyber-threat discovery module is supervised by an IT expert (Bob, [O1], see more details below) that is responsible to add, annotate, and approve the crawling of new seeds [A10] (i.e., websites of interest), tune the crawling parameters [A10] that enable their discovery, and evaluates existing seeds in terms of usefulness [UCG-19].

While on operation, the cyber-threat discovery surfaces information about a new zero-day vulnerability and inserts it into the eVDB with a low confidence level [UCG-16]. Then, the system updates information about the risk that this new exploit poses to the affected registered devices [UCG-15], the trust score that is associated with the devices [UCG-16], and the available strategies (represented as attack graphs) that attackers might follow for compromising the devices [UCG-15]. Based on their preferences [UCG-02], Tom is notified through multiple channels [UCG-14], e.g. via email messages or the intelligent UI, for the new vulnerability and the affected devices (since he requires low confidence levels), but, Mary does not (since she is seeking high confidence). After examining the eVDB [A07] info about the new threat [UCG-05], Tom decides to take appropriate defense actions. [UCG-18].

John is an external actor [O1] working as a vulnerability assessment expert who is examining and assessing newly discovered cyber-threats [UCG-06]. Over the last few days he has been reviewing the new vulnerabilities that were surfaced by Cyber-Trust [UCG-06] and now decides that there exists enough evidence to update the *report confidence* (RC) field of the newly discovered vulnerabilities in the eVDB [A07] from “not defined” to other confidence levels (e.g. “unknown”, “reasonable”, or “confirmed”) that are being assigned after the existence of the vulnerability is acknowledged [UCG-06]. Due to this update, Mary is now notified for the newly confirmed vulnerability [UCG-14]. John also provides feedback on the quality of the information gathered about considers some new seeds; some are approved and are annotated for usage [UCG-06].

Finally, Sarah, a security officer [O2] working in the control room at the Smart Home operator [O4], has been alerted about suspicious behaviour in the provider’s infrastructure [UCG-06]. She uses the eVDB [A07, UCG-06] to query for similar behavioural patterns in the hope to learn more about attack types that produce this type behaviour and to identify in advance possible solutions [UCG-06]. In an analogous way, the eVDB [A07] information is also utilized, by the different Cyber-Trust modules to query [UCG-05] for relevant intelligence (e.g., similar threats, rule updates, identified signatures, or mitigation strategies [UCG-06], see also [UCG-18, UCG-14].

Moreover, Sarah wants to understand how the operators in the control room behaved in similar situation what was the status of the network and the devices. Thus, she decides to activate the Time Machine functionality on the 2D-OMCP (Online Middleware/Component Provider) [UCG-05]. She selects a time slot in the past and obtains an extraction of the information collected by the system in the period. With a slider, she can go back and forth while continuing to interact with the 2D-OMCP as if it were operational but with a past

Cyber-Trust Consortium. All rights reserved.

view. She realizes that there are some similarities in the status of the network and requires further investigation and that the actions put in place by the operators have not been effective.

4.2 Monitoring and vulnerability assessment

Mary, a technology-aware person [P1], has bought a new IP camera for her smart home. She has registered the device to the Cyber-Trust platform [UCG-02] and the device model, firmware & operating system version, and the list of patches that have been applied to the device are known and stored in the device profile service [A17]; Mary did not enter this information during the device registration phase [UCG-02], however the Cyber-Trust profiling service [A17] was able to determine this information through remote detection techniques [UCG-16]. As the eVDB [A07] has been recently updated with new vulnerabilities, the TMS retrieves the IoT device data from the device profile service [UCG-10, A17] and newly added vulnerabilities from the eVDB [UCG-06, A07] and identifies that a new vulnerability has been discovered for this camera, which can be exploited to install malware on the camera. Therefore, the TMS triggers a new computation of the device trust level [UCG-13]: in this context, the Network architecture and assets repository [A16] is queried to determine security defenses that are present on the device and the Network architecture and assets repository [A16] is queried to identify network-level security defenses that are present for this device at network level. Only a firewall (a specific element of the network architecture) is identified to be in effect for the particular device; this firewall is able to block exploitation attempts from outside the smart home network perimeter, however is not able to mitigate attacks from rogue or infected devices being inside the smart home network perimeter. Given that the technical impact of the vulnerability is severe and that the attack is exploitable, the TMS reduces the device trust level from 0.8 to 0.3. The risk level related to the current status of the device is increased from 0.1 to 0.6 [UCG-15]. The mitigation policy database is consulted [UCG-18] to determine which actions need to be taken in response to these changes to trust and risk level. Following the specifications of the retrieved policy, an alert is raised for Tom (the security officer working at a Smart Home operator [O2, UCG-06, UCG-05] and an alert is also issued for Mary [P1, UCG-06, UCG-05]. Finally, the TMS [A05] updates information about the available strategies (represented via attack graphs) attackers might follow in order to compromise the IoT device [UCG-15].

At the information security department of the ISP, Tom (a security officer working for the ISP) receives the alert and decides to check the vulnerability status and trust levels of all cameras that are produced by the same manufacturer and are registered with the Cyber-Trust system. To this end, he uses the Intelligent UI to request firstly a visual report of the devices of type “IP Camera” that are produced by the same manufacturer [UCG-05]. The system displays the requested visualization [A01], indicating that 10 cameras have vulnerabilities of high impact, 6 cameras have vulnerabilities of medium impact, 2 cameras have vulnerabilities of low impact and 8 cameras have no known vulnerabilities. Then, Tom requests that the trust level visualization [A01] is displayed [UCG-05]; Tom notices that some cameras with medium vulnerability levels are reported as having low trust levels, and based on this he concludes that these cameras are highly likely to have been hacked and the low trust level is owing to their observed behavior. Tom notifies the ISP field service team to schedule a detailed security inspection for these devices.

Tom, while reviewing his mailbox, finds out that a new class of products for Smart Homes is released, namely smart door locks. Tom schedules a meeting with other security officers and they conclude that even medium-level vulnerabilities for this class of devices should be considered as critical, because if they are exploited they can lead to either uncontrolled access to the area they protect or inability to access the area. To this end, Tom curates the mitigation policy database [UCG-14] to enter a policy rule that reflects the decision reached.

Cyber-Trust Consortium. All rights reserved.

Mary’s [P1] smart home installation hosts also a Smart TV, which is malfunctioning, therefore she takes it to be serviced. Since the device has been however already registered to the Cyber-Trust platform with an “Always available” designation, before plugging the Smart TV out, Mary [P1] logs on to the Cyber-Trust platform [UCG-02] and designates that the Smart TV is temporarily disabled [UCG-10]. This allows the Cyber-Trust platform to know that (a) no activity should be present on behalf of the device (and similar activity traces should be flagged as anomalies) and (b) the inability to communicate with the device is not a security-related status demotion (e.g. a result of a DoS attack), but rather a scheduled outage.

Mary’s [P1] Smart TV returns from the service, where it has undergone a factory reset procedure. Mary installs it back, and the Cyber-Trust platform detects activity taking place from a device that is flagged as being temporarily disabled due to being serviced [UCG-09]. An alert is raised for Mary [P1, UCG-06], asking whether the device is legitimately reactivated (temporarily or permanently); otherwise the activity is owing to an identity theft attack. Until Mary [P1] responds, the trust level of the Smart TV is demoted to 0.1 and its risk level is raised to 0.9, to guard other devices from potential attack. Mary responds that the device is legitimately reactivated, so its trust and risk levels are restored to 0.8 and 0.1, respectively [UCG-10].

Since the vulnerability level of the Smart TV has not been assessed for the last 15 days, a vulnerability scanning is initiated [UCG-09]. The vulnerability scanner identifies that the Smart TV is vulnerable because the default login credentials for the administrator account are used; this flags a risk for complete device takeover (which implies the risk of use of the device to attack other devices) and personal data leakage. The Network architecture and assets repository [A16] is queried to identify network-level security defenses that are present for this device at network level. No security defenses are identified to be in effect for the specific device. A TMS running on Mary’s smartphone [A05] which is registered as a peer-level TMS in the domain of Mary’s smart home is queried to provide its own view on the level of trust of Mary’s Smart TV [UCG-13]; Mary’s smartphone [A05] replies reporting a trust level of 0.85. Given that the technical impact of the vulnerability is severe and that the attack is exploitable, the TMS reduces the device trust level from 0.9 to 0.2 [UCG-13]; the view of the peer-level TMS is taken into account for this computation. The risk level related to the current status of the device is increased from 0.2 to 0.65 [UCG-15]. The mitigation policy database is consulted [UCG-18] to determine which actions need to be taken in response to these changes to the trust and risk level. Following the specifications of the retrieved policy, an alert is raised for Tom (the security officer working at a Smart Home operator) [O2, UCG-06] and an alert is also issued for Mary [P1, UCG-06]. Further, the firewall present at the Smart Home Gateway of Mary’s Smart Home (a special case of a network-level security control) is instructed to block all incoming packets from the Internet to the Smart TV, except for the ones that are sent in the context of TCP connections established at the initiative of the Smart TV (to maintain its functionality) [UCG-18]. Finally, the TMS updates information about the available strategies (represented via attack graphs) attackers might follow in order to compromise the IoT device [UCG-15] which the malicious packet belongs is disrupted [UCG-18] and the network address from which the packet originates is blacklisted in the firewall present at the Smart Home Gateway of Mary’s Smart Home (a special case of a network-level security control) for a period of 20 minutes [UCG-18]. Information about the available strategies (represented via attack graphs) that attackers might follow in order to compromise the IoT device are updated accordingly [UCG-18].

4.3 Network-level attacks

Mary [P1], having already registered her smart home gateway into the Cyber-Trust platform [UCG-02], enabled the profiling service [A17] to gather information about the smart home’s network [UCG-16, UCG-09, UCG-16, UCG-10]. The information gathered from Mary’s network is used to update the Network architecture

Cyber-Trust Consortium. All rights reserved.

and assets repository [A16] that contains information about connectivity, and the profile DB [A17] where the vulnerabilities of smart home network's devices are enumerated. Mary is kept updated via her cross-platform visualization portal [A01] via [UCG-05] about the health status of her smart home's network and her devices. The Smart Home's traffic profile has already been established via [UCG-06], which establishes baseline traffic statistics, and so with the addition of the Smart TV [UCG-19] enables the baseline traffic statistics to be updated to take the new device into account.

The devices in the smart home network, for which Mary provides consent to be monitored [UCG-02] by Cyber-Trust enabled components, constitute critical resources and potential targets of an attacker; Mary could define the ones considered to be critical [UCG-04]. By retrieving from the VDB the exploits associated with all the vulnerabilities having been found in the smart home network [UCG-06, UCG-14], the Cyber-Trust components running at the smart home gateway compute the strategies on how an attacker can infiltrate the home network [UCG-15]. The necessary information that is retrieved from the VDB [UCG-06, UCG-14] will allow estimating an attack's likelihood and success probability [UCG-15] and determining the available mitigation actions [UCG-18], which are permissible according to the rules obtained from the mitigation policy database [UCG-18]. The necessary information on exploits' preconditions (i.e. the security conditions that must be true in order for the exploit to be attempted), such as necessary privileges or connectivity, and the postconditions (i.e. the security conditions that become true if the exploit is successfully carried out), like privileges gained or service disabled, are managed [UCG-16] by the VDB supervisor Bob [O1].

The Cyber-Trust's intelligent cyber-defense system [A04], running on Mary's [P1] smart home's gateway, has access to real-time security alerts [UCG-16] that are generated by the intrusion detection systems (i.e. smart home's IDS devices [A11, A12]) that allow to assess the current security status [UCG-15] and the extent to which a possibly ongoing cyber-attack threatens important assets of the smart home's network (the value of each asset is sourced from the Network architecture and assets repository [A16]). This system, being an *intelligent intrusion response system* (iIRS), has the ability of selecting the response actions in real-time [UCG-18] to mitigate the progression of a cyber-attacker in the smart home network while minimizing the negative impact that reactions have to the availability of network resources [UCG-04] to trusted devices (e.g. by refusing communication requests, shutting down running services, etc.). These responses modify a smart home's network security state (and lead to updated associated risk and trust scores [UCG-15, UCG-13]) and aim at mitigating an attack and blocking an attacker's progression by effectively blocking exploits that can be used from succeeding [UCG-18]. Since information coming from IDSs [UCG-16] usually suffers from false alarms, the iIRS manages the uncertainty over an attacker's current capabilities (what has been achieved so far) and true strategy by constructing beliefs [UCG-15] based on which the optimal response decisions [UCG-18] are made. The optimal response actions are either applied automatically [UCG-18] or they are first communicated [UCG-06] to Sarah that is a member of Operator SOC team [O2].

Sarah [O2] through the Visualisation portal [A01] is able to monitor IoT-SP [O4] traffic and the devices health status on the Gateway [UCG-05]. She noticed an unusual situation in her dashboard [A01]. Automatic response has been applied [UCG-18] and seems the network traffic returned to normal. However, Sarah wants to investigate what has happened and to make sure that the automatic response applied was the optimal. Through her dashboard she can move back in time [UCG-05] and investigate the network spikes. She zooms in the timeline and she notice that the network anomaly came from Mary's [P1] network. After reading the incident logs and network data stored in the secure database [UCG-12] through the DPI activated services [UCG-11] she found that the automated heating system controlled from a PLC was infected with a botnet and was trying to attack ISP servers through SYN flood attack. The DPI collected network data [UCG-08] were

Cyber-Trust Consortium. All rights reserved.

sent to the cloud where they will be analysed through the machine learning algorithm to produce new signatures for the iIRS.

The iIRS uses knowledge on an attack's impact and the costs of applying response actions [UCG-04] so as to quantify the trade-off between maintaining security and preserving availability of the smart home network. Based on the outcome of the response decision [UCG-18], the TMS is updated [UCG-13], and devices' information on the intelligent UI is also updated [UCG-05] (e.g. highlighting whether an IoT device has been compromised or ill-behaved) to alert Sarah. Depending on the situation (e.g. the impact of the attack being underway), Mary [P1] is also informed [UCG-06].

4.4 Device-level attacks

Mary [P1] is aware of the occurrence of persistent cyber-attacks and she would be interested in predominantly protecting her personal data [D3]. She is therefore interested in accessing the Cyber-Trust visualisation platform and assessing possible vulnerabilities related to her devices [UCG-05] and the overall risk of her household [UCG-01, UCG-09].

Mary [P2], a technology enthusiast has equipped her home with a series of smart devices. Mary [P1], who has heard of Cyber-Trust [O1] decided to create an account [UCG-02], [D1] and register some of her devices [UCG-02] for active monitoring [A03] and the rest for passive [UCG-09]. She therefore chooses to secure her main network gateway along with other IoT devices for active monitoring [A03]; device level agents are installed on resource unconstraint devices [UCG-01] while monitoring [A03] at gateway level is performed for the rest [UCG-09].

Mary runs a health scan for her devices for the detection of possible vulnerabilities related to her recently registered devices [UCG-07] and the overall risk of her household [UCG-15] through the Cyber-Trust device management system [A05] and the Trust Management System [A05].

Mary would be greatly interested in the prevention of eavesdropping and hacking attacks [UCG-18]. For this, Cyber-Trust monitors in real time the traffic towards and from these devices [UCG-08] as well as use of resources (with metrics such as CPU and memory consumption as well as running processes) [UCG-10], generating insights on behaviour trends and patterns [UCG-01, UCG-08]. The active monitoring of Cyber-Trust maintains hashes and signatures for critical system data [UCG-08] to its centralized content management system which is continuously updated against eVDB [A07] for emerging vulnerabilities for the prevention of fraudulent software [UCG-14, UCG-16, UCG-09] and firmware update [UCG-07] related to Mary's registered devices [P1]. Critical information such as firmware hashes, digital signatures, timestamps of access and modification, source and destination IP addresses/ports and transmission protocols are securely stored on the Cyber-Trust blockchain for integrity preservation. In the event of malicious traffic detection, intelligent mitigation and remediation actions taken place where possible [UCG-18, UCG-17], also depending on the configuration Mary [P1] has made in her personal profile [D3].

For the remaining of her devices, Mary [P1] has chosen to proceed with passive monitoring [A03] and as a result she has provided Cyber-Trust with the relevant information with regards to the make, model and specifications of each device (including installed firmware version and production details) [UCG-10]. In case new vulnerabilities emerge with respect to any of her devices, Mary [P1] is notified through the Cyber-Trust portal [UCG-06] for the rise of her home risk factor and will be advised with recommendations towards increasing the security of his household [UCG-18].

Cyber-Trust Consortium. All rights reserved.

Having heard of emerged cyber threats that take into advantage the resources of powerful devices, Mary has decided to add a device [UCG-02], that was up to that point in passive monitoring [A03] to active monitoring [UCG-09, A03]. Upon registration of this device [A06] the Cyber-Trust platform monitors the network activity of this device [UCG-08] and performs checks with regards to firmware integrity, patching status and known vulnerabilities [UCG-07, UCG-14]. Cyber-Trust monitors the utilisation of resources over time and may recognize attempts to utilise power from such devices [UCG-10]. She therefore proceeds by integrating Cyber-Trust in the communication of this device. Cyber-Trust generates analytics and statistics on the use of this device and may recognise abnormal usage of device resources. In such cases the Cyber-Trust platform requests Mary [P1] to justify the increased usage of resources [UCG-18]. In the case of suspicious activity Cyber-Trust may block malicious requests to the device and syncs the new findings with the Cyber-Trust backend [UCG-17, UCG-10]. Additionally, Mary may observe discrepancies in device resource consumption by comparing the vendor's and Cyber-Trust's statistics.

4.5 Forensic evidence collection

Bob, CEO of a Smart Device Security Company [O5], after seeing its flagship home surveillance product being hacked, has decided to join Cyber-Trust, hence, he registered himself [UCG-02] and his organization in Cyber-Trust [UCG-02] and registered a new device class for its home surveillance router [UCG-02]. Then, the new device is Cyber-Trust-enabled and marketed as such.

Tom, an ISP security officer [O2] has registered the new Cyber-Trust-enabled home router [UCG-02]. Mary, a smart home owner [P1] changed her provider to CityISP provider who offers Cyber-Trust enabled smart appliances. Mary [P1] also has legacy smart appliances, like her home surveillance system. After registering and logging herself on Cyber-trust platform [A04], UCG-02], she can see all devices on her local network and their information [UCG-10]. Thus, she can choose the level of information sharing of her appliances with Cyber-Trust platform [UCG-19]. In addition, she chooses to share maximum data to be protected. She logs out of the platform [UCG-03]. Her devices will now store their logs into the DLT [UCG-14, A02].

Tom, [O2] receives an alert [UCG-18] about unusual behavior of one of its company devices which is a Cyber-Trust-enabled appliance. The behavior suggests that the device is under cyber-attack (DDOS), also effecting/endangering the ISP. The affected device is a home surveillance system, which is the Customer's property, so he cannot investigate further, he then informs Hutch [O3], a Police officer. Hutch asks for anonymized device information [UCG-04] from Cyber-Trust [UCG-10] and decides to explore and visualize the logs [UCG-12] for a selection of these devices, as well as on the related Cyber-Trust enabled routers [UCG-12]. The logs show that the attack is targeting the device's telnet/FTP UPNP ports on the router and is running a .exe associated with recent DDoS, and Spam campaigns. He stores the evidence in the DLT [A02, UCG-14]. To propagate this data on the network the DLT [A02] will validate the block of evidence [UCG-12, A02].

Due to the great threat imposed from the attack, Mary [P1] is notified by an ISP representative [O2] for the severity of the situation and to provide her consent regarding the ISP [O2] implementing any measures necessary in order to mitigate the threat. Thus, the ISP [O2] decides to remotely shut down the Cyber-Trusted -enabled surveillance system. The shutdown command is sent to the affected device but is ignored by the firmware. Then, as per [UCG-18] the router is instructed to stop relaying traffic from the mac address range of the device [UCG-19].

Due to the nature of the attack Police [O3] continues the investigation and arrests a suspect. Based on the trusted logs [UCG-12], the evidences [UCG-12] and the explanation/methodology used for storing these evidences [UCG-14] and the data found in the suspects machines the judge rules for the conviction of the suspect.

Cyber-Trust Consortium. All rights reserved.

Cyber-Trust Consortium. All rights reserved.

5 Domain 2 - Mobile Devices

Mobile, or cellular, networks are made up of "cells" that connect to one another and to telephone switches or exchanges. These cells are areas of land that are typically hexagonal, have at least one transceiver, and use various radio frequencies. These transceivers are the cell towers that have become ubiquitous in our electronically connected world. They connect to each other to hand off packets of signals—data, voice, and text—ultimately bringing these signals to mobile devices such as phones and tablets that act as receivers. Providers use each others' towers in many areas, creating a complex web that offers the widest possible network coverage to subscribers.

Machine-to-machine (M2M) communication is an enabling technology for the Internet-of-Things (IoT), a modern edge-device networking concept defined previously in Domain 1. It enables autonomous connectivity and communication among devices ranging from embedded low-power devices to powerful compute-rich devices. Device-to-device (D2D) connections can be used to establish M2M communication in IoT networks and devices since they afford ultra-low latency and hence, real-time responses [7], which allow safety and time critical devices to function as required as shown in Figure 5.1. A particular application is vehicle-to-vehicle (V2V) communication where D2D links can be utilized to share information between neighboring vehicles quickly and offload traffic efficiently. They can also be harnessed for vehicle-to-infrastructure and vehicle-to-pedestrian communication. Using D2D communication, a large amount of data can be transferred quickly between mobile devices in short range.

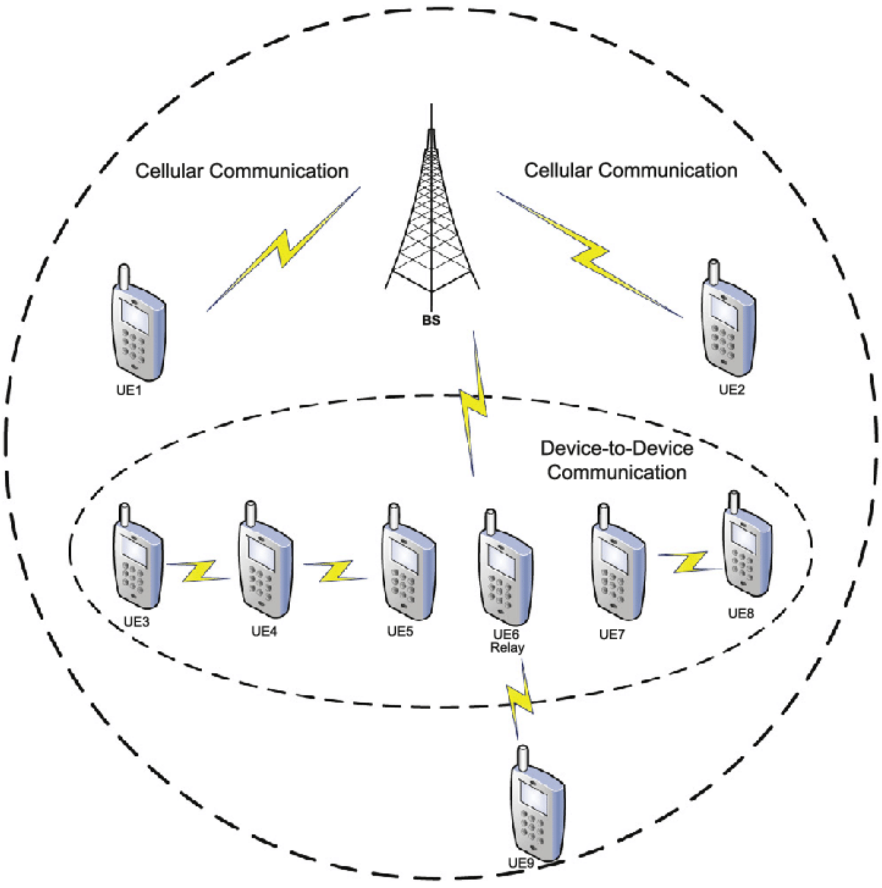

Figure 5.1: M2M and Cellular Communication Network (Kar and Sanyal, 2017)

Cyber-Trust Consortium. All rights reserved.

D2D communication affords stronger anonymity and data privacy compared to conventional cellular communication since the data are not stored at a central location. However, various common attacks like eavesdropping, denial of service, man-the-middle, node impersonation, IP spoofing, malware attack, etc. can paralyze D2D links. Users would also like to protect their privacy, e.g., by restricting the availability of their sensitive personal data. The same lack of a central authority makes it difficult to implement security and privacy measures. Authors in [3] model threats in a three-dimensional space: (1) whether the attacker is internal or external, (2) whether the attacker is active (e.g., it modifies in-transit data) or passive (e.g., it only snoops on data), and (3) whether the attack is local or extended across the network. Several proposals to safeguard D2D networks are reviewed in [3,22].

Mobile device security threats are on the rise. In 2014, Kaspersky Lab detected almost 3.5 million pieces of malware on more than 1 million user devices. And as reported by IT Web, the number of new malware programs detected each day has reached over 230,000--many of which target mobile devices. That shows attackers have increasing interest on using our Mobile Devices for mobile malware that mines monero, bombards our devices with unwanted ads, and can even be used to launch denial of service attacks.

To this end this scenario explores the reaction of Cyber-Trust to devices entering the Cellular provider's network infected with the RottenSys botnet, an Android-based adware which uses a play store app for initial installation and evasion processes once the app is installed, and has successfully infected nearly five million devices since 2016[1], and aggressively displays on the device's home screen, as pop-up windows or full-screen ads to generate fraudulent ad-revenues. The infected devices are communicating through Bluetooth and WiFi with Cyber-Trust enabled and not Cyber-Trust enabled devices and exchanging files. Figure 8.1 Domain 2, shows the Cyber-Trust cellular architecture in high-level so as to place the domain, scenario and use cases in the correct context.

5.1 Cyber-threat intelligence discovery and sharing

Mary, a mobile device owner [P2], has been informed about Cyber-Trust from her ISP [O2] that also provides all the smart home services. Mary [P2] is registered in the Cyber-Trust platform [UCG-02] where she can monitor [UCG-05] her devices' health status [UCG-05], [UCG-10]. She decided to add her mobile device on the Cyber-Trust Platform [UCG-02] in order to monitor the device and detect misbehaving activity [UCG-05]. As such, Mary [P2] relies on the Cyber-Trust platform to ensure that her mobile devices are protected and will indeed remain secure across the existing Cellular provider network.

Mary [P2] buys a new smartphone; she decides to register it into the Cyber-Trust platform to safeguarding [UCG-02] it through Cellular provider network. During registration [A06], Cyber-Trust system allows Mary [P2] to provide information about the smartphone (e.g., name, version of firmware, operating system, and etc.) and use Cyber-Trust's eVDB [A07] to search [UCG-05] for any security issues that pertain to her newly acquired smartphone [UCG-06]; at the moment, nothing comes up. She decides to subscribe to the publish/subscribe service that is offered by the Cyber-Trust platform to be promptly notified about any updates and security-related issues that may rise in the future [UCG-02]. Mary is able to tune the information she would like to receive [UCG-02] from Cyber-Trust platform (e.g., type of updates/alerts, desired level of alert confidence, desired impact threshold). As Mary is not a security analyst, she decides to be notified only for high confidence/high impact alerts [UCG-14].

Tom is a security officer [O2] working at a Cellular provider network and wants to search for, uncover, [UCG-06] and be notified about possible attacks [UCG-02] that are likely to pose a risk to the mobile devices his

[1] https://research.checkpoint.com/rottensys-not-secure-wi-fi-service/

Cyber-Trust Consortium. All rights reserved.

company supports. He also wants to identify and prioritize these cyber-threats [UCG-16] with the highest potential for negative impact on the supported mobile devices by resorting to gathered cyber-threat intelligence. To do so, he registers the supported mobile devices with the Cyber-Trust platform [UCG-02] and subscribes to its publish/subscribe service [UCG-02]; the system stores the mobile devices' profiles and matches them [UCG-14] against the contents of the eVDB [A07] to determine possible exploits and attacks that have been collected from the clear, deep, and dark web. The system then communicates the matched vulnerabilities and exploits to the security officer through an appropriate intelligent UI [UCG-14], indicating also issues that are pivotal or of high priority.

Since Tom is particularly interested in protecting the mobile devices from certain types of attacks, he augments his subscription with keywords related to the attacks he is interested in being notified for [UCG-02]. Moreover, to stay on the safe side regarding new threats that may affect the mobile devices his company supports, he sets the confidence level of receiving alerts to the lowest possible [UCG-02]. This means that a continuous query for the registered mobile devices is created, allowing him to receive notifications for all newly discovered vulnerabilities and exploits [UCG-14] that are inserted into the eVDB [A07] (even without verification) and be presented with a summary of the eVDB [A07] vulnerabilities affecting the mobile operator's devices [UCG-11]. The difference in the Cyber-Trust usage between Mary (a technology aware person [P2]) and Tom (a security officer [O2]) lies not only on the number of mobile devices they control, but also on the attack mitigation options they may apply [UCG-14]; for instance, Tom [O2] has access to a wider variety of mobile devices and gateways.

Meanwhile, the cyber-threat discovery module of Cyber-Trust is already bootstrapped and since then is continuously crawling popular social media streams [A10], popular security-related websites and deep/dark web forums and marketplaces [UCG-16]. Cyber-Trust searches for cyber-threat information including zero-day vulnerabilities and exploits, signatures, executables, and other related information. To this end, it uses an ensemble of state-of-the-art data and knowledge processing and machine learning techniques to identify the (clear/deep/dark) web pages that should be crawled and to extract and contextualize all relevant threat information [UCG-16]. The collected data may refer to a new threat that has to be inserted into the eVDB [A07], or new information about known threats (e.g., exploits) that will update the eVDB entries and enrich the stored intelligence [UCG-16]. New information is initially added to the eVDB [A07] with a low level of confidence in the existence of the vulnerability (as it has possibly not been validated yet by security experts) and the credibility of the known technical details [UCG-06]. The function of the cyber-threat discovery module is supervised by an IT expert (Bob, [O2], see more details below) that is responsible to add, annotate, and approve the crawling of new seeds [A10] (i.e., websites of interest), tune the crawling parameters [A10] that enable their discovery, and evaluates existing seeds in terms of usefulness [UCG-19].

While on operation, the cyber-threat discovery surfaces information about a new zero-day vulnerability and inserts it into the eVDB [A07] with a low confidence level [UCG-16]. Then, the system updates information about the risk that this new exploit poses to the affected registered mobile devices [UCG-15], the trust score that is associated with the mobile devices [UCG-16], and the available strategies (represented as attack graphs) that attackers might follow for compromising the mobile devices [UCG-15]. Based on their preferences [UCG-02], Tom is notified through multiple channels [UCG-14], e.g. via email messages or the intelligent UI, for the new vulnerability and the affected mobile devices (since he requires low confidence levels), but, Mary does not (since she is seeking high confidence). After examining the eVDB [A07] info about the new threat, Tom decides to take appropriate [UCG-18].

John is an external actor [O1] working as a vulnerability assessment expert which is examining and assessing newly discovered cyber-threats [UCG-06]. Over the last few days he has been reviewing the new

Cyber-Trust Consortium. All rights reserved.

vulnerabilities that were surfaced by Cyber-Trust [UCG-06] and now decides that there exists enough evidence to update the *report confidence* (RC) field of the newly discovered vulnerabilities in the eVDB [A07] from "not defined" to other confidence levels (e.g. "unknown", "reasonable", or "confirmed") that are being assigned after the existence of the vulnerability is acknowledged [UCG-06]. Due to this update, Mary is now notified for the newly confirmed vulnerability [UCG-14]. John also provides feedback on the quality of the information gathered about considers some new seeds; some are approved and are annotated for usage [UCG-06].

Finally, Sarah, a security officer working in the control room at the Cellular provider network operator [O2], has been alerted about suspicious behaviour in the Cellular provider network [UCG-06]. She uses the eVDB [A07, UCG-06] to query for similar behavioural patterns in the hope to learn more about attack types that produce this type behaviour and to identify in advance possible solutions [UCG-06]. In an analogous way, the eVDB [A07] information is also utilized, by the different Cyber-Trust modules to query for relevant intelligence (e.g., similar threats, rule updates, identified signatures, or mitigation strategies [UCG-06], see also [UCG-18] and [UCG-14].

5.2 Monitoring and vulnerability assessment

Mary, a mobile device owner [P2], has bought a new smartphone. She has registered the mobile device to the Cyber-Trust platform [UCG-02] and the device model, firmware & operating system version, and the list of patches that have been applied to the mobile device are known and stored in the device profile service [UCG-10, A17]. Mary did not enter this information during the mobile device registration phase [UCG-02, A06] however, the Cyber-Trust profiling service [A17] was able to determine this information through remote detection techniques [UCG-16]. As the eVDB [A07] has been recently updated with new vulnerabilities, the TMS retrieves the mobile device data from the device profile service [UCG-10] and newly added vulnerabilities from the eVDB [UCG-06, A07] and identifies that a new vulnerability has been discovered for this device, which can be exploited to install malware on the smartphone. Therefore, the TMS triggers a new computation of the mobile device trust level [UCG-13] in this context, the network architecture and assets repository [A16] is queried to determine security defences that are present on the device and the Network architecture and assets repository [A16] is queried to identify network-level security defences that are present for this mobile device at network level. Only a firewall (a special case of a network-level security control) is identified to be in effect for the particular mobile device, which is able to block exploitation attempts from outside the Cellular provider network perimeter, however is not able to mitigate attacks from rogue or infected mobile devices being inside the Cellular provider perimeter. Given that the technical impact of the vulnerability is severe and that the attack is exploitable, the TMS reduces the mobile device trust level from 0.8 to 0.3. The risk level related to the current status of the device is increased from 0.1 to 0.6 [UCG-06]. The mitigation policy database is consulted [UCG-18] to determine which actions need to be taken in response to these changes to trust and risk level. Following the specifications of the retrieved policy, an alert is raised for Tom (the security officer working at a Cellular provider network) [UCG-06] and an alert is also issued for Mary [P2, UCG-06, UCG-05]. Finally, the TMS updates information about the available strategies (represented via attack graphs) attackers might follow in order to compromise the mobile device [UCG-15].

At the information security department of the ISP, Tom (a security officer working for the ISP) receives the alert and decides to check the vulnerability status and trust levels of all mobile devices that are produced by the same manufacturer and are registered with the Cyber-Trust system. To this end, he uses the Intelligent UI to request firstly a visual report of the mobile devices of a particular type that are produced by the same

Cyber-Trust Consortium. All rights reserved.

manufacturer [UCG-05]. The system displays the requested visualization [A01], indicating that 10 mobile devices have vulnerabilities of high impact, 6 mobile devices have vulnerabilities of medium impact, 2 mobile devices have vulnerabilities of low impact and 8 mobile devices have no known vulnerabilities. Then, Tom requests that the trust level visualization is displayed [UCG-05, A01]; Tom notices that some mobile devices with medium vulnerability levels are reported as having low trust levels and based on this he concludes that these mobile devices have been hacked and the low trust level is owing to their observed behaviour. Tom notifies the ISP field service team to schedule a detailed security inspection for these devices.

Tom, while reviewing his mailbox, finds out that a new model of mobile devices is released. Tom schedules a meeting with other security officers and they conclude that even medium-level vulnerabilities for this model of mobile devices should be considered as critical, because if they are exploited they can lead to either uncontrolled access to the area they protect or inability to access the area. To this end, Tom curates the mitigation policy database [UCG-14] to enter a policy rule that reflects the decision reached.

Mary's [P2] Cellular provider installation hosts also a mobile device, which is malfunctioning; therefore, she takes it to be serviced. Since the mobile device has been however already registered to the Cyber-Trust platform with an "Always available" designation, before turning the mobile device off, Mary [P2] logs on to the Cyber-Trust platform [UCG-02] and designates that the mobile device is temporarily disabled [UCG-10]: this allows the Cyber-Trust platform to know that (a) no activity should be present on behalf of the device (and similar activity traces should be flagged as anomalies) and (b) the inability to communicate with the device is not a security-related status demotion (e.g. a result of a DoS attack), but rather a scheduled outage.

Mary's [P2] mobile device returns from the service, where it has undergone a factory reset procedure. Mary installs it back, and the Cyber-Trust platform detects activity is taking place from a device that is flagged as being temporarily disabled due to being serviced [UCG-09]. An alert is raised for Mary [P2, UCG-06], asking whether the mobile device is legitimately reactivated (temporarily or permanently); otherwise the activity is owing to an identity theft attack. Until Mary [P2] responds, the trust level of the mobile device is demoted to 0.1 and its risk level is raised to 0.9, to guard other mobile devices from potential attack. Mary responds that the device is legitimately reactivated, so its trust and risk levels are restored to 0.8 and 0.1, respectively [UCG-10].

Since the vulnerability level of the mobile device has not been assessed for the last 15 days, a vulnerability scanning is initiated [UCG-09]. The vulnerability scanner identifies that the mobile device is vulnerable because the default login credentials for the administrator account are used; this flags a risk for complete device takeover (which implies the risk of use of the device to attack other devices) and personal data leakage. The Network architecture and assets repository [A16] is queried to identify network-level security defences that are present for this device at network level. No security defences are identified to be in effect for the specific device. A TMS running on Mary's smartphone which is registered as a peer-level TMS in the domain of Mary's smart home is queried to provide its own view on the level of trust of Mary's mobile device [UCG-13]; Mary's smartphone replies reporting a trust level of 0.85. Given that the technical impact of the vulnerability is severe and that the attack is exploitable, the TMS reduces the device trust level from 0.9 to 0.2; the view of the peer-level TMS is taken into account for this computation. The risk level related to the current status of the device is increased from 0.2 to 0.65 [UCG-15]. The mitigation policy database is consulted [UCG-18] to determine which actions need to be taken in response to these changes to the trust and risk level. Following the specifications of the retrieved policy, an alert is raised for Tom (the security officer working at a Cellular provider network) [UCG-06] and an alert is also issued for Mary [P2, UCG-06]. Further, the firewall present at the Cellular provider Gateway of Mary's Cellular provider network (a special case of a network-level security control) is instructed to block all incoming packets from the Internet to the

Cyber-Trust Consortium. All rights reserved.

mobile device, except for the ones that are sent in the context of TCP connections established at the initiative of the mobile device (to maintain its functionality) [UCG-18]. Finally, the TMS updates information about the available strategies (represented via attack graphs) attackers might follow in order to compromise the mobile device [UCG-15] which the malicious packet belongs is disrupted [UCG-18] and the network address from which the packet originates is blacklisted in the firewall present at the Cellular provider Gateway of Mary's Cellular provider network (a special case of a network-level security control) for a period of 20 minutes [UCG-18]. Information about the available strategies (represented via attack graphs) that attackers might follow in order to compromise the mobile device are updated accordingly [UCG-18].

5.3 Network-level attacks

Mary [P2], having already registered her smartphone into the Cyber-Trust platform [UCG-02], enabled the profiling service [A17] to gather information about the network, which contains all the devices that are connected to Mary's smartphone [UCG-16, UCG-09, UCG-10]. The information gathered from Mary's smartphone network is used to update the Network architecture and assets repository [A16] and the network architecture and assets repository [A16] that also contain information about connectivity, and the profile DB [A17] where the vulnerabilities of the network's devices are enumerated. Mary is kept updated via her cross-platform visualization portal [A01] via [UCG-05] about the health status of her smartphone's network. The smartphone's traffic profile has already been established via [UCG-06], which establishes baseline traffic statistics, and so with the addition of the Smart TV [UCG-19] enables the baseline traffic statistics to be updated to take the new device into account.

The devices in the network, for which Mary provides consent to be monitored [UCG-02] by Cyber-Trust enabled components, constitute critical resources and potential targets of an attacker; Mary [P2] could define the ones considered to be critical [UCG-04]. By retrieving from the VDB the exploits associated with all the vulnerabilities having been found in the smartphone's network [UCG-06, UCG-14], the Cyber-Trust components running at the gateway compute the strategies on how an attacker can infiltrate the network [UCG-15]. The necessary information that is retrieved from the VDB [UCG-06, UCG-14] will allow estimating an attack's likelihood and success probability [UCG-15] and determining the available mitigation actions [UCG-18], which are permissible according to the rules obtained from the mitigation policy database is consulted [UCG-18]. The necessary information on exploits' preconditions (i.e. the security conditions that must be true in order for the exploit to be attempted), such as necessary privileges or connectivity, and the postconditions (i.e. the security conditions that become true if the exploit is successfully carried out), like privileges gained or service disabled, are managed [UCG-16] by the VDB supervisor Bob [O1].

The Cyber-Trust's intelligent cyber-defense system [A04], running on Mary's [P2] smartphone gateway, has access to real-time security alerts [UCG-16] that are generated by an intrusion detection system (i.e. smartphone's IDS devices [A11, A12]) that allows to assess the current security status [UCG-15] and the extent to which a possibly ongoing cyber-attack threatens important assets of the smartphone's network (the value of each asset is sourced from the Network architecture and assets repository [A11]). This system, being an *intelligent intrusion response system* (iIRS), has the ability of selecting the response actions in real-time [UCG-18] to mitigate the progression of a cyber-attacker in the smartphone's network while minimizing the negative impact that reactions have to the availability of network resources [UCG-04] to trusted devices (e.g. by refusing communication requests, shutting down running services, etc.). These responses modify the network's security state (and lead to updated associated risk and trust scores [UCG-15, UCG-13]) and aim at mitigating an attack and blocking an attacker's progression by effectively blocking exploits that can be used

Cyber-Trust Consortium. All rights reserved.

from succeeding [UCG-18]. Since information coming from the IDS [UCG-16] usually suffers from false alarms, the iIRS manages the uncertainty over an attacker's current capabilities (what has been achieved so far) and true strategy by constructing beliefs [UCG-15] based on which the optimal response decisions [UCG-18] are made. The optimal response actions are either applied automatically [UCG-18] or they are first communicated [UCG-06] to Sarah that is a member of Operator SOC team [O2].

Sarah [O2] through the Visualisation portal [A01] she is able to monitor IoT-SP [O4] traffic and the devices health status on the network [UCG-05]. She noticed an unusual situation on her dashboard [A01]. Automatic response has been applied [UCG-18] and seems the network traffic returned to normal. However, Sarah wants to investigate what was happen and make sure that the automatic response applied was the optimal. Through her dashboard she can move back in time [UCG-05] and investigate the network spikes. She zooms in the timeline and she notice that the network anomaly came from Mary's[P1] mobile device. After reading the incident logs and network data stored in the secure database [UCG-12] through the DPI activated services [UCG-11] she found that Mary's[P1] mobile device was infected with a botnet and was trying to attack ISP servers through SYN flood attack. The DPI collected network data[UCG-08] were sent to the cloud where they will be analysed through the machine learning algorithm to produce new signatures for the iIRS.

The iIRS uses knowledge on an attack's impact and the costs of applying response actions [UCG-04] so as to quantify the trade-off between maintaining security and preserving availability of the network. Based on the outcome of the response decision [UCG-18], the TMS is updated [UCG-13], and devices' information on the intelligent UI is also updated [UCG-05] (e.g. highlighting whether an IoT device has been compromised or ill-behaved) to alert Sarah. Depending on the situation (e.g. the impact of the attack being underway), Mary [P2] is also informed [UCG-06].

5.4 Device level attacks

Mary [P2], a technology enthusiast is using a series of smartphones devices of different kinds. Mary [P2], who has heard of Cyber-Trust decided to create an account [UCG-02], [D1] and register some of her smartphone devices into Cyber-Trust platform [UCG-02] and the rest with passive monitoring [A03, UCG-07]. She therefore chooses to secure her devices for active monitoring; therefore, device level agents apps are installed on devices [UCG-01].

Mary [P2] is aware of the occurrence of persistent cyber-attacks and she would be interested in predominantly protecting her personal data. She is therefore interested in accessing the Cyber-Trust visualisation platform and assessing possible vulnerabilities related to her smartphone devices [UCG-05].

Mary [P2] would be greatly interested in the prevention of eavesdropping and hacking attacks [UCG-16]. For this, Cyber-Trust monitors in real time the traffic towards and from these smartphone devices [UCG-08] as well as use of resources (with metrics such as processor and memory consumption as well as running processes) [UCG-14], generating insights on behavior trends and patterns [UCG-10]. The active monitoring [A03] of Cyber-Trust maintains hashes and signatures for critical system data [UCG-07] to its centralized content management system [A05] which is continuously updated against eVDB [A07] for emerging vulnerabilities for the prevention of fraudulent software [UCG-07] and firmware update [UCG-14] related to Mary's registered devices [P2]. Critical information such as firmware hashes, digital signatures, timestamps of access and modification, source and destination IP addresses/ports and transmission protocols are securely stored on the Cyber-Trust blockchain for integrity preservation purposes [UCG-14]. In the event of

Cyber-Trust Consortium. All rights reserved.

malicious traffic detection, intelligent mitigation [UCG-18] and remediation actions [UCG-17] take place where possible, also depending on the configuration Mary [P2] has made in her personal profile.

For the remaining of her smartphone devices, Mary [P2] has chosen to proceed with passive monitoring [A03] and as a result she has provided Cyber-Trust with the relevant information with regards to the make, model and specifications of each device (including installed firmware version and production details) [UCG-07]. In case new vulnerabilities emerge with respect to any of her devices, Mary [P2] is notified through the Cyber-Trust portal [UCG-14] for the rise of her smartphone risk factor and will be advised with recommendations towards increasing the security of her devices [UCG-15, UCG-14].

Having heard of emerged cyber threats that take into advantage the resources of smartphone devices, Mary [P2] has decided to add a device, that was up to that point in passive monitoring [A03] to active monitoring instead [UCG-01]. Upon registration [A06] of this device the Cyber-Trust platform monitors the network activity of this device [UCG-18] and performs checks with regards to firmware integrity [UCG-07], patching status and known vulnerabilities [UCG-07]. Cyber-Trust monitors the utilisation of resources over time and may recognise attempts to utilise power from such devices. She therefore proceeds by integrating Cyber-Trust in the communication of this device. Cyber-Trust generates analytics and statistics on the use of this device and may recognise abnormal usage of device resources. In such cases the Cyber-Trust platform requests Mary [P2] to justify the increased usage of resources [UCG-10]. In the case of suspicious activity Cyber-Trust may block malicious requests to the smartphone device and syncs the new findings with the Cyber-Trust backend [UCG-18, UCG-17, UCG-10]. Additionally, Mary [P2] may observe discrepancies in device resource consumption by comparing the vendor's and Cyber-Trust's statistics [UCG-19].

5.5 Forensic evidence collection

Bob, CISO [O2] of SmartphoneSec Ltd phone manufacturer, after seeing its flagship smartphone product being hacked [UCG-18], decide to export the trusted logs of the incriminated devices [UCG-12], if their owner activated the maximum sharing information level [UCG-19]. The trusted logs show that the device is now exposing telnet/FTP/FTP UPNP ports on the network router and is conducting DDoS, and Spamming. He decides to store its conclusion on its company forensic evidence DB [UCG-14]. The Cyber-Trust platform is being notified of the addition of a new forensic off-chain. It receives the timestamp of the attack, the type of the incriminated device in the attack, the target of the attack [UCG-14]. The system creates the hash based on the metadata it received and validate the block of evidence [UCG-12].

In the same time, Mary [P-2] owner of one of the smartphones performing the attack receives an email informing her of the on-going attack. She decides to close the port of the smartphones which is being used to DDOS via the Cyber-Trust platform [UCG-19].

Due to the nature of the attack Police [O3] starts an investigation. They start it by using the visualization tool provided by the Cyber-Trust platform [UCG-12]. The platform allows them to filter the forensic data by the device performing the attack and the type of the attack. They found the metadata data provided by Bob, CISO [O2] of SmartphoneSec Ltd phone manufacturer, the Police[O3] export the metadata of the forensic [UCG-12]. In order to continue their investigation, the Police [O3] ask SmartphoneSec for the evidence which is stored off chain on the company's forensic evidence DB. The manufacturer refuses to provide the actual evidence without a warrant of a judge.

Cyber-Trust Consortium. All rights reserved.

6 Use cases

The use cases presented in this section composed from the functional components of Cyber-Trust project. The use case covers the two (2) domains incidents and the respective scenarios of each domain explained in Section 4 and 5. This use case will the stepping stone to produce in WP4 the architecture of the Cyber-Trust Ecosystem.

6.1 Overview of identified use cases

From the domains in Section 4 and 5 we have identified 82 total use cases which are group in 19 Categories and presented in the table below. The use cases will be explained in detail in section 6.3

Category 1: Setup End Device - UCG-01

UC ID	UC Name
UCG-01-01	Activate device agent
UCG-01-02	Deploy Cyber-Trust device agent

Category 2 Registration Policies & Sessions - UCG-02

UC ID	UC Name
UCG-02-01	Register user into Cyber-Trust platform
UCG-02-02	Register organization into Cyber-Trust platform.
UCG-02-03	Register device (including device class) into Cyber-Trust platform.
UCG-02-04	Log on to the Cyber-Trust platform
UCG-02-05	Register to the eVDB sharing service

Category 3: Deactivation Policies & Sessions - UCG-03

UC ID	UC Name
UCG-03-01	Log out from the Cyber-Trust platform
UCG-03-02	Unregister User
UCG-03-03	Unregister Organisation
UCG-03-04	Unregister device

Category 4: System Definitions - UCG-04

UC ID	UC Name
UCG-04-01	Private IoT Device Profile generation
UCG-04-02	Characterize asset’s importance
UCG-04-03	Define mitigation actions’ impact

Cyber-Trust Consortium. All rights reserved.

Category 5: Cyber-Trust Portal: Visualisation Tools - UCG-05

UC ID	**UC Name**
UCG-05-01	2D View Systems State
UCG-05-02	3D-Virtual Reality View Systems State
UCG-05-03	Visualize summary of eVDB contents matching an operator's devices
UCG-05-04	Visualize network's health status
UCG-05-05	Visualize device vulnerability levels
UCG-05-06	Visualize network traffic
UCG-05-07	Visualize device trust level
UCG-05-08	Visualize known and zero day vulnerabilities
UCG-05-09	Visualize historical (heterogeneous) data

Category 6: Cyber-Trust Portal: Decision Support & Alerting - UCG-06

UC ID	**UC Name**
UCG-06-01	Raise alert for security officer
UCG-06-02	Raise alert for device owner
UCG-06-03	Establish baseline traffic statistics
UCG-06-04	Query and retrieve information from eVDB
UCG-06-05	Review and validate eVDB entries.
UCG-06-06	Provide feedback/rating on sources of vulnerabilities.
UCG-06-07	Communicate iIRS actions to the security officer

Category 7: Host based health check: UCG-07

UC ID	**UC Name**
UCG-07-01	Check device patching status
UCG-07-02	Host based vulnerability scanning
UCG-07-03	Ensure Device firmware integrity

Category 8: Network based health check: UCG-08

UC ID	**UC Name**
UCG-08-01	Monitor device at gateway (network traffic filtering)
UCG-08-02	Capture and classify network packets (DPI)

Category 9: Cyber-Trust Monitoring Activities: UCG-09

UC ID	**UC Name**
UCG-09-01	Monitor device critical OS files / vulnerabilities

Cyber-Trust Consortium. All rights reserved.

UCG-09-02	Monitor activity on device
UCG-09-03	Perform vulnerability scanning
UCG-09-04	Detect network attacks

Category 10: IoT Profiling & Data Analytics: UCG-10

UC ID	UC Name
UCG-10-01	Device Profiling
UCG-10-02	Data Anonymisation
UCG-10-03	Retrieve device profile information
UCG-10-04	Manually curate device profile
UCG-10-05	Gateway Network Device Profiling
UCG-10-06	Get Device Information

Category 11: Forensic Evidence Collection: UCG-11

UC ID	UC Name
UCG-11-01	Gather device forensic evidence
UCG-11-02	Gather network forensic evidence

Category 12: Forensic Evidence Exploration & Export: UCG-12

UC ID	UC Name
UCG-12-01	Export Trusted logs
UCG-12-02	Export Forensic evidence
UCG-12-03	Explore trusted logs
UCG-12-04	Visualize forensics
UCG-12-05	Validate evidence block

Category 13: Cyber-Trust Trust Characterisation: UCG-13

UC ID	UC Name
UCG-13-01	Retrieve trust level from TMS
UCG-13-02	Compute device trust level

Category 14: Data Repositories & Correlation: UCG-14

UC ID	UC Name
UCG-14-01	Update device critical OS files/vulnerabilities
UCG-14-02	Manage available patch databases
UCG-14-03	Curate mitigation policy database

Cyber-Trust Consortium. All rights reserved.

UCG-14-04	Curate forensic evidence database
UCG-14-05	Store Trusted logs
UCG-14-06	Store forensic evidence
UCG-14-07	Notify about updates and security-related issues.
UCG-14-08	Match device profile with eVDB contents

Category 15: Computation of attack surface & metrics: UCG-15

UC ID	UC Name
UCG-15-01	Compute cyber-attack graphical security model
UCG-15-02	Compute device risk level
UCG-15-03	Compute attack's likelihood and success probability
UCG-15-04	Compute a belief on current security status

Category 16: Discovery & Intelligence: UCG-16

UC ID	UC Name
UCG-16-01	Determine device firmware and software through remote detection
UCG-16-02	Discover network
UCG-16-03	Receive intrusion detection system(s) alerts
UCG-16-04	Identify and prioritize cyber-threats.
UCG-16-05	Crawl the clear/deep/dark web and update the eVDB.

Category 17: Remediation Policies: UCG-17

UC ID	UC Name
UCG-17-01	Remediate Device

Category 18: Mitigation Policies: UCG-18

UC ID	UC Name
UCG-18-01	Apply Mitigation Policy on Device
UCG-18-02	Retrieve mitigation policy information
UCG-18-03	Apply network security defense rule
UCG-18-04	Notify of device compromise
UCG-18-05	Compute optimal intrusion response actions
UCG-18-06	Define applicable mitigation actions

Category 19: Parametrization operational parameters: UCG-19

UC ID	UC Name

Cyber-Trust Consortium. All rights reserved.

UCG-19-01	Update baseline traffic statistics
UCG-19-02	Choose data sharing level
UCG-19-03	Change Device configuration
UCG-19-04	Tune the crawling parameters and evaluate existing seeds.

6.2 Use cases inter-relationships

The main actors of the Use Cases are defined in section 2 of this report, they are detailed as primary or secondary actors across the Use Cases in Section 6.3 below. In addition, each Use Case details the inter-relations between the Use Cases so as to provide a meta-picture within each Use Case of the dependencies resulting between the components of Cyber-Trust.

	A01	A02	A03	A04	A05	A06	A07	A08	A09	A10	A11	A12	A13	A14	A15	A16	A17
UCG-01-01			X			X						X					
UCG-01-02			X			X						X		X			
UCG-02-01						X									X		
UCG-02-02						X									X		
UCG-02-03						X									X		
UCG-02-05							X		X								
UCG-03-02															X		
UCG-03-03															X		
UCG-03-04															X		
UCG-04-01								X									X
UCG-04-02													X				
UCG-04-03				X	X				X				X			X	
UCG-05-01	X		X														
UCG-05-02	X	X															
UCG-05-03										X							
UCG-05-04	X																
UCG-05-05						X	X										
UCG-05-06	X		X														
UCG-05-07			X		X	X											
UCG-05-08							X										
UCG-05-09	X																
UCG-06-01			X														
UCG-06-02					X		X										
UCG-06-03	X			X													

Cyber-Trust Consortium. All rights reserved.

	A01	A02	A03	A04	A05	A06	A07	A08	A09	A10	A11	A12	A13	A14	A15	A16	A17
UCG-06-04				X					X								
UCG-06-05							X		X								
UCG-06-06							X			X							
UCG-06-07				X									X				
UCG-07-01	X		X	X								X					
UCG-07-02			X	X		X	X									X	
UCG-07-03		X		X	X							X	X				
UCG-08-01				X													
UCG-08-02								X			X						
UCG-09-01			X	X								X				X	
UCG-09-02			X	X		X						X				X	
UCG-09-03						X	X										
UCG-09-04				X							X						
UCG-10-01			X			X						X					
UCG-10-02									X								X
UCG-10-03	X			X	X												
UCG-10-04					X			X									
UCG-10-05			X	X							X	X					
UCG-10-06						X											
UCG-11-01	X	X	X	X	X	X	X									X	
UCG-11-02	X	X	X	X	X		X									X	
UCG-12-01		X															
UCG-12-02		X															
UCG-12-03	X	X															
UCG-12-04	X	X															
UCG-12-05		X															
UCG-13-01					X			X									
UCG-13-02				X	X			X								X	X
UCG-14-01			X	X		X						X					
UCG-14-02		X	X	X		X						X					
UCG-14-03								X									
UCG-14-04	X	X			X		X									X	
UCG-14-05		X															
UCG-14-06		X															
UCG-14-07							X										
UCG-14-08						X	X		X	X							X

Cyber-Trust Consortium. All rights reserved.

	A01	A02	A03	A04	A05	A06	A07	A08	A09	A10	A11	A12	A13	A14	A15	A16	A17
UCG-15-01							X		X				X				
UCG-15-02	X				X			X					X			X	X
UCG-15-03							X		X				X				
UCG-15-04											X		X				
UCG-16-01					X							X					X
UCG-16-02	X		X	X				X			X	X					
UCG-16-03											X		X				
UCG-16-04				X	X												X
UCG-16-05							X		X	X							
UCG-17-01	X			X								X					
UCG-18-01	X		X	X								X	X			X	
UCG-18-02					X			X									
UCG-18-03		X	X	X							X						
UCG-18-05				X									X				
UCG-18-06									X				X				
UCG-19-01				X							X						
UCG-19-03						X									X		
UCG-19-04									X	X							

6.3 Use case detailed specifications

UCG-01-01: Activate device agent

Name: Activate Device Agent

Description: Device agent [A12] is been activated on the smart device and the user has agreed to the term and services.

Type: Business Use case

Primary Actor: [P2] A Smart Device owner

Supporting/Secondary actors: [P1] A smart home owner, [O2] ISP, [O4] IoT-SP

Stakeholders	Interest
Smart Device Agents [A12]	Activate the installed agent and turn a device to a Cyber-Trust enabled device
Monitoring Service [A03]	Once the agent is activated the monitoring service is activated

Pre-conditions
The smart device owner agrees to the Cyber-Trust terms and conditions

Cyber-Trust Consortium. All rights reserved.

Trigger conditions
Registration of a Cyber-Trust eligible device under a user's profile for active monitoring.

Post-conditions
The network traffic monitoring and device profiling and services run regularly, and all incoming and outgoing traffic undergoes monitoring.

Minimum guarantees
The device should support an OS or the ability to make calls to Cyber-Trust web services.

Frequency of use
Continuous Operation

Non-functional requirements
Usability

Related use cases
UCG-01-02 Deploy Cyber-Trust device agent

Traceability to
Implied Functionality

Example
A Cyber-Trust user has registered a profile to the platform and added a Cyber-Trust eligible device to their profile [A06]. The Cyber-Trust device agent [A12] is deployed on the end device and the user through the portal activates the agent for active monitoring [A03].

Main scenario

Step	Actor	Action description
1	Cyber-Trust User	Registers a user account to the platform
2	System	A user profile has been created
3	Cyber-Trust User	The user registers a Cyber-Trust device to its profile for active monitoring. The user accepts the platforms terms and conditions and advices the deployment of a smart device agent [A12].

Cyber-Trust Consortium. All rights reserved.

4	System	The device information repository processes the device information and checks capabilities for that specific device.
5	System	The system transfers the smart device agent [A12] on the end device and initiates installation.
6	System	The Cyber-Trust system notifies through the UI portal on the installation state of the smart device agent [A12].
7	Cyber-Trust User	The user activates the operation of the smart device agent through the UI portal.
8	System	The Cyber-Trust device level services initiate monitoring [A03] at all supported levels.

UCG-01-02: Deploy Cyber-Trust device agent

Name: Deploy Cyber-Trust device agent

Description: The owner of the device has previously agreed to the terms of use of the Cyber-Trust platform. The device agent [A12] is installed on the device and monitoring [A03] is activated. This use case applies to devices that allow the deployment of new software on its OS

Type: System Use case

Primary Actor: [P2] A Smart Device owner

Supporting/Secondary actors: [P1] A smart home owner, [O2] ISP, [O4] IoT-SP

Stakeholders	Interest
Smart Device owner [P2] Smart Home Owner [P1]	The deployment of the Cyber-Trust device agent is initiated by the Smart Device owner [P2] in acknowledgement of the Smart Home Owner [P1].

Pre-conditions
The device is registered to Cyber-Trust and the smart device owner [P2] agrees to the Cyber-Trust terms and conditions

Trigger conditions
Registration of a Cyber-Trust eligible device under a user’s profile for active monitoring [A03]

Post-conditions
The monitoring service [A03] and device profiling and services are installed and await the activation

Minimum guarantees
The device should support an OS or the ability to make calls to Cyber-Trust web services

Cyber-Trust Consortium. All rights reserved.

Frequency of use
Once

Non-functional requirements
None

Related use cases
UCG-01-01-01 Activate device agent UCG-10-03 Retrieve device profile information

Traceability to
Figure 1.1 - Detailed view of Cyber-Trust project

Example
A Cyber-Trust user has registered a profile to the platform [A06] and added a Cyber-Trust eligible device to their profile for active monitoring [A03]. The Cyber-Trust device agent is deployed on the end device and all relevant services are ready for activation. In the case the end device does not allow for the deployment of the smart device agent [A12] then a software module is setup to manage communication with the end device through web services.

Main scenario

Step	Actor	Action description
1	Cyber-Trust User	Registers a user account to the platform
2	System	A user profile has been created
3	Cyber-Trust User	The user registers a Cyber-Trust device to its profile for active monitoring [A03]. The user accepts the platforms terms and conditions and advices the deployment of a smart device agent [A12]
4	System	The device information repository [A16] processes the device information and checks capabilities for that specific device
5	System	The system transfers the smart device agent [A12] on the end device and initiates installation
6	System	The Cyber-Trust system notifies through the UI portal on the installation state of the smart device agent [A12]

UCG-02-01: Register user into Cyber-Trust platform

Name: Register user into Cyber-Trust platform

Cyber-Trust Consortium. All rights reserved.

Description: Depicts the methodology/steps for a user to register in the platform [A06, A15].

Type: Business use case

Primary Actor: [P1, P2] user

Supporting/Secondary actors: None

Stakeholders	Interest
[P1, P2] user	Register to Cyber-Trust platform in order to enhance their protection against cyber-attacks

Pre-conditions
Smart devices

Trigger
None

Post-conditions
The new user is now listed on the system; The devices are now listed on the system

Minimum guarantees
Web page with a form for the basic info (email, password, etc)

Frequency of use
At least once per user

Related use cases
None

Traceability to
Figure 1.1 - Detailed view of Cyber-Trust project

Example
As a smart home owner (Actor: P1) I want to register to the platform in order to add my devices to the platform [A06].

Main scenario

Cyber-Trust Consortium. All rights reserved.

Step	Actor	Action description
1	Actor: P1/P2	The user connects to the cyber trust web site and go to the register page
2	Actor: P1/P2	Then he fills in the form on the page and click to the validate button
3	System	The system adds the user to the platform after it validates the data given by the user
4	System	The system sends a confirmation email asking the user to confirm its email address and redirect him to a page asking him to do so
5	Actor: P1/P2	The user clicks on the link in the email.
6	System	User is now validated and gets redirected on its profile page

Extension scenarios

After step 2		The information given by the user via the form is incorrect or the user is already registered.
1	System	The system redirects the user to the web page and write a message to help the user to understand what happened.

UCG-02-02: Register organization and people working in the organization into Cyber-Trust platform

Name: Register organization into Cyber-Trust platform

Description: Depicts the methodology/steps for an organization to register in the platform [A06, A15].

Type: Business use case

Primary Actor: [O2] ISP, [O3] Law Enforcement Agency

Supporting/Secondary actors: None

Stakeholders	Interest
ISP [O2]	Register the organization on the platform
The designated administrator regarding the usage of Cyber-Trust Platform [O2]	Register people of the organization on the platform
Law Enforcement Agency [O3]	Register the organization on the platform
The designated administrator regarding the usage of Cyber-Trust Platform [O3]	Register people of the organization on the platform

Pre-conditions
The designated person responsible to sign and validate that the organization desires to be part of the Cyber-Trust platform (e.g. CEO, Chief of Police etc.)

Cyber-Trust Consortium. All rights reserved.

Trigger
None

Post-conditions
The new organization is now listed on the system; The designated administrator/liaison of the organization can create profiles and provide access to people of the organization (also access rights and privileges).

Minimum guarantees
Web page with a form for the respective info

Frequency of use
Once per organization for the organization itself; at least one for the people working for the respective organization.

Related use cases
UCG-02-01 Register user into Cyber-Trust platform
UCG-02-04 Log on to the Cyber-Trust platform

Traceability to
Figure 1.1 - Detailed view of Cyber-Trust project

Example
As the CEO of the organization I have registered my organization to the platform, and I declared the administrator/liaison. As the administrator/liaison (regarding the Cyber-Trust platform) of the ISP (Actor: O2) I receive the registration email (as per UCG-02-01) and I confirm the registration. Then, I want to register people from within my organization to the platform as well as to add its devices to the system [A06].

Main scenario

Step	Actor	Action description
1	Actor: O2	The CEO of the organization registered the organization to the platform through formal procedures, sending the necessary information and documents. One of the information provided through the registration is the designation of the administrator/liaison on behalf of the organization.
2	System	Sends email to the designated administrator/liaison to validate the information provided by the CEO and finalize the his/her registration as the administrator/liaison.

Cyber-Trust Consortium. All rights reserved.

3	Actor: O2	As the administrator/liaison I confirm my personal information and finalize my registration.
4	Actor: O2	The administrator/liaison to the cyber trust web site and log in to the platform in order to register more users under his organization and provide access rights for each one.
5	System	The platform send email to each person to validate the information and finalize their registration
6	Actor: O2	The user connects to the cyber trust web site and log in to the platform
7	Actor: O2	The administrator/liaison registers the devices they want to register under the Cyber-Trust platform.

Extension scenarios

After step 3		**The information given by the user via the form is incorrect.**
1	System	The system redirects the user to the web page and write a message to help the user to understand what happened.

UCG-02-03: Register device (including device class) into Cyber-Trust platform.

Name: Register device (including device class) into Cyber-Trust platform.

Description: Depicts the methodology/steps for an organization to register the devices [A06, A15] along with their class into the platform

Type: Business use case

Primary Actor: [O2] A security officer (Tom) working at an ISP – telecom operator.

Supporting/Secondary actors: System

Stakeholders	**Interest**
Telecom operator [02]	Register its device on the platform
System	Register the new class on the database.

Pre-conditions
A user has already registered itself and his company. This same user is connected to the platform. He is on its company's profile page.

Trigger conditions
A user requests the 'Register a new device page'

Post-conditions

Cyber-Trust Consortium. All rights reserved.

The new device is now listed on the system

Minimum guarantees
Web page with a form for the basic info

Frequency of use
Every time a user requests it.

Related use cases
UCG-02-02, UCG-02-04, UCG-03-01, UCG-03-02, UCG-03-03

Non-functional requirements
User experience.

Traceability to
Figure 1.1 - Detailed view of Cyber-Trust project

Example
As an employee of ISP [O2] I want to register a device [A06] produce by my organization to the platform along with its class and create it if necessary, in order to add refer it inside the Cyber-Trust platform

Main scenario

Step	Actor	Action description
1	Security officer	On his company's page, he clicks 'Register a new device'. He gets redirect to the form page.
2	Security officer	Then he fills in the form on the page and click to the validate button. The new device's classes already exist inside the system.
3	System	The system adds the device to the DLT after it validates the data given by the user. The user is redirected to its company page. Inside the table which list the devices own by the company, the new device appears.
4	System	The system prompts user to check which devices will be monitored from Cyber-Trust.
5	Security officer	The user reads the License Agreement and choose devices Cyber-Trust module will be activated and be protected.
6	System	Cyber-Trust component is activated on selected devices

Cyber-Trust Consortium. All rights reserved.

Extension scenarios

After step 2	Actor	The information given by the user via the form is incorrect.
1	System	The system does not validate the form and write a message under each incorrect field to help the user to understand what happened.

During step 2	Actor	The class of the new device doesn't exist. The user needs to create it.
1	Security officer	The user clicks on 'Create a new class'. A pop-up appears with the fields to fill in order to create a class. He fills in the fields, click and click the validation button.
2	System	The system creates the new class if the data provided in the previous step are correct. Otherwise message appears under the fields incorrectly filled in.

UCG-02-04: Log on to the Cyber-Trust platform.

Name: Log on to the Cyber-Trust platform.

Description: Depicts the methodology/steps for an organization/user to log on the devices along with their class into the platform

Type: Business use case

Primary Actor: [P1, P2] user, [O2] A security officer working at an ISP – telecom operator

Supporting/Secondary actors: System

Stakeholders	Interest
User	Connect to the platform
System	Authorize or not the user to connect to the platform

Pre-conditions
A user has already registered itself. He is on the log on page.

Trigger conditions
A user connects to the log on page.

Post-conditions
The user is logged in.

Cyber-Trust Consortium. All rights reserved.

Minimum guarantees
Web page with a form for public/private key.

Frequency of use
Once per session for each user

Related use cases
UCG-02-01, UCG-03-01, UCG-03-02, UCG-03-03

Non-functional requirements
User experience.

Traceability to
Figure 1.1 - Detailed view of Cyber-Trust project

Example
As an employee of ISP (Actor: O2) I want to log in to the platform in order to access my personal page.

Main scenario

Step	Actor	Action description
1	Security officer	A user connects to the cyber trust web site and go the log on page
2	Security officer	He filled in the form with its personal information.
3	System	The system validates the login query. It redirects the user to its personal page

Extension scenarios

After step 1	Actor	The information given by the user via the form is incorrect or the user is does not exist.
1	System	The system redirects the user to the log on page and writes the following message. 'Incorrect username or password.'

After step 1	Actor	The user forgot its password and click the 'Forgot Password' button

Cyber-Trust Consortium. All rights reserved.

1	System	The system redirects the user to a web page asking him its email address.
2	Security officer	The user provides its email address.
3	System	If a user exists in the database with this email address, the system sends an email to this address with a link.
4	Security officer	The user clicks the link and fills in the form for password registration.
5	System	The user's password is changed.

UCG-02-05: Register to the eVDB sharing service

Name: Register to the eVDB sharing service

Description: The profile of a user is registered into the eVDB [A07, D1, D3, D5].

Type: business use case

Primary Actors: [P1, P2] user, [O2] Security officer working at an ISP – telecom operator, [O1] Cyber-Trust Service Provider CISO, [O1] Vulnerability assessment expert (John), [O2] Security officer working at the SOC of the telecom operator (Sarah), [A09] eVDB Sharing Service

Supporting/Secondary actors: -

Stakeholders	Interest
Intelligent UI user	Register information about user's profile

Pre-conditions
User is logged into the Cyber-Trust system The profile of the users is inserted EVDB is properly populated and validated

Trigger conditions
User request

Post-conditions
The user is registered in the system user database.

Frequency of use
One registration per user. Users may alter their profiles, but this is not expected to happen frequently (most likely less than once per trimester).

Cyber-Trust Consortium. All rights reserved.

Non-functional requirements
None

Related use cases
UCG-06-04 Query and retrieve information from eVDB UCG-14-07 Notify about updates and security-related issues UCG-16-04 Crawl the clear/deep/dark web and update the eVDB UCG-06-05 Review and validate eVDB entries UCG-19-04 Tune the crawling parameters and evaluate existing seeds UCG-06-06 Provide feedback/rating on sources of vulnerabilities UCG-14-08 Match device profile with eVDB contents

Traceability to
Figure 1.1 - Detailed view of Cyber-Trust project

Example
[P1, P2] user [O2] Security officer (Tom) working at an ISP – telecom operator, [O1] Cyber-Trust Service Provider CISO (Bob), [O1] Vulnerability assessment expert (John), [O2] Security officer working at the SOC of the telecom operator (Sarah), may register a profile [D1, D3, D5] to the eVDB [A07].

Main scenario

Step	Actor	Action description
1	User	The user requests to be registered to the service
2	System	The system, depending on a user's role (e.g., smart home owner, security officer, IT expert, vulnerability assessment expert) displays an appropriate registration interface.
3	User	The user completes her profile information and submits it to the system
4	System	The system accepts and validates the given information
5	System	The system creates the new user
6	System	The system displays a success message

Extensions

Cyber-Trust Consortium. All rights reserved.

4a	Actor	**Invalid or incomplete profile data** **Condition: the data provided by the user are invalid or incomplete**
1	System	The system displays an appropriate error message.
2	System	Control is returned to step 3

Variations

1a	Actor	Profile update
1	System	The system may help user and guide users to update their profiles with appropriate UI.

UCG-03-01: Log out from the Cyber-Trust platform

Name: Log out from the Cyber-Trust platform.

Description: Depicts the methodology/steps for an organization/user to log out the devices along with their class into the platform

Type: Business use case

Primary Actor: [P1, P2] user, [O2] A security officer working at an ISP – telecom operator.

Supporting/Secondary actors: System

Stakeholders	Interest
User	Connect to the platform
System	Close the user’s session on the platform

Pre-conditions
A user has already registered itself and is logged to the platform.

Trigger conditions
The user clicks the ‘Log out’ button

Post-conditions
The user is logged out.

Minimum guarantees
A button.

Cyber-Trust Consortium. All rights reserved.

Frequency of use
Once per session for each user

Related use cases
UCG-02-01, UCG-03-01, UCG-03-02, UCG-03-03

Non-functional requirements
User experience.

Traceability to
Figure 1.1 - Detailed view of Cyber-Trust project

Example
As an employee of ISP (Actor: O2) I want to log out of the platform in order to protect the integrity of my account.

Main scenario

Step	Actor	Action
1	security officer	A user is connected to the Cyber-Trust platform. He clicks the 'Log out' button
2	System	The system validates the log out query. It redirects the user to him to the homepage of the product.

UCG-03-02: Unregister User

Name: Unregister User

Description: Depicts the process and steps on how a user can unregister from the platform [A06, A15].

Type: Business use case

Primary Actor: [P1, P2] user, [O2] A security officer (Tom) working at an ISP – telecom operator.

Supporting/Secondary actors: System

Stakeholders	Interest
[P1, P2] user	Delete a profile on the platform.
A security officers	Remove the account of the user based on the information given.

Cyber-Trust Consortium. All rights reserved.

Pre-conditions
A user has already registered itself.

Trigger conditions
A user requests the login page.

Post-conditions
The user deletes his account along with all his personal data.

Minimum guarantees
A web pages

Frequency of use
Occasionally

Related use cases
UCG-02-02, UCG-02-03, UCG-02-04, UCG-03-01, UCG-03-03

Traceability to
Figure 1.1 - Detailed view of Cyber-Trust project

Example
As a user [P1, P2] I want to delete my account in order to delete my personal data and the monitored devices I registered [A06] [A15].

Main scenario

Step	Actor	Action description
1	[P1, P2] user	The actor goes to his personal page. He clicks on 'Manage my account' and then 'Dee melty account'
2	System	Asks the user to give the username password
3	A security officers	The system removes the user from tend he user database.
4	System	User is now deleted completely.

Extension scenarios

After step 1	Actor	The information given by the user via the form is incorrect.

Cyber-Trust Consortium. All rights reserved.

1	System	The system redirects the user to the web page and write a message to help the user to understand what happened. For instance, he should provide valid username and password.

After step 1		**The user's password is too weak**
1	System	The system redirects the user to the log on page ask him to provide a more details in case he has forgot the password.

UCG-03-03: Unregister Organization

Name: Unregister Organization

Description: Depicts the process and steps on how an organization can unregister from the platform [A06, A15].

Type: Business use case

Primary Actor: [O2] A security officer working at an ISP – telecom operator.

Supporting/Secondary actors: System

Stakeholders	Interest
ISP	Get unregistered from the platform
Telecom operator [02]	Get unregistered from the platform
System	Unregister the company inside the platform

Pre-conditions
A user has already registered itself along with its company.

Trigger conditions
A user requests the unregister of an organization page.

Post-conditions
The user deletes his organization along with its personal data.

Minimum guarantees
A web pages

Frequency of use
Occasionally

Cyber-Trust Consortium. All rights reserved.

Related use cases
UCG-02-02, UCG-02-03, UCG-02-04, UCG-03-01, UCG-03-02

Traceability to
Figure 1.1 - Detailed view of Cyber-Trust project

Example
As an employee of ISP (Actor. O2) I want to delete my organization in order to delete its personal data and its devices [A06] [A15].

Main scenario

Step	Actor	Action description
1	[O2] A security officer (Tom) working at an ISP – telecom operator	The actor goes to his organization page. He clicks on 'Manage my organization' and then 'Delete my organization'
2	System	The system deletes the organization of the user along with its devices. The user that has registered device from this company are alerted that their devices are no longer monitored by Cyber-Trust. After that the user is redirected to its personal page.

Extension scenarios

After step 1		The information given by the user via the form is incorrect.
1	System	The system redirects the security officer to the web page and write a message to help the user to understand what happened.

UCG-03-04: Unregister device

Name: Unregister device

Description: Depicts the process and steps on how a user can unregister devices from the platform [A06, A15].

Type: Business use case

Primary Actor: [P1, P2] user.

Supporting/Secondary actors: System

Stakeholders	Interest
[P1, P2] user	Delete device from the platform
System	Unregister the device of the user along with its data from the database.

Cyber-Trust Consortium. All rights reserved.

Pre-conditions
A user has already registered itself along with its devices.

Trigger conditions
Can also be triggered by UCG-03-02 and UCG-12-04

Post-conditions
The user deletes one of her devices along with its personal data.

Minimum guarantees
A web page

Frequency of use
Occasionally

Related use cases
UCG-02-02, UCG-02-03, UCG-02-04, UCG-03-01, UCG-03-02,

Traceability to
Figure 1.1 - Detailed view of Cyber-Trust project

Example
As a user [P1, P2], I want to delete one of my devices in order to delete its personal data[A06][A15] and its monitoring [A03] by the platform.

Main scenario

Step	Actor	Action description
1	[P1, P2] user	The actor goes to his personal page. She goes to her devices list and click to the 'Delete device' button of the device she wants to delete.
2	System	The system deletes the device of the user along with its data. A message is display on the screen to inform the user of the end of the monitoring of her device.

Cyber-Trust Consortium. All rights reserved.

During step 1	Actor	The class of the new device doesn't exist. The user needs to create it.
1	[P1, P2] user	The user clicks on 'Delete device' then a security question appears with the fields to fill in order to delete the device (username and password).
2	System	The system deletes the device of the user along with its data. Otherwise message appears under the fields incorrectly filled in with wrong username and password.

UCG-04-01: Private IoT Device Profile generation

Name: Private IoT Device Profile generation

Description: Implementation of one-way cryptographic hash functions to pseudonymise data and secure multi-party communications for anonymous data distribution.

Type: System

Primary Actor: System

Supporting/Secondary actors: [A17] Profiling Service, [A08] TrustDB Admin Module

Stakeholders	Interest
System	Generates IoT device profile
Profiling Service [A17]	Retrieves the required device information
Trust DB Admin Module [A08]	Stores the generated private device profile

Pre-conditions
The device must be register with the Cyber-Trust

Trigger conditions
New Device is registered

Post-conditions
Profile of IOT Device was generated

Frequency of use
Multiple times per day

Non-functional requirements
None

Cyber-Trust Consortium. All rights reserved.

Related use cases
[UCG-10-01]

Traceability to
Figure 1.1 - Detailed view of Cyber-Trust project

Example
One-way cryptographic hash functions to pseudonymise data and secure multi-party communications for anonymous data distribution.

Main scenario

Step	Actor	Action description
1	System	The system uses profile service to retrieves device status and its operational resource information
2	System	The system performs one-way cryptographic hash operation using hashing algorithms (e.g. SHA 256, SHA512)
3	Trust DB Admin module [A08]	The generated hash digest is stored in the Trust DB Admin Module [A08]

Extension scenarios

After step 1		The device already profiled
1	System	The system checks if the device has been profiled with the Trust DB Admin Module [A08].
2	System	System checks the next device.

UCG-04-02: Characterize asset's importance

Name: Characterize asset's importance

Description: The user ([P1, P2]) prioritizes the attributes of the devices and their services according to her preferences [D3]. This information is vital for the iIRS [A13], because the defense actions to be applied (i.e. which exploits to block and which to leave open so as to ensure availability of network services) have to consider these preferences in order to maximize user's satisfaction. This information is important for the security officer as well for the same reason.

Type: System type

Primary Actor: [P1, P2] user

Supporting/Secondary actors: [O2] Security officer (Sarah), [A13] iris, [A16] Network architecture and assets repository.

Cyber-Trust Consortium. All rights reserved.

Stakeholders	Interest
[P1, P2] user	Define the importance of the various network assets in a personalized fashion.
Security officer [02]	Provide security services by taking into account the user's preferences.

Pre-conditions
Knowledge of the cyber-network structure, configuration and the associated services.

Trigger conditions
Need for security analysis, recommendation of defence strategies, automated defence; change of smart user's preferences.

Post-conditions
The iris builds a utility function that reflects the user's preferences. This utility function is used to make the defence decisions at a later phase.

Frequency of use
Initially before the first time the iris is deployed. Every time the user wants to change the network assets' importance.

Non-functional requirements
None

Related use cases
UCG-18-05 Compute optimal intrusion response actions

Traceability to
Figure 1.1 - Detailed view of Cyber-Trust project

Example
A user, Mary ([P1, P2] user), states her preferences (on network services preferences) [D3] on the relevant Cyber-trust platform. Then, either automatically or by the security officer Sarah ([O2]) a utility function which represents Mary's preferences is built and it is given as input to the iIRS ([A13]). This utility function is critical on the defence actions that the iIRS ([A13]) will decide upon later on.

Cyber-Trust Consortium. All rights reserved.

Main scenario

Step	Actor	Action description
1	[P1, P2] user	The user initiates the process of characterizing her home's assets.
2	System	The system retrieves the Network configuration from the network architecture and assets repository [A16].
3	System	The system displays a user interface for allowing the user to define assets' importance.
4	[P1, P2] user	The user chooses an importance level for each asset (e.g. low/medium/high) or retains the default value (e.g. unknown) through the UI and submits the information to the system.
5	System	The system accepts and validates the owner's preferences.

Extension scenarios

After step 5	Actor	**Update utility function parameters** ***Condition: change in preferences***
1	System	Based on the updated user's preferences, the iIRS's parameters (used in the utility function) are recomputed.
2	System	Stores the new parameters and communicates the updates to the user's iIRS.
3	iIRS	The iIRS receives and stores locally the updated parameters for use in the utility function.

UCG-04-03: Define mitigation actions' impact

Name: Define mitigation actions' impact

Description: The security officer quantifies the impact that the various mitigation actions [A04] have on the availability of the network resources to trusted devices [A05] (e.g. by refusing communication requests, shutting down running services, etc.). This information, along with the smart home user's preferences [D3] is used to define the utility function which is required by the iIRS [A13].

Type: System type

Primary Actor: [O2] Security officer (Sarah)

Supporting/Secondary actors: [A16] Network architecture and assets repository, [A09] eVDB Sharing Service, [A13] iIRS

Stakeholders	Interest
Security officer [02]	More accurate model and as a result better mitigation actions suggested by the iIRS.

Cyber-Trust Consortium. All rights reserved.

Pre-conditions
Knowledge of the network configuration and mitigation actions' impact on the network availability. Knowledge of the cyber-network structure and configuration. Access to the TMS.

Trigger conditions
Need for security analysis, recommendation of defence strategies, automated defence. Change in the number and/or relations of the security conditions; new exploit discovery.

Post-conditions
Definition of the iIRS utility function.

Frequency of use
Initially for the security analysis task. Every time a change in security conditions and/or their relations happens; Every time a new exploit is discovered.

Non-functional requirements
None

Related use cases
UCG-18-05 Compute optimal intrusion response actions UCG-04-02 Characterize asset's importance UCG-18-06 Define applicable mitigation actions

Traceability to
Figure 1.1 - Detailed view of Cyber-Trust project.

Example
The security officer Sarah [O2] consults the cyber-attack graphical security model and quantifies the impact that the mitigation actions [A04] have on network availability [D3]. Then, she builds a utility function for the iIRS [A13], along with the smart home user's preferences, to give as input to the iIRS [A13].

Main scenario

Step	Actor	Action description
1	Security officer	The security officer initiates the process of defining/updating the impact of the applicable mitigation actions.

Cyber-Trust Consortium. All rights reserved.

2	System	The system retrieves the cyber-attack graphical security model.
3	System	The system requests from the Network architecture and assets repository information about the importance level for each asset.
4	Network architecture and assets repository	The Network architecture and assets repository returns the requested information.
5	System	The system displays a user interface for allowing the security officer to define the mitigation actions' impact.
6	Security officer	The security officer quantifies the impact of each mitigation action (e.g. low/medium/high) on the assets.
7	System	The system accepts and validates the security officer's preferences.

Extension scenarios

After step 7	Actor	Update utility function parameters *Condition: change in security model parameters*
1	System	Based on the security officer's input, the iIRS's parameters (used in the utility function) are recomputed.
2	System	Stores the new parameters and communicates the updates to the user's iIRS.
3	iIRS	The iIRS receives and stores locally the updated parameters for use in the utility function.

UCG-05-01: 2D View Systems State

Name: 2DView System State

Description: 2D Visualization [A01] is composed by the a) Operator Monitoring and Control Panel (OMCP) and by User Monitoring Panel (UMP) [A03]. In particular, the OMCP is for the ISP operator and presents the status of the network for real time system control and actuation, while the UMP is basically though for the user [P1, P2] that is interested in a lightweight and intuitive tool to understand what the issue is and how to tackle it.

Type: System Use case

Primary Actor: [O4] IoT-SP

Supporting/Secondary actors: [O2] ISP, [P1] A Smart Home owner

Stakeholders	Interest
Smart home owner [P1] and smart device owner [P2]	interested in a lightweight and intuitive tool to understand what the issue is and how to tackle it

Cyber-Trust Consortium. All rights reserved.

Pre-conditions
Data availability from the network

Trigger conditions
Registration of a Cyber Trust eligible device under a user’s profile for active monitoring.

Post-conditions
The network traffic monitoring and device profiling and services run regularly, and all incoming and outgoing traffic undergoes monitoring.

Frequency of use
Continuous Operation

Non-functional requirements
Usability- Human Factors based design

Related use cases
N.A.

Traceability to
Figure 1.1 - Detailed view of Cyber-Trust project

Example
IOT-ISP operator uses the 2D OMCP to continuously monitor the network status. In case of attack he is able to understand and react in a proper way without being overwhelmed by not useful information and signals.

Main scenario

Step	Actor	Action description
1	IoT-SP operator	Log in into Cyber Trust portal and access to the 2D-OMCP interface for start his/her monitoring session

UCG-05-02: 3D-Virtual Reality View Systems State

Name: 3D-Virtual Reality - View System State

Cyber-Trust Consortium. All rights reserved.

Description: The 3D-VR based View System State is realised by the 3D-VR- Operator Monitoring Environment OME [A03], a tool based on head-mounted display and an aptic device for object manipulation and navigation [A01].

The 3D-VR-OME tool presents the status of the network in a dynamic and immersive way in order to enhance the capability of the operator of having a better understanding of what is happening. The 3D-VR tool allows an in-deep inspection of the network leveraging human senses to represent informative dimensions

Type: System Use case

Primary Actor: [O4] IoT SP

Supporting/Secondary actors: [O2] ISP, System.

Stakeholders	Interest
[O4] IoT-SP and [O2] ISP	Interested in an innovative and more effective tool to understand the situation and inspect more in deep the network condition

Pre-conditions
Data availability from the network status representation

Trigger conditions
IoT ISP Operator decide to start the network monitoring with the 3D-VR-OME

Post-conditions
The network traffic monitoring and device profiling and services run regularly, and all incoming and outgoing traffic undergoes monitoring with 3D-VR-OME

Frequency of use
On trigger base

Non-functional requirements
User experience - Human Factors based design

Related use cases
UCG-05-01

Traceability to
Figure 1.1 - Detailed view of Cyber-Trust project

Cyber-Trust Consortium. All rights reserved.

Example
IOT-ISP operator uses the 3DVR-OME to inspect network status because of the wide diffusion of the attack. The operator is no longer able to understand the extension of issue with the 2D-OMCP tool.

Main scenario

Step	Actor	Action description
1	IoT SP Operator	Wear the head-mounted display and the aptic interface (e.g. a glove)
2	System	The tool retrieves the information from the Cyber Trust. The tools transform numerical variables into visual perception-based features (e.g. colour, dimension)
3	IoT SP Operator	Spatially navigates and visually inspects the situation of the network. Moreover, decides of touch and open some objects (devices) to see their internal status

UCG-05-03: Visualise summary of eVDB contents matching an operator’s devices

Name: Visualize summary of eVDB contents matching an operator’s devices.

Description: The interface provides a search tool to where the [P1, P2] user can perform a search and discovery action of the vulnerability on the base of the device description. The result will be displayed in a tabular form and include the result of the deep/dark web processing [A10].

Type: System Use case

Primary Actor: [O4] IoT-SP, [P1] Smart Home Owner, [P2] A smart device owner, [O3] LEA.

Supporting/Secondary actors: [P1] Smart Home Owner, [O2] ISP, [O6] Smart Device Manufacturer, [P2] A Smart Device owner, System.

Stakeholders	Interest
[O4] IoT-SP and [O2] ISP	Interests in access to vulnerabilities to prevent and mitigate attacks
[P1] A Smart Home Owner, [P2] A Smart Device owner	Interest in assessing before the installation or purchase which are the vulnerabilities for a specific product
[O6] Smart Device Manufacturer	Interest in understanding which are the vulnerabilities of its products and similar ones in order to release bug/vulnerability fix for the device in due time.

Pre-conditions
eVDB filled out with the information retrieved by deep/dark web about vulnerabilities and exploitations e.g. 0-day.

Cyber-Trust Consortium. All rights reserved.

Trigger conditions
Each time that a device is selected in the 2D-MCP and each time user (whoever he is)

Post-conditions
The vulnerability information is displayed on the 2D-MCP and on the search engine web page result

Frequency of use
Continuous Operation

Non-functional requirements
Usability

Related use cases
UCG-05-01 2D View System State

Traceability to
Figure 1.1 - Detailed view of Cyber-Trust project

Example
A Cyber Trust user can access to the information about the vulnerability of a devices through the Cyber Trust web portal after he is logged in. The user provides some data related to the device (e.g. firmware version, brand, type, etc.) and then receives back all the information retrieved from the deep/dark web [A10].

Main scenario

Step	**Actor**	**Action description**
1	[P1,P2], O3	Log in the Cyber Trust portal and access the eVDB search interface in order to discover vulnerabilities information about a specific device
2	System	The query is performed on the eVDB with specific criteria and keywords as firmware version, brand, type and displayed in a tabular form on the webpage.
3	[P1,P2], O3	The user orders the results in case they are more than one and analyses the data in order to find the exact match between what is looking for the results. In case the results are too much, the use decides to refine the search adding more criteria.

Cyber-Trust Consortium. All rights reserved.

UCG-05-04: Visualize network’s health status

Name: Visualize network's health status

Description: The network health will be displayed through 2D-OMCP, 2D-UMP and 3D-VR-OMCE (Oracle Mobile Cloud Enterprise) tools. In particular on 2D-OMCP the information will be presented through widget-like and correlated data visualization [A01] methods (e.g. trend chart, timelines, etc.).

In 3D instead will be used perceptive-based clues and affordance (basically colours, object dimensions, object distance, motion) to represent the relevant dimensions to evaluate the health of the IoT network

Type: System Use case

Primary Actor: [O4] IoT SP, [P1] A Smart Home Owner

Supporting/Secondary actors: [O2] ISP, [O4] IoT SP, [P2] A Smart Device owner

Stakeholders	Interest
[O4] IoT SP, [P1] A Smart Home Owner	Interest in a fast and perceptive based assessment of the network health in order to react timely

Pre-conditions
Available information on the network

Trigger conditions
[P1, P2] user requests information on the Cyber Trust website about the status of the home system through the 2D-UMP O4 IoT SP Operator requests information about the home system when selected on the 2D-OMCP or 3D-VR-OMCE

Post-conditions
The information about the health status of the smart home system is displayed on the 2D-OMCP, 2D-UMP and 3D-VR-OMCE

Frequency of use
Dependant on the trigger

Non-functional requirements
User Experience

Related use cases

Cyber-Trust Consortium. All rights reserved.

UCG-05-01 2D View System State

Traceability to
Figure 1.1 - Detailed view of Cyber-Trust project

Example
Cyber Trust operator wants to have a general idea of the healt status of the network of the Smart Home devices [A01]. The operator wears a head mounted display and the haptic glove to navigate with the 3D-VR-OMCE tool. The operator can spatially navigate in the network thorough an immersive experience and can have a perceptive-based overview of the network health provided with visual signals [A01] as node colours (colour code), node dimensions, etc. The operator can inspect the network even if it is complex and extended and to have a genral overview, he/she can have an eagle-eye view zooming out the network representation and spatially clustering the nodes, so that the health status is possible to be accessed with colour's density and extension.

Main scenario

Step	Actor	Action description
1	IoT SP Operator	The user Wear the head-mounted display and the haptic glove of the 3D-VR-OMCE tool where is displayed the network with specific perceptive-based elements to better orient the use in the virtual environment.
2	IoT SP Operator	The user navigates the virtual environment with body movement and hand gesture performed with the haptic device. The user decides to have an eagle-eye view of a part of the network in order to have a comprehensive understanding of the status simply visually assessing color's density of the node clusters generated by the low-level of zoom.

UCG-05-05: Visualize device vulnerability levels

Name: Visualise device vulnerability levels

Description: in the 2D OMCP is also represented the level of vulnerability of the devices targeted [A01].

Type: System Use case

Primary Actor: [O4] IoT SP, [P2] A Smart Device owner

Supporting/Secondary actors: [P1] A Smart Home Owner, [O2] ISP, [O6] Smart Device Manufacturer, [O4] IoT SP.

Stakeholders	Interest

Cyber-Trust Consortium. All rights reserved.

[O4] IoT SP, [P2] A Smart Device owner	Interest in understanding the level of vulnerability of the device owned or managed in the network in order to undertake the appropriate actions

Pre-conditions
Available information on the network

Trigger conditions
O4 IoT SP Operator requests information about the device level vulnerability present in the

Post-conditions
Device vulnerability shown

Frequency of use
Dependant on the trigger

Non-functional requirements
Usability

Related use cases
UCG-05-01 2D View System State

Traceability to
Figure 1.1 - Detailed view of Cyber-Trust project

Example
The IoT ISP Operator wants to know which the level of vulnerability of the new Smart Home systems is connected to the Cyber Trust in order to estimate the potential risks brought by the new comers/clients. The operator filters the Smart Home systems with a registration [A06] date of today and yesterday on the 2D-OMCP. The list is then presented. The operator clicks on a device and obtains the current vulnerability level and the list of the vulnerabilities retrieved from the eVDB [A07]

Main scenario

Step	Actor	Action description
1	IoT SP Operator	Log in the Cyber-Trust Platform and access to the 2D-OMCP

Cyber-Trust Consortium. All rights reserved.

2	IoT SP Operator	Filter the smart home systems on the base of data registration
3	IoT SP Operator	Click on a device belongs to a smart home system filtered and obtain the current vulnerability level with the list of the vulnerabilities retrieved from the eVDB

UCG-05-06: Visualize network traffic

Name: Visualise device trust levels

Description: the network traffic will be displayed on the 2D MCP [A01] with several widgets able to represent the traffic flow dynamics.

Type: System Use case

Primary Actor: [O4] IoT SP

Supporting/Secondary actors: [O2] ISP, [O4] IoT SP, System

Stakeholders	Interest
[O4] IoT SP, [O2] ISP	Interest in visualizing the network traffic for detecting anomalies

Pre-conditions
Available information on the entire network

Trigger conditions
Information continuously updated and presented in the 2D-OMCP and in 3D-VR-OMCE

Post-conditions
Visualization of the information on the 2D-OMCP and in 3D-VR-OMCE

Frequency of use
Real time

Non-functional requirements
Usability – understandability of the data visualization solution

Related use cases
UCG-05-01 2D View System State

Cyber-Trust Consortium. All rights reserved.

Traceability to
Figure 1.1 - Detailed view of Cyber-Trust project

Example
The IoT ISP Operator needs to monitor in real time the status of the network or part of it [A03]. The information related to the traffic flows is presented in a dedicated widget (trend-like view) and continuously updated in the 2D-OMCP. In particular is displayed the last 3 hours by default, but thanks to a slider representing the timeline, it is possible to change the time window displayed up to days. In this way the operator can visually explore [A01] if there were some anomaly or recurrent picks in a longer period.

Main scenario

Step	Actor	Action description
1	[O4] IoT SP Operator	Log in the Cyber Trust Platform and access to the 2D-OMCP
2	[O4] IoT SP Operator	Visually inspect the widget that display the network traffic flow in real time with a time widow of 3 hours
3	[O4] IoT SP Operator	The operator decides to move the timeline slider back in order to have a day view.
4	System	The UI backend change the periodic query parameters in order to obtain the right time slot for the database and represent it on the widget

UCG-05-07: Visualize device trust level

Name: Visualise device trust levels

Description: In the 2D OMCP is also represented the level of trust of the devices targeted [A05].

Type: System Use case

Primary Actor: [O4] IoT SP, [P1] A smart home owner, [P2] A smart device owner

Supporting/Secondary actors: [P1] Smart Home Owner, [O2] ISP, System

Stakeholders	Interest
[P1, P2] user	Visualise the trust level of the devices connected to the smart home system
IoT SP Operator [04]	Visualise the trust level of the devices in the context of the network

Pre-conditions

Cyber-Trust Consortium. All rights reserved.

Available information on the network

Trigger conditions
A user requests information on the Cyber Trust website about the status of the home system through the 2D-UMP [O4] IoT SP Operator requests information about the home system when selected on the 2D-OMCP or 3D-VR-OMCE

Post-conditions
Device Trust level visualised

Frequency of use
Dependant on the trigger

Non-functional requirements
Usability

Related use cases
UCG-05-01 2D View System State

Traceability to
Figure 1.1 - Detailed view of Cyber-Trust project

Example
The user [P1,P2] wants to see the level of trust [A05] of the devices connected to its system since he is hosting a party at home and a number of new devices starts to be monitored by Cyber Trust service [A03]. After the login, the user [P1,P2] goes to its profile on the Cyber Trust portal and lists the devices connected to his registered smart home gateway [A06]. He is able to verify that one of them has assigned a quite low score [A05] and decide to keep the automatic remediation enabled.

Main scenario

Step	Actor	Action description
1	[P1, P2] A smart home owner, A smart device owner	New external devices are connected to the smart home gateway
2	System	Cyber Trust service start the monitoring of the new devices

Cyber-Trust Consortium. All rights reserved.

3	[P1, P2] A smart home owner, A smart device owner	Login Cyber Trust portal and goes to its profile where his gateway device and list all the devices currently connected to the gateway are displayed. The Trust Level and if the devices are monitored by Cyber Trust or not are information represented in the tabular-like interface

UCG-05-08: Visualize known and zero-day vulnerabilities

Name: Visualize known and zero-day vulnerabilities

Description: The user can obtain from the vulnerability search interface of the eVDB ([A07]) (MISP) the list of known, zero-day, etc. vulnerabilities retrieved using different classification criteria assigned during the deep/dark web processing.

Type: System Use case

Primary Actor: [O4] IoT SP,

Supporting/Secondary actors: [P1, P2] user, [O2] ISP, [O4] IoT-SP, System.

Stakeholders	Interest
[O4] IoT SP, [P1] A Smart Home Owner	Interest in obtaining information about the device vulnerability

Pre-conditions
Available information on the network

Trigger conditions
A user requests information on the Cyber Trust website about the status of the home system through the 2D-UMP O4 IoT SP Operator requests information about the home system when selected on the 2D-OMCP or 3D-VR-OMCE

Post-conditions
Zero-day vulnerabilities information provided to the user

Frequency of use
Dependant on the trigger

Non-functional requirements

Cyber-Trust Consortium. All rights reserved.

Usability

Related use cases
UCG-05-01 2D View System State

Traceability to
Figure 1.1 - Detailed view of Cyber-Trust project

Example
The IoT ISP Operator wants to understand which the 0-day vulnerability are associated to a specific class of devices that are part of the Smart Home Systems managed. He logs in the Cyber Trust portal and goes on the eVDB [A07] search interface. He provides the name of the devices and the version of the firmware installed and retrieves the list of the 0-day vulnerabilities.

Main scenario

Step	Actor	Action description
1	IoT SP	Logs in the Cyber Trust portal
2	IoT SP	Provide the information related to the name of the device and the version of the firmware installed in the eVDB search interface
3	System	The system performs a SQL-like query in the VBD (MISP), retrieves the information and present the results with a tabular-like layout on the web

UCG-05-09: Visualize historical (heterogeneous) data

Name: Visualize historical heterogeneous data

Description: the 2D-OMCP allows the ISP operator defining a time slot in the past and see what happened. This 2D-OMCP Time Machine functionality is a different but full-interactive 2D-OMCP where the information that was displayed on the OMCP in the time slot selected, is time-dependently represented. In fact, the Operator with a UI slider has the possibility to move back and forth in time to check carefully that was the information but also the actions applied by the operator in that moment. The interface allows interaction with the past but not changes. Moreover, the Operator can open a number of 2D-OMCP Time Machine instances with different time slots simultaneously to perform a parallel visual inspection [A01] of the differences.

Type: System Use case

Primary Actor: [O4] IoT SP

Supporting/Secondary actors: [O2] ISP, system

Cyber-Trust Consortium. All rights reserved.

Stakeholders	Interest
[O4] IoT SP, [O2] ISP	Interest in analysing past events and assessing operator behaviours

Pre-conditions
Available historical data of the network and operator behaviours/actions

Trigger conditions
O4 IoT SP Operator open 2D-OMCP-TM functionality

Post-conditions
The past information is re-presented in the 2D-OMCP Time Machine according to the time selection and within the time slot

Frequency of use
Dependant on the trigger

Non-functional requirements
Usability

Related use cases
UCG-05-01 2D View System State

Traceability to
Figure 1.1 - Detailed view of Cyber-Trust project

Example
A Cyber-Trust Operator wants to understand what happened one day and two days ago at the same time period: 11.00 – 13.00 because of similar attacks occurred. Moreover, he would like to understand and compare how the operators behaved, what actions were taken and when. The functionality retrieves the information according to the time slot defined and presents the data on the 2D-OMCP-TM instance. The interface allows multiple instances of 2D-OMCP-TM so that is possible to perform multiple comparisons. The 2D-OMCP-TM is a full interactive 2D-OMCP where is possible to query and obtain all kind of info in 'read-only' mode from the past.

Main scenario

Cyber-Trust Consortium. All rights reserved.

Step	Actor	Action description
1	[O4] IoT SP Operator	An Operator through the 2D-OMCP interface opens the 2D-OMCP-TM functionality and select a time period of interest
2	System	The 2D-OMCP-TM retrieve all the information for the Cyber Trust storage with a time-dependent query
3	System	The 2D-OMCP-TM save in local database the requested data and presents the information on the interface starting for the t0 of the time slot selected
4	[O4] IoT SPOperator	The Operator moves the slider back and forth in order to see how the information changed that the dime considered.
5	[O4] IoT SP Operator	The Operator selects also some devices from the 2D-OMCP-TM interface to see what their status at that time was.
6	[O4] IoT SP Operator	Once the inspection is concluded the 2D-OMCP-TM functionality is closed.

UCG-06-01: Raise alert for security officer

Name: Raise alert for security officer

Description: this case study is to raise an alert to intelligent UI user when for example, there is a mitigation policy to be applied as a response to a threat originated from IoT device.

Type: System

Primary Actor: Monitoring Service [A03]

Supporting/Secondary actors: Security officer [O2]

Stakeholders	Interest
System	Send an alert to intelligent UI user
Security officer	Receives the alert sent by the system

Pre-conditions
Mitigation policy database is consulted.

Trigger conditions
Device risk level is changed

Post-conditions
An alert is sent to the Security officer

Cyber-Trust Consortium. All rights reserved.

Frequency of use
Multiple times per day

Non-functional requirements

Related use cases
[UCG-18-02]

Traceability to
None

Example
A security officer [O2] working in the control room as a telecom operator [O4], has been alerted about suspicious behaviour in the provider's infrastructure.

Main scenario

Step	Actor	Action description
1	System	The risk level related to the current status of the device is changed as a result of threat
2	System	The system retrieves threat information from T6.3 and device profile from device profile module
3	System	The System sends an alert to the corresponding security officer with the details of the device risk level, profile information and policy specifications retrieved from mitigation policy database.
4	Security officer	Security officer receives the threat and policy information along with device profile.

Extension scenarios

After step 4	Actor	The applicable mitigation actions
1	Security officer	The security officer starts the process of defining/updating the impact of the applicable mitigation actions

UCG-06-02: Raise alert for device owner

Name: Raise alert for device owner

Cyber-Trust Consortium. All rights reserved.

Description: This use case study is to raise an alert to the [P1, P2] user when for example, there is a threat is detected in one of the owners' s IoT devices.

Type: System

Primary Actor: System

Supporting/Secondary actors: Security officer working at a telecom operator [O2]

Stakeholders	Interest
System	Send an alert to intelligent UI user
[P1, P2] user	Receives the alert sent by the system

Pre-conditions
Mitigation policy database is detected, and a mitigation policy is applied

Trigger conditions
Device risk level is changed

Post-conditions
An alert is sent to device owner [P2]

Frequency of use
Multiple times per day

Non-functional requirements
None

Related use cases
[UCG-14-03]

Traceability to
None

Example
A technology-aware person [P2], has bought a new device. The person has registered the device to the Cyber-Trust platform [A06]. As the eVDB [A07] has been recently been updated and newly added vulnerabilities from the eVDB [A07] and identifies that a new vulnerability has been discovered for this

Cyber-Trust Consortium. All rights reserved.

device which can be exploited to install malware on it. The TMS reduces the device trust level [A05] from 0.8 to 0.3. The risk level related to the current status of the device is increased from 0.1 to 0.6. The mitigation policy database is consulted [UCG-18-02] and an alert is sent to the technology-aware person [deP2, UCG-06-02] detailing the that IP device vulnerable, and the type action was taken to secure the device/network.

Main scenario

Step	Actor	Action description
1	System	The risk level related to the current status of the device is changed as a result of threat
2	System	The system retrieves threat information from T6.3 and device profile from device profile module
3	System	The System sends an alert to the device owner with the details of the device risk level, profile information and policy specifications retrieved from mitigation policy database.
4	[P1, P2] user	The user receives the issued alert

Extension scenarios

After step 4	Actor	Device owner responding
1	Device owner	The device owner will respond that the device is legitimately reactivated (temporarily or permanently); otherwise the activity is owing to an identity theft attack

UCG-06-03: Establish baseline traffic statistics

Name: Establish baseline traffic statistics

Description: Traffic statistics of the network will be displayed on the 2D Monitoring [A03] and Control Panel (MCP) [A01] in order to allow ISP operator [O2] in being aware about the situation.

Type: System

Primary Actor: [A03] Monitoring Service

Supporting/Secondary actors: System

Stakeholders	Interest
System	Manage the traffic via the network
[A03] Monitoring Service	analyses and tracks inbound and outbound packets

Pre-conditions
Packet Sniffer has been installed

Cyber-Trust Consortium. All rights reserved.

Trigger conditions
Network traffic

Post-conditions
The baseline has been established

Minimum guarantees
None

Frequency of use
Multiple times per minute

Non-functional requirements
None

Related use cases
None

Traceability to
None

Example
Traffic statistics will be visualised through chart and through graph representation [A01] where possible. Traffic dynamics will be also represented in the 3D virtual reality mode in order to verify the actual capability of such a technology of enhancing the operator's situation awareness and response capacity.

Main scenario

Step	Actor	Action description
1	System	The system will check each packet passing through network
2	System	The system uses Packet Sniffer to capture the entire stream of network data.
3	Monitoring Service	Monitoring Service uses a network probe to capture raw packet data.

Cyber-Trust Consortium. All rights reserved.

4	System	System checks what the users are actually doing on the network.
5	Monitoring Service	Monitoring Service determines users and the specific applications that consume the most bandwidth within the network.
6	System	The system creates the baseline traffic statistics

Extension scenarios

After step 3	Actor	If the captured traffic belongs to new device
1	System	The system creates new profile to store the gathered stats.
2	System	The System checks match any followed stats with the newly created profile.

UCG-06-04: Query and retrieve information from eVDB

Name: Query and retrieve information from eVDB

Description: Users search and retrieve for any security issues and intelligence that pertain to devices [D5, D6]

Type: business use case

Primary Actors: [P1, P2] user, [O2] Security officer (Tom) working at an ISP – telecom operator, [O1] Cyber-Trust Service Provider CISO (Bob), [O1] Vulnerability assessment expert (John), [O2] Security officer working at the SOC of the telecom operator (Sarah), [A09] eVDB Sharing Service

Supporting/Secondary actors: -

Stakeholders	Interest
Intelligent UI user	Query and retrieve information

Pre-conditions
User is logged into the Cyber-Trust system EVDB is properly populated and validated

Trigger conditions
User request

Post-conditions
None

Cyber-Trust Consortium. All rights reserved.

Frequency of use
Thousand times per day

Non-functional requirements
None

Related use cases
UCG-02-05 Register to the eVDB sharing service UCG-14-07 Notify about updates and security-related issues UCG-16-04 Crawl the clear/deep/dark web and update the eVDB UCG-06-05 Review and validate eVDB entries UCG-19-04 Tune the crawling parameters and evaluate existing seeds UCG-06-06: Provide feedback/rating on sources of vulnerabilities UCG-14-08: Match device profile with eVDB contents

Traceability to
Figure 1.1 - Detailed view of Cyber-Trust project

Example
[P1, P2] user [O2] Security officer (Tom) working at an ISP – telecom operator, [O1] Cyber-Trust Service Provider CISO (Bob), [O1] Vulnerability assessment expert (John), [O2] Security officer working at the SOC of the telecom operator (Sarah), may use [D5, D6] Cyber-Trust’s eVDB ([A09]) (a) to search for any security issues that pertain their device (b) to search for and uncover possible attacks [UCG-02-05], (c) to query for similar behavioral patterns in the hope to learn more about attack types that produce this type behavior and to identify in advance possible solutions (d) to query for relevant intelligence (e.g., similar threats, rule updates, identified signatures, or mitigation strategies [A04])

Main scenario

Step	Actor	Action description
1	User	The user requests to submit a query to the eVDB
2	System	The system, depending on the status of a user (e.g., smart home owner, security officer, IT expert, vulnerability

Cyber-Trust Consortium. All rights reserved.

		assessment expert) creates and displays the appropriate query interface.
3	User	The user fills in the query and requests its execution
4	System	The system validates the query
5	System	The system computes the answer to the query by searching the eVDB.
6	System	The system returns the answer to the user.

Extensions

4a	Actor	**Invalid query** **Condition: The query entered by the user is invalid**
1	System	The system displays an appropriate error message
2	System	Processing of the query terminates

UCG-06-05: Review and validate eVDB entries

Name: Review and validate eVDB entries

Description: The vulnerability assessment expert examines and assesses newly discovered cyber-threats, reviews the new vulnerabilities that were surfaced by Cyber-Trust and decides if there exists enough evidence to update the report confidence (RC) field of the discovered vulnerabilities [D6].

Type: business use case

Primary Actor: [O1] A vulnerability assessment expert (John).

Supporting/Secondary actors: [A09] eVDB Sharing Service

Stakeholders	Interest
Vulnerability assessment expert [01]	Keep the contents of the eVDB updated regarding the confidence in the existence of the new vulnerabilities accurate
Infrastructure owner	Protect registered devices through reliable and up-to-date cyber-threat intelligence

Pre-conditions
Vulnerability assessment expert is logged into the Cyber-Trust system

Trigger conditions
Periodically

Post-conditions

Cyber-Trust Consortium. All rights reserved.

eVDB has been updated to reflect the true confidence levels of newly discovered vulnerabilities.

Frequency of use
A few times per week

Non-functional requirements
None

Related use cases
UCG-06-04 Query and retrieve information from eVDB UCG-14-07 Notify about updates and security-related issues UCG-16-04 Crawl the clear/deep/dark web and update the eVDB UCG-19-04 Tune the crawling parameters and evaluate existing seeds UCG-06-06 Provide feedback/rating on sources of vulnerabilities UCG-14-08 Match device profile with eVDB contents

Traceability to
Figure 1.1 - Detailed view of Cyber-Trust project

Example
While on operation, the Cyber-Threat discovery module has surfaced last week information about a new zero-day vulnerability and has inserted it into the eVDB ([A07], [D6]) with a low confidence level. John, a vulnerability assessment expert ([O1]) is examining and assessing newly discovered cyber-threats; over the last few days he has been reviewing the new vulnerabilities that were surfaced by Cyber-Trust. He now decides that there exists enough evidence to update in the eVDB the *report confidence* (RC) field of the vulnerability that was discovered last week from “not defined” to “reasonable”. He uses and appropriate UI to search for the eVDB record of the vulnerability and perform the update accordingly.

Main scenario

Step	Actor	Action description
1	Vulnerability assessment expert	The vulnerability assessment expert selects the “Review and curate vulnerabilities” functionality.
2	System	The system presents a form to allow the vulnerability assessment expert to enter search criteria.
3	Vulnerability assessment expert	The vulnerability assessment expert enters the search criteria (such as new vulnerabilities or vulnerabilities with report confidence score set to “Not defined”) and submits the form.

Cyber-Trust Consortium. All rights reserved.

4	System	The system retrieves from the eVDB a list of vulnerability records that match the criteria.
5	System	The system presents the list of vulnerability records that match the specified criteria to the vulnerability assessment expert.
6	Vulnerability assessment expert	The vulnerability assessment expert selects the vulnerability to be assessed and submits this information.
7	System	The system presents a detailed record of the vulnerability and appropriate controls to facilitate the assessment and/or edit the vulnerability information according to the expert's assessment.
8	Vulnerability assessment expert	The vulnerability assessment expert chooses the desired update; additional information may be entered to document the reason/rationale/source for the update.
9	Vulnerability assessment expert	The vulnerability assessment expert submits the information.
10	System	The system validates the completeness and validity of the information.
11	System	The system updates vulnerability information in the eVDB.
13	System	The system informs the vulnerability assessment expert that the update has been performed.

Extension scenarios

4a	Actor	No vulnerability matches the criteria
1	System	The system notifies the vulnerability assessment expert that no vulnerabilities were retrieved
2	System	Control returns to step #2

9a	Actor	The information submitted by the user is incomplete/erroneous
1	System	The system informs the vulnerability assessment expert regarding the errors or omissions
2	System	Control returns to step #7

*a	Actor	The IT expert cancels the process (at any step)
1	Vulnerability assessment expert	The vulnerability assessment expert cancels the process

Cyber-Trust Consortium. All rights reserved.

2	System	The system terminates the procedure and destroys the form.

UCG-06-06: Provide feedback/rating on sources of vulnerabilities.

Name: Provide feedback/rating on sources of vulnerabilities.

Description: A vulnerability assessment expert provides feedback on the quality of the information gathered from the crawling of new seeds [A10, D6]. He also approves and annotates approved seeds for usage by the crawl module.

Type: business use case

Primary Actor: [O1] A vulnerability assessment expert (John)

Supporting/Secondary actors: -

Stakeholders	Interest
Vulnerability assessment expert [01]	Ensure that Cyber-Trust monitors credible and information-rich sources
Infrastructure owner	Protect registered devices through reliable and up-to-date cyber-threat intelligence

Pre-conditions
Vulnerability assessment expert is logged into the Cyber-Trust system

Trigger conditions
Periodically

Post-conditions
New seeds have been added, approved and annotated. Existing seeds have been evaluated.

Frequency of use
A few times per month

Non-functional requirements
None

Related use cases
UCG-16-04 Crawl the clear/deep/dark web and update the eVDB

Cyber-Trust Consortium. All rights reserved.

UCG-19-04 Tune the crawling parameters and evaluate existing seeds

Traceability to
Figure 1.1 - Detailed view of Cyber-Trust project

Example
The cyber-threat discovery module has crawled ([A10, D6]) a number of new sites this month and has surfaced a variety of new cyber-threat intelligence. John, a vulnerability assessment expert ([O1]) uses an appropriate UI to access the new cyber-threat intelligence that was discovered from these sites --and is stored in the eVDB [A07, D6] and inspects them to assess the for credibility and the quality of the identified intelligence; the UI provides anonymized/aggregated information without links to particular individuals. Some of the new seeds have indeed provided a number of useful cyber-threat intelligence regarding new vulnerabilities and information about existing ones, while others contain repetitive and/or outdated information. He then proceeds to providing an appropriate rating for each one of the sources alongside textual feedback that briefly explain the rationale behind each individual the rating.

Main scenario

Step	Actor	Action description
1	Vulnerability assessment expert	The vulnerability assessment expert selects the “Rate seeds” functionality.
2	System	The system presents a form to allow the vulnerability assessment expert to enter seed search criteria.
3	Vulnerability assessment expert	The vulnerability assessment expert enters the search criteria (such as new or unrated seeds) and submits the form.
4	System	The system retrieves the list of seeds that match the criteria.
5	System	The system presents the list of seeds that match the specified criteria to the vulnerability assessment expert.
6	Vulnerability assessment expert	The vulnerability assessment expert selects the seed to be assessed and submits this information.
7	System	The system presents a detailed record of the seed that includes high-level seed features (such as top-ranked terms/tags, recently extracted text snippets, annotations) alongside appropriate controls to facilitate the seed assessment or further examine the seed (regarding vulnerabilities that were discovered from it).
8	Vulnerability assessment expert	The vulnerability assessment expert chooses the desired seed rating update; additional information

Cyber-Trust Consortium. All rights reserved.

		may be entered to document the reason/rationale/source for the update.
9	Vulnerability assessment expert	The vulnerability assessment expert submits the information.
10	System	The system validates the completeness and validity of the information.
11	System	The system updates the seed information.
13	System	The system informs the vulnerability assessment expert that the update has been performed.

Extension scenarios

4a	Actor	No seed matches the criteria
1	System	The system notifies the vulnerability assessment expert that no seeds were retrieved
2	System	Control returns to step #2

8a	Actor	The user decides to further examine the available seed information
1	Vulnerability assessment expert	The vulnerability assessment expert chooses to further examine the seed; he selects the “View identified vulnerabilities” functionality for a specific seed.
2	System	The system retrieves from the eVDB a list of vulnerability records.
3	System	The system presents the list of vulnerability records that were retrieved to the vulnerability assessment expert.
4	Vulnerability assessment expert	The vulnerability assessment expert selects to review the information about a specific vulnerability.
5	System	The system presents a detailed record of the vulnerability.
6	Vulnerability assessment expert	The vulnerability assessment expert closes the vulnerability information windows.
7	System	Control returns to step #7

9a	Actor	The information submitted by the user is incomplete/erroneous
1	System	The system informs the vulnerability assessment expert regarding the errors or omissions

Cyber-Trust Consortium. All rights reserved.

2	System	Control returns to step #7

*a	Actor	The IT expert cancels the process (at any step)
1	Vulnerability assessment expert	The vulnerability assessment expert cancels the process
2	System	The system terminates the procedure and destroys the form.

UCG-06-07: Communicate iIRS actions to the security officer

Name: Communicate iIRS actions to the security officer.

Description: The iIRS [A13] after computing the optimal defense action ([A04]), it informs the Security officer.

Type: system type

Primary Actor: [A13] iIRS

Supporting/Secondary actors: [O2] Security officer (Sarah)

Stakeholders	Interest
Security officer [02]	Knowledge about system defensive actions taken.

Pre-conditions
Operating iIRS.

Trigger conditions
Security officer request; Defence action decided by the iIRS.

Post-conditions
The security officer is informed about the iIRS activity.

Frequency of use
Periodically (at a rate predefined by the security officer). Upon request by the security officer.

Non-functional requirements
None

Related use cases

Cyber-Trust Consortium. All rights reserved.

UCG-18-05 Compute optimal intrusion response actions

Traceability to
Figure 1.1 - Detailed view of Cyber-Trust project.

Example
Security officer Sarah ([O2]) configures the iIRS ([A13]) so that it informs her about every defence action applied by the iIRS ([A13]) or about specific defence actions, for example about the most critical ones. Then, every time the iIRS ([A13]) applies such actions, Sarah ([O2]) is informed about it.

Main scenario

Step	Actor	Action description
1	iIRS [A13]	Logs the best defense action having been decided.
2	iIRS [A13]	A notification is sent to the security officer to inform her about the defense action.
3	Security officer	Views the defense action.
4	Security officer	Closes the notification and updates the local log file.

Extension scenarios

2a	Actor	Batch notification of the security officer Condition: The security officer requires notifications to be sent meeting certain criteria.
1	iIRS [A13]	Recent actions are filtered according to criteria.
2	iIRS [A13]	The set of notifications selected is sent to the security officer to inform her about the defense actions.
3	System	control goes to step #3

Extension scenarios

3a	Actor	Configuration by the security officer Condition: The security officer configures criteria that notifications should meet.
1	Security officer	Views the defense actions.
2	Security officer	Configures the frequency and under which circumstances the iIRS informs her about the defense actions.
3	System	control goes to step #4

Cyber-Trust Consortium. All rights reserved.

UCG-07-01: Check device patching status

Name: Check device patching status

Description: Intelligence regarding the latest versions of firmware is stored in the Cyber-Trust backend system. Periodically, the installed firmware and software on monitored devices [A03] is checked and when outdated the end user is notified.

Type: System Use case

Primary Actor: [P2] A Smart Device owner

Supporting/Secondary actors: [P1] Smart Home Owner, [O2] ISP, [O4] IoT SP, [O6] Smart Device Manufacturer

Stakeholders	Interest
Cyber-defense Service [A04]	Detection of suspicious content triggers backend services for threat detection and mitigation.
Smart Device Agents [A12]	The smart device agent [A12] is responsible for the monitoring of device related aspects.

Pre-conditions
Available information on current patching status and updates need to be available by the manufacturer or firmware provider.

Trigger conditions
Regular Checks and whenever new information become available by the manufacturer or firmware provider.

Post-conditions
Health status of each device is displayed on the Intelligent UI.

Frequency of use
Dependent on the trigger

Non-functional requirements
None

Related use cases
UCG-09-01 Monitor device critical OS files/vulnerabilities UCG-17-01 Remediate Device UCG-14-02 Manage available patch databases

Cyber-Trust Consortium. All rights reserved.

Traceability to
Figure 1.1 - Detailed view of Cyber-Trust project

Example
A Cyber-Trust enabled device is actively monitored [A03] with a healthy status in the visualisation portal [A01]. The MUD service indicates that a new security patch has been released. The device profile CMS filters Cyber-Trust enabled devices that are affected with this update. The smart agent on the device [A12] raises an alert that the device is no longer secure as a new patch has been released. The Cyber-Trust end user is prompted to update their device. Once this is done the smart device agent [A12] checks the integrity of the installed firmware and updates the relevant information in the device profile.

Main scenario

Step	Actor	Action description
1	System	A Cyber-Trust enabled device is actively monitored with a healthy status in the visualisation portal.
2	External Service	The MUD service indicates that a new security patch has been released.
3	System	The patch repository is enriched with the new patch and metadata information
4	System	The device profile CMS filters Cyber-Trust enabled devices that are affected with this update.
5	Smart Device Agent [A12]	The smart agent on the device [A12] raises an alert on the UI that the device is no longer secure as a new patch has been released.
6	Cyber-Trust User	The Cyber-Trust end user is prompted to update their device through the UI portal.
7	Smart Device Agent [A12]	An image of the device firmware is secured and stored for future reference
8	System	Automated firmware updating is triggered by the device information repository
9	System	The device information record is updated to contain the current device information
10	Smart Device Agent [A12]	The smart device agent [A12] checks the integrity of the installed firmware
11	Smart Device Agent [A12]	The result of integrity check is updated in the device profile. and depicted in the visualisation portal.

Cyber-Trust Consortium. All rights reserved.

Extension scenarios

<8>a	Actor	The device does not support for automated firmware updating
1		The user is prompted to manually install the new patch.
2	Cyber-Trust User	The user confirms the patch update

UCG-07-02: Host based vulnerability scanning

Name: Host based vulnerability scanning

Description: The monitoring [A03] of each end user device involves the correlation of information gathered in the eVDB [A07] with vulnerabilities and device characteristics gathered at device level. Information such a communication protocol, open ports, running services, installed firmware etc constitute correlation parameters for the detection of possible vulnerabilities specific to each device.

Type: System Use case

Primary Actor: [P2] A Smart Device owner

Supporting/Secondary actors: [P1] Smart Home Owner

Stakeholders	Interest
Monitoring Service [A03]	To provide information related to types of vulnerabilities to scan for.
Network Modelling [A16]	Check for abnormal network traffic
Cyber-defense Service [A04]	Detection of vulnerabilities trigger backend services for threat detection and mitigation.

Pre-conditions
The smart device agent [A12] is activated.

Trigger conditions
Regular process

Post-conditions
Status update in the detection and mitigation backend content management system [A05]

Minimum guarantees

Cyber-Trust Consortium. All rights reserved.

None

Frequency of use
Periodically multiple times per hour

Non-functional requirements
None

Related use cases
UCG-09-02 Monitor activity on device UCG-10-01 Device Profiling

Traceability to
Figure 1.1 - Detailed view of Cyber-Trust project

Example
A Cyber-Trust enabled device is active and connected to the Cyber-Trust user profile. Upon registration [A06] of the device to Cyber-Trust, information related to the type, make and characteristics of the device are provided. The end device is monitored [A03] in terms of scanned ports and running processes. Information is synced with the central backend database [A07]. In case any attempt is made in modifying the state of the device, backend services are triggered to check the status of vulnerability.

Main scenario

Step	Actor	Action description
1	Smart Device Agent [A12]	The end device actively runs the smart device agent [A12]
2	Smart Device Agent [A12]	On fixed intervals, the smart device agent [A12] checks the device's system for open ports and active processes
3	System	Measured metrics are synced periodically with the device profile repository
4	System	When an attempt is made in modifying the state of the device, backend services are triggered to check the status of vulnerability.

Extension scenarios

<4>a	Actor	Vulnerabilities not detected

Cyber-Trust Consortium. All rights reserved.

1	Monitoring service	Periodic scanning proceeds without alerting or triggering any backend devices.

UCG-07-03: Ensure Device firmware integrity

Name: Ensure Device firmware integrity

Description: A backend service runs between the host and the devices information database to ensure that activated devices operate with the vanilla firmware. In case a fraudulent or altered firmware is detected then backend services for DPI are triggered for remediation and mitigation actions to take place [A04].

Type: System Use case

Primary Actor: System

Supporting/Secondary actors: [O6] Smart Device Manufacturer

Stakeholders	Interest
Cyber-Defence Service [A04]	In the case of fraudulent or infected firmware the Cyber-Defence service [A04] needs to carry out the relevant operations; The device detection and mitigation service will take action when the integrity of a device's firmware is compromised.
Trust Management System [A05]	The trust score of a device is heavily dependent on the integrity of its operating firmware.

Pre-conditions
Available information on current firmware status and updates need to be available by the manufacturer or firmware provider.

Trigger conditions
On the detection of an attempt to alter critical OS files [D5].

Post-conditions
Triggering of relevant services for the handling of the detection of a compromised firmware, in case this happens.

Frequency of use
Dependent on the trigger

Non-functional requirements
None

Cyber-Trust Consortium. All rights reserved.

Related use cases
UCG-09-01 Monitor device critical OS files [D5] /vulnerabilities UCG-07-01 Check device patching status UCG-17-01 Remediate Device

Traceability to
Figure 1.1 - Detailed view of Cyber-Trust project

Example
A Cyber-Trust enabled device is active and connected to the Cyber-Trust user profile. Upon registration of the device to Cyber-Trust [A06], information related to the type, make and characteristics of the device are provided. The Cyber-Trust device repository [A16] system interfaces with the patch database and the MUD services and therefore instructs the Cyber-Trust device agent [A12] on the critical OS files [D5] and vulnerabilities the device is susceptible. The indicated files are continuously monitored, while the relevant rules are set up to allow scanning for vulnerabilities. The smart device agent [A12] suddenly detects that the device's firmware has been altered due to a malware that is trying to adjust its communication practices. The smart device agent [A12] has recognised that critical OS files [D5] have been altered. The smart device agent [A12] instructs for the dumping of the current device firmware to a secured container and instructs the storage of key information in the blockchain [A02]. The vanilla version of the firmware is retrieved from the Patching Database (if available) and installed on the device. The smart device agent [A12] runs checks on the health status of the device again and recognises the correctness of the firmware hashes and the integrity of the device.

Main scenario

Step	Actor	Action description
1	Smart Device Agent [A12]	The list of critical OS files [D5] and vulnerabilities related to the device type are retrieved from the Patch Database
2	Device Information Management System [A05]	The monitoring services [A03] continuously compare the hash information from the device's critical files and the values provided by the device information management system [A05].
3	System	The integrity of the device's firmware is continuously monitored and assured [A03].

<3> a	Actor	Firmware Integrity assurance fails
1	System	The firmware integrity check fails on a device

Cyber-Trust Consortium. All rights reserved.

2	System	The device information management system [A05] is notified
3	System	Remediation actions take place

UCG-08-01: Monitor device at gateway (network traffic filtering)

Name: Monitor device at gateway (network traffic filtering)

Description: The getaway is running network intrusion detection systems (NIDS) to check for signatures and anomalies based on signature.

Type: Network Use case

Primary Actor: Cyber-defense Service [A04]

Supporting/Secondary actors: [P1] Smart Home Owner, [O2] ISP, [O4] IoT SP

Stakeholders	Interest
Cyber-defense Service [A04]	Detect anomalies

Pre-conditions
Known malicious signatures have been updated. Network traffic (Packets)

Post-conditions
Apply network security rules

Frequency of use
Continuous operation

Non-functional requirements
None

Related use cases
UCG-09-02 UCG-06-01

Cyber-Trust Consortium. All rights reserved.

UCG-08-02

Traceability to
Figure 1.1 - Detailed view of Cyber-Trust project

Example
Mary agrees as part of the Cyber-Trust agreement that her ISP platform will be conducting Network Intrusion detection system (NIDS), using Cyber-defense Service [A04], as part of the service to her, so as to be able to protect her systems and services by having her network gateway data monitored.

Main scenario

Step	Actor	Action description
1	System	The system retrieves Known attack signatures eVDB
2	System	The system will check each packet passing through gateway
3	System	The system uses Smart Gateway Agent [A11] to detect the attacks.
4	Smart Gateway Agent [A11]	Smart Gateway Agent uses a network probe to capture raw packet data.
5	network probe	Network probe retrieves packet information such as source and destination IP address, source and destination ports, flags, header length, checksum.
6	Smart Gateway Agent[A11]	Smart Gateway Agent [A11] compares the packets information with known attack signatures to identify threats
7	Smart Gateway Agent [A11]	Smart Gateway Agent [A11] reports the attack to security officer.
8	security officer	security officer tracks down the attacker.

Extension scenarios

<#>a	Actor	No anomaly packet was identified
1	System	The system allows the packet passing to the gateway to network.
2	System	System checks the next packet.

Cyber-Trust Consortium. All rights reserved.

UCG-08-02: Capture and classify network packets (DPI)

Name: Capture and classify network packets (DPI)

Description: the system automatically captures and classify the packets based on their contents; this can achieve using Deep Packet Inspection (DPI) approach. The DPI will characterize the packets into various categories such as benign, anomaly, suspected.

Type: Network use case

Primary Actor: DPI

Supporting/Secondary actors: Network administrator [O2]

Stakeholders	Interest
Trust DB Admin Module [A08]	Manage the traffic via the network
Smart Gateway Agent [A11]	Analysing the packets

Pre-conditions
Network administrator is logged into the network

Trigger conditions
Network traffic (Packets)

Post-conditions
Deep Packet Inspection (DPI) has been updated to detect new unwanted packets.

Frequency of use
Multiple times per minute

Non-functional requirements
None

Related use cases
Detect abnormal packets within network traffic of IOT

Traceability to
None

Example

Cyber-Trust Consortium. All rights reserved.

The DPI characterizes the packets into various categories such as benign, anomaly, suspected [A11].

Main scenario

Step	Actor	Action description
1	System	The system retrieves intelligence from T5.2
2	System	The system will check each packet transferring between nodes.
3	System	The system uses Deep Packet Inspection (DPI), Smart Gateway Agent [A11] to read the headers and the payloads of packets.
4	Deep Packet Inspection (DPI)	DPI analyzing the packets and correlating information across multiple packets to identify the network application.
5	Deep Packet Inspection (DPI)	DPI will identify the anomalies packets that generated by the that application.
6	Deep Packet Inspection (DPI)	The DPI can either take the decision to block, tag, or redirects these packets to the network administrator.
7	Network Administrator	Network Administrator uses the tagging packets for prioritizing and assigning different QoS (Quality Of Service) levels to various traffic flows.
8	Network Administrator	Network Administrator redirects the packets in case of intrusion detection to the “honey-pots” to track down the attacker.

Extension scenarios

After step 5	Actor	No anomaly packet was identified
1	System	The system allows the packet passing to the target node.
2	System	System checks the next packet.

UCG-09-01: Monitor device critical OS files / vulnerabilities

Name: Monitor device critical OS files / vulnerabilities

Description: The critical OS files/directories [D5] are recognised in this use case and are continuously monitored [A03]. The device is scanned for open ports and running processes. Information is synced with the central backend database. In case any attempt is made in modifying the state of the device, backend services are triggered to check the status of vulnerability.

Type: System Use case

Primary Actor: [P2] A Smart Device owner

Supporting/Secondary actors: [P1] Smart Home Owner, [O2] ISP, [O4] IoT SP

Cyber-Trust Consortium. All rights reserved.

Stakeholders	Interest
Smart Device Agents [A12]	The smart device agent is responsible for the monitoring of device OS files/ vulnerabilities
Cyber-defense Service [A04]	Detection of suspicious content triggers backend services for threat detection and mitigation.

Pre-conditions
The monitored device is Cyber-Trust eligible and the smart device agent [A12] is activated.

Trigger conditions
Smart device agent [A12] is activated

Post-conditions
The intelligent UI and backend services are triggered for DPI analysis.

Frequency of use
Continuous operation

Non-functional requirements
None

Related use cases
UCG-07-01 Checking Device Patching Status UCG-07-02 Host based Vulnerability Scanning UCG-14-01 Update device critical OS files/vulnerabilities

Traceability to
Figure 1.1 - Detailed view of Cyber-Trust project

Example
A Cyber-Trust enabled device is active and connected to the Cyber-Trust user profile. Upon registration of the device to Cyber-Trust [A06], information related to the type, make and characteristics of the device are provided. The Cyber-Trust device repository system [A16] interfaces with the patch database and the MUD services and therefore instructs the Cyber-Trust device agent [A12] on the critical OS files [D5] and vulnerabilities the device is susceptible. The indicated files are continuously monitored [A03], while the relevant rules are set up to allow scanning for vulnerabilities.

Cyber-Trust Consortium. All rights reserved.

Main scenario

Step	Actor	Action description
1	Cyber-Trust User	The user registers a Cyber-Trust device to its profile for active monitoring and provides all available information with regards to device characteristics.
2	System	The device profile repository is enriched with the new information and builds the device profile by retrieving all available information through the interfaced repositories.
3	Cyber-Trust User	The user activates the operation of the smart device agent [A12] through the UI portal.
4	System	The Cyber-Trust device repository system interfaces with the patch database and the MUD services and therefore instructs the Cyber-Trust device agent on the critical OS files [D5] and vulnerabilities the device is susceptible.
5	Smart Device Agent [A12]	The Cyber-Trust device level services initiate monitoring [A03] at all supported levels. The indicated files are continuously monitored, while the relevant rules are set up to allow scanning for vulnerabilities.

UCG-09-02: Monitor activity on device

Name: Monitor activity on device

Description: This use case involves the monitoring [A03] of communication and data transactions on the monitored device. It involves the logging of key device communication

Type: System Use case

Primary Actor: [P2] A Smart Device owner

Supporting/Secondary actors: [P1] A Smart Device owner

Stakeholders	Interest
Smart Device Agents [A12]	The smart device agent [A12] is responsible for the monitoring of device related aspects.
Network Modelling [A16]	Depending on the types of supporting connections and protocols the network topology will be feeding information with regards to the monitored protocols and traffic trends
Cyber-defense Service [A04]	Detection of vulnerabilities trigger backend services for threat detection and mitigation.

Pre-conditions

Cyber-Trust Consortium. All rights reserved.

The smart device agent [A12] is activated

Trigger conditions
Continuous operation whenever traffic flows through the device.

Post-conditions
Alerts and triggering of backend analysis services for DPI. Analysis results and verified alerts are visualised in the intelligent UI.

Minimum guarantees
None

Frequency of use
Continuous whenever network traffic flows and data transactions occur.

Non-functional requirements
None

Related use cases
UCG-09-01 Monitor device critical OS files [D5] / vulnerabilities UCG-14-01 Update device critical OS files [D5] /vulnerabilities UCG-10-03 Retrieve device profile information

Traceability to
Figure 1.1 - Detailed view of Cyber-Trust project

Example
A Cyber-Trust enabled device is active and connected to the Cyber-Trust user profile. Upon registration of the device to Cyber-Trust [A06], information related to the type, make and characteristics of the device are provided. The end device is monitored [A03] in terms of communication and data transactions. Traffic flows in and out the monitored device [A03], the protocol and type of communication are extracted and go through the rule based smart agent for anomaly detection.

Main scenario

Step	Actor	Action description

Cyber-Trust Consortium. All rights reserved.

1	Smart Device Agent [A12]	The end device actively runs the smart device agent [A12]
2	Smart Device Agent [A12]	Continuously, the smart device agent [A12 checks the device's system for monitored [A03] in terms of communication and data transactions. Incoming and outgoing packets go through a rule-based anomaly detection system. Packets are temporarily stored and overwritten over time
3	System	When anomalies are detected in the traffic, measured metrics along with temporarily stored packets are synced with the device profile repository and the blockchain ledger
4	System	Backend analysis services are triggered for further analysis in the characteristics of network traffic and packet payload with DPI

Extension scenarios

<3>a	Actor	Anomalies are not detected in the traffic
1	Monitoring service	Monitoring continuous without alerting or triggering any backend devices.

UCG-09-03: Perform vulnerability scanning

Name: Perform vulnerability scanning

Description: the system performs vulnerability scanning on all IoT devices when the eVDB [A07] is updated with new vulnerabilities or new IoT device is in registered to the Cyber-Trust [A06].

Type: System

Primary Actor: System

Supporting/Secondary actors: IoT device

Stakeholders	Interest
System	Performs vulnerability scan on the IoT device
IoT device	Replies to the scan requests

Pre-conditions
There is an active IoT device

Cyber-Trust Consortium. All rights reserved.

Trigger conditions
eVDB [A07] is updated with new vulnerabilities
New IoT device is registered to Cyber-Trust [A06]

Post-conditions
Vulnerability scan report is generated

Frequency of use
Multiple times per day

Non-functional requirements

Related use cases
[UCG-10-03]

Traceability to
None

Example
The system performs vulnerability scanning on all IoT devices that the vulnerability level of these devices has not been assessed for the last 15 days.

Main scenario

Step	Actor	Action description
1	System	The system retrieves intelligence form the Enriched eVDB
2	System	The system locates the list of devices to be scanned
3	System	The System retrieves devices profile information
4	System	The System performs venerability scan on the devices
5	System	The System issues a scan report to the security officer with the details of the vulnerability scan results.

Extension scenarios

Cyber-Trust Consortium. All rights reserved.

After step 4	Actor	Vulnerabilities not detected
1		Periodic scanning proceeds without alerting or triggering any backend devices.

UCG-09-04: Detect network attacks

Name: Detect network attacks

Description: Intrusion detection system (IDS) [A11] is utilized to monitor packets on the network in order to detect the attacks and malicious threats in network. IDS compare packets signature with against a database of signatures or attributes from known malicious threats.

Type: Network use case

Primary Actor: Cyber-defense Service [A04]

Supporting/Secondary actors: Network data [D4]

Stakeholders	Interest
Cyber-defense Service [A04]	Manage the traffic via the network
Smart Gateway Agent [A11]	Detect network attacks

Pre-conditions
known malicious threats has been updated

Trigger conditions
Network traffic (Packets)

Post-conditions
Intrusion detection system alerted the network administrator with the detected threats.

Frequency of use
Multiple times per minute

Non-functional requirements
None

Related use cases
Detect threats within network traffic of IOT

Cyber-Trust Consortium. All rights reserved.

Traceability to
None

Example
The IDS compare packets signature with against a database of signatures or attributes from known malicious threats.

Main scenario

Step	Actor	Action description
1	System	The system retrieves Known attack signatures form T5.2
2	System	The system will check each packet passing through network
3	System	The system uses IDS to detect the attacks.
4	IDS	IDS use a network probe to capture raw packet data.
5	network probe	network probe retrieves packet information such as source and destination IP address, source and destination ports, flags, header length, checksum.
6	IDS	IDS compare the packets information with known attack signatures to identify threats to the network.
7	IDS	IDS reporting the attack to network administrator.
8	Network Administrator	Network Administrator track down the attacker.

Extension scenarios

After step 6	Actor	No anomaly packet was identified
1	System	The system allows the packet passing to the target node.
2	System	System checks the next packet.

After step 7	Actor	The Network Administrator found it is false alarm
1	Network Administrator	The Network Administrator dismiss the alert
2	Network Administrator	The Network Administrator ensures that the device is unblocked

UCG-10-01: Device Profiling

Name: Device Profiling

Cyber-Trust Consortium. All rights reserved.

Description: This use case is responsible for the gathering of as much information as possible with regards to the state and characteristics of a device. Information is gathered [A03] from both system info at device level (CPU, memory, running processes, network usage etc) and also from the input of the end user. Information retained by Cyber-Trust is also enriched with manufacturer use guidelines whenever these are available; such information may greatly assist in the detection of abnormal behaviour as per the manufacturer. Through this use case the end user is also capable of determining if partial or full monitoring [A03] will be performed on its devices.

Type: System Use case

Primary Actor: [P2] A Smart Device owner

Supporting/Secondary actors: [P1] Smart Home Owner, [O2] ISP, [O4] IoT SP

Stakeholders	Interest
Smart Device Agent [A12]	The smart device agent [A12] is responsible for the monitoring of device [A03] key characteristics.

Pre-conditions
The smart device agent [A12] is deployed and activated.

Trigger conditions
No trigger required

Post-conditions
Device performance metrics are synced with the detection and mitigation backend content management system [A05]

Minimum guarantees
The device holds an OS that supports the retrieval of performance metrics and operation parameters.

Frequency of use
Continuous operation

Non-functional requirements
None

Related use cases
UCG-01-01-01 Activate device agent UCG-09-02 Monitor activity on device

Cyber-Trust Consortium. All rights reserved.

UCG-10-03 Retrieve device profile information UCG-07-03 Ensure Device firmware integrity

Traceability to
Figure 1.1 - Detailed view of Cyber-Trust project

Example
A Cyber-Trust enabled device is active and connected to the Cyber-Trust user profile. Upon registration of the device to Cyber-Trust [A06], information related to the type, make and characteristics of the device are provided. Depending on the characteristics of the device, the smart device agent [A12] continuously gathers information with regards to the state and characteristics of a device such as CPU, memory, running processes and network usage. This information is synced with the device profile repository and serves as enriched information for the detection of abnormal activity and the construction on device use trends.

Main scenario

Step	Actor	Action description
1	Cyber-Trust User	Upon device registration [A06] the user provides as much information and device characteristics as possible to the Cyber-Trust system through the UI portal.
2	Device Information Management System [A05]	Newly admitted information is added to the device information management system for storage.
3	Device Information Management System [A05]	The device information management system [A05] instructs the smart device agent [A12] to continuously monitor its state and performance.
4	Smart Device Agent [A12]	Monitored parameters go through a rule based HIDS and when abnormal device performance is detected the device information management system [A05] is notified to trigger analysis from backend components.
5	Smart Device Agent [A12]	The smart device agent [A12] periodically syncs device information with the device information management system [A05]

UCG-10-02: Data Anonymisation

Name: Data Anonymisation

Description: Data related to the operation of Cyber-Trust[A06] is useful throughout the Cyber-Trust ecosystem and also to external platforms. Such information is anonymised and shared within the system for the improvement of system operations [A04]. This use case is also involved in cases sharing of information with other external platforms is desired.

Type: System Use case

Cyber-Trust Consortium. All rights reserved.

Primary Actor: [P1] Smart Home Owner, [O2] ISP, [O4] IoT SP

Supporting/Secondary actors: [O6] Smart Device Manufacturer

Stakeholders	Interest
Profiling Service [A17]	Anonymised data will serve as input to the profiling service [A17] as enriched information to assist in the adjustment and updating of profiling rules and operations.
ISP [02]	The ISP will gain access to data insights gathered from the monitored Cyber-Trust infrastructure to better manage own resources.
Cyber-Trust Service Provider [01]	Anonymised data will become available to Cyber-Trust platform components for improving their operation and performance.
Visualisation Portal [A01]	Statistics and data insights extracted from all monitored devices will be visualised in the portal [A01].

Pre-conditions
The user has consent to the use of their data for the needs of the identified stakeholders.

Trigger conditions
none

Post-conditions
Anonymised enriched information is disseminated within the Cyber-Trust infrastructure for the improvement of provisioned functionality.

Minimum guarantees
None

Frequency of use
Ad hoc

Non-functional requirements
None

Related use cases
UCG-09-02 Monitor activity on device

Cyber-Trust Consortium. All rights reserved.

Traceability to
Figure 1.1 - Detailed view of Cyber-Trust project

Example
None

Main scenario

Step	Actor	Action description
1	Smart Device Agent [A12]	Data transactions, network traffic and data profiling are continuously monitored at the smart device agent [A12] level
2	Device Information Management System [A05]	Key information is synced with the device information management system [A05]
3	System	Anonymised data are serviced to the relevant entity

Extension scenarios

<3> a	Use anonymised information to internal components
1	Internal Cyber-Trust components request for anonymised data from the device information management system [A05]
2	The device information management system [A05] filters personal and restricted data and responds to the request

<3> a	Share anonymised information to external systems
1	An external component requests for anonymised data from the device information management system [A05]
2	The device information management system [A05] filters personal and restricted data and responds to the request

UCG-10-03: Retrieve device profile information

Name: Retrieve device profile information

Description: Information related to device characteristics as well as an evolving log of alteration and events related to each device are maintained in the system. This information will become available to system components needing this for analysis and visualisation purposes [A01].

Cyber-Trust Consortium. All rights reserved.

Type: Business Use case

Primary Actor: [P2] A smart device owner, [O2] ISP, [O4] IoT-SP

Supporting/Secondary actors: [P1] Smart Home Owner

Stakeholders	Interest
Visualisation Portal [A01]	Device related information will be visualised in the portals [A01] for the user to monitor/ observe.
Cyber-Defence Service [A04]	Device profile information will become available to the Cyber-Defence service [A04] to carry out device related operations.

Pre-conditions
The device is registered to the Cyber-Trust platform.

Trigger conditions
Ad Hoc whenever needed by Cyber-Trust backend services and for the updating of information found on the visualisation portals [A01].

Post-conditions
None

Minimum guarantees
None

Frequency of use
Ad Hoc

Non-functional requirements
None

Related use cases
UCG-10-01 Device Profiling

Traceability to
Figure 1.1 - Detailed view of Cyber-Trust project

Cyber-Trust Consortium. All rights reserved.

Example
The TMS service is called to calculate the trust score of a monitored device [A03]. For this it calls the exposed web service of device profile repository [A16] with a request to retrieve all relevant device profile information [A04]. The Trust score is calculated as per UCG-14-08

Main scenario

Step	Actor	Action description
1	System	An internal Cyber-Trust component requests the device information management system [A05] for the profile of a specific device
2	Device Information Management System [A05]	The device information management system [A05] logs the request and responds with the relevant information.

UCG-10-04: Manually curate device profile

Name: Manually curate device profile

Description: The administrator manually curates the TrustDB [A08]; this is required to reduce device trust status as a result of a risk not identified by the platform or restore device trust level after a successful clean-up. Devices can be taken administratively off to cater for service time and avoid thus alarms being raised to the intelligent UI user.

Type: System Use Case

Primary Actor: TrustDB Admin Module [A08], System

Supporting/Secondary actors: - N/A

Stakeholders	Interest
TrustDB administrator	Keep the contents of the Trust DB up to date
Intelligent UI user	Receive only accurate alerts

Conditions
Trust DB administrator logged into the Cyber Trust system

Trigger conditions
User request

Post-conditions

Cyber-Trust Consortium. All rights reserved.

Trust DB[A08] has been updated to reflect the new health status of the device. The device trust level has been recomputed.

Frequency of use
Multiple times per day

Non-functional requirements
None

Related use cases
UCG-10-01

Traceability to
Figure 1.1 - Detailed view of Cyber-Trust project

Example
Smith, a Trust DB administrator [A08] alerted that the Smartphone XIU234958 has been cleaned of the malware that was installed on it. John locates the profile of the phone within the Trust DB [A08] and updates it to reflect that the device is healthy. The trust database management module triggers a re-assessment of the device trust level [A05].

Main scenario

Step	Actor	Action Description
1	Trust DB administrator [A08]	The Trust DB administrator selects the “Find device” functionality.
2	System	The system presents a form to allow the Trust DB administrator [A08] to enter search criteria.
3	Trust DB administrator	The Trust DB administrator enters the search criteria and submits the form.
4	System	The system retrieves from the Trust DB device records that match the criteria.
5	System	The system presents the device information to the Trust DB administrator.
6	Trust DB administrator	The Trust DB administrator selects the device to be updated and submits this information.

Cyber-Trust Consortium. All rights reserved.

7	System	The system presents a detailed record of the device trust status and appropriate controls to allow the update, including “change status”, “delete”, “take offline”.
8	Trust DB administrator	The Trust DB administrator chooses the desired update; additional information may be entered to document the reason for the device trust status change.
9	Trust DB administrator	The Trust DB administrator submits the information.
10	System	The system validates the completeness and validity of the information.
11	System	The system updates the trust status of the device in the Trust DB [A08] and registers additional information in the device history.
12	System	The system recalculates the trust level of the device.
13	System	The system informs the Trust DB administrator that the update has been performed.

Extension scenarios

4a		No device matches the criteria
1	System	The system notifies the user that no devices were retrieved
2	System	Control returns to step #2

10a	Actor	The information submitted by the user is incomplete/erroneous
1	System	The system informs the Trust DB administrator[A08] regarding the errors or omissions
2	System	Control returns to step #8

*a	Actor	The Trust DB administrator cancels the process (at any step)
1	Trust DB administrator	The Trust DB administrator cancels the process
2	System	The system terminates the procedure and destroys the Trust DB management form

UCG-16-01: Determine device firmware and software through remote detection

Name: Determine device firmware and software through remote detection

Cyber-Trust Consortium. All rights reserved.

Description: A backend service runs between the device and central device profile database to identify device's firmware and software thereby building and updating the central database with all firmware. As a result, the system can be able to generate metrics such as vulnerability and trust.

Type: System Use case

Primary Actor: System

Supporting/Secondary actors: Smart Device Agent [A12]

Stakeholders	Interest
Trust Management System [A05]	The trust score of a device is heavily dependent on the integrity of its operating firmware.

Pre-conditions
Available information on current firmware status and updates need to be available by the manufacturer or firmware provider.

Trigger conditions
Firmware and software

Post-conditions
Triggering of relevant services for the updating of the central device profile database.

Frequency of use
Dependent on the trigger

Non-functional requirements
None

Related use cases
UCG-09-01: Monitor device critical OS files **[D5]** /vulnerabilities UCG-07-01: Check device patching status UCG-07-03: Ensure Device firmware integrity

Traceability to
None

Example

Cyber-Trust Consortium. All rights reserved.

A Cyber-Trust enabled device is active and connected to the Cyber-Trust user profile [A17]. Upon registration of the device to Cyber-Trust [A06], information related to the type, make and characteristics of the device are provided. The Cyber-Trust device repository system interfaces with the patch database and the MUD services and therefore instructs the Cyber-Trust device agent [A12] on the critical OS files [D5] and vulnerabilities the device is susceptible. The indicated files are continuously monitored, while the relevant rules are set up to allow scanning for vulnerabilities.

Main scenario

Step	Actor	Action description
1	Smart Device Agent [A12]	The list of critical OS files [D5] and vulnerabilities related to the device type are retrieved from the Patch Database
2	monitoring services [A03]	The monitoring services [A03] continuously compare the hash information from the device's critical files and the values provided by the device information management system [A05].
3	System	The system continuously updates the central device profile database with new device's firmware.

Extension scenarios

<#>a	Actor	Firmware detection fails
1	System	The firmware check fails on a device
2	System	The device information management system [A05] is notified

UCG-10-05: Gateway Network Device Profiling

Name: Gateway Network Device Profiling

Description: The gateway module will profile traffic for each device the user accepted the terms and conditions to allow the necessary monitoring [A03] to detect abnormal traffic.

Type: System

Primary Actor: [A03] Monitoring Service

Supporting/Secondary actors: [A04] Cyber-defense Service, [A11] Smart Gateway Agent, [A12] Smart Device Agent, System, [A17] Profiling Service

Stakeholders	Interest
System	Provides profiling data

Pre-conditions
Monitoring Service is active, and network is live

Cyber-Trust Consortium. All rights reserved.

Trigger conditions
Devices registered on the Cyber-Trust network and network live

Post-conditions
DPI supported as required

Frequency of use
Continuous Operation

Non-functional requirements
None

Related use cases
UCG-08-02 Capture and classify network packets

Traceability to
Figure 1.1 - Detailed view of Cyber-Trust project

Example
Supports DPI by the provision of network data covering IP, Headers and Data Payloads for analysis by DPI when DPI is activated by an alert.

Main scenario

Step	Actor	Action description
1	System	New device is registered on the network
2	Profiling Service [A17]	The profiling service uses the monitoring service to gather intelligence from devices' traffic
3	System	The profile is generated
5	System	Gateway module supplies DPI capability with full network data

Extension scenarios

After step 2	Actor	The monitoring service is activated
1	System	gathers data from the network and the devices

Cyber-Trust Consortium. All rights reserved.

UCG-10-06: Get Device Information

Name: Get Device Information.

Description: A user wants to get information regarding a device that he previously registers on the platform [A06].

Type: Business use case

Primary Actor: [P1, P2] user,

Supporting/Secondary actors: System

Stakeholders	Interest
[P1, P2] user	Get more information about a device that belongs to her.
System	Provide the user to access the information she requests.

Pre-conditions
A user has already registered itself and register one or more device. He is logged to the platform and on its profile page.

Trigger conditions
The user clicks on the button 'Get information' next to the device he wants to get information about.

Post-conditions
The user access to the web page he asks for.

Minimum guarantees
A web pages.

Frequency of use
Once per user request.

Related use cases

Example
As a user ([P1, P2]) user I want to get information of a specific device own by a specific user in order to investigate.

Main scenario

Cyber-Trust Consortium. All rights reserved.

Step	Actor	Action description
1	[P1, P2] user	The actor selects the device. He clicks on get the 'Get information'.
2	System	The system redirects the user to a new page containing the information she asked for.

UCG-11-01: Gather device forensic evidence

Description: The procedure of gathering evidence specially in IoT environment differs based on the device, it's storage capabilities and software. This UC will depict the collection and storage of forensic evidences [A02] (e.g. device log files, timestamps etc.) from the cyber-trust registered devices [A06].

Type: system use case

Primary Actor: [O3] LEA, [O2] ISP, [P1, P2] user, System

Supporting/Secondary actors: [A16] Network architecture and assets repository, [A01] Visualisation Portal, Peer trust management systems [A05], Intelligent UI, Advanced 2D/3D visualization Portal [A01], DLT Service [A02], eVDB Admin Module [A07], DLT Service [A02]

Stakeholders	Interest
DLT Service [A02]	Store the forensic evidences.
Intelligent UI	Receive alerts on device risk changes, especially for devices risk level is above some critical level
Infrastructure owner	Protect other devices from attacks coming from devices with high risk level

Pre-conditions
Device is Cyber-Trust registered; Cyber-attack, malware infection, abnormally behavior; low trust level of device;

Trigger conditions
Manual/on demand; Automatically from the Cyber-Trust system;

Post-conditions
In case of automatic triggering raise alert for the user that data that may contain forensic evidences (e.g. audit logs, critical s/w and OS files, information regarding the firmware and relevant configurations) are been collected [A02].

Frequency of use

Cyber-Trust Consortium. All rights reserved.

N/A

Non-functional requirements
Policy; National Legislation;

Related use cases
UCG-01-01-01; UCG-09-01; UCG-09-02; UCG-10-01; UCG-07-03; UCG-06-01; UCG-06-02; UCG-10-05; UCG-12-05;

Traceability to
Figure 1.1 - Detailed view of Cyber-Trust project

Example
After the detection of an attack, malware infection, abnormally behavior [A04] or low score of devices [A05], Cyber-Trust system is automatically collecting data that may contain forensic evidences [A03]. The alternative is that the owner chooses to manually run the process and collect this data. In both cases the evidences are stored in the Forensic Evidence DB and the hash value is stored in the DLT [A02] in order to validate the evidences. The user is able to explore the evidences and visualize the respective information [A01].

Main scenario

Step	Actor	Action
1	System	The forensic evidence collection is triggered
1	Actor	The actor decides to trigger the forensic evidence collection process
2	System	Collection of relevant data such as, log files, audit logs, critical s/w and OS files, information regarding the firmware and relevant configurations
3	System/Forensic Evidence eVDB	Storage of the data in the Forensic evidence DB
4	Forensic Evidence eVDB	Once the data is stored in the respective DB notification is send to the ISP as well as the hash value of the stored data, respective time stamps, owner of the data etc. in order to store the information in the DLT

Extension scenarios

Cyber-Trust Consortium. All rights reserved.

After Step 4	Actor	Action
1	ISP	The ISP is responsible to store the information of Step 4 in the DLT.
2	DLT Device	Explore forensic evidences
3	DLT Device	Visualize forensic evidences
4	DLT Device	Export forensic evidences

UCG-11-02: Gather network forensic evidence

Name: Gather network forensic evidence

Description: The process (automatic) and conditions (e.g. with the identification of an attack) under which the Cyber-Trust will start collecting relevant network data [A03] in order to be used as digital forensic evidences in in the court of law as well as the collection mechanisms/techniques (e.g. DPI)

Type: system use case

Primary Actor: [O3] LEA, [O2] ISP, [P1, P2] user, System

Supporting/Secondary actors: [A16] Network architecture and assets repository, [A01] Visualisation Portal, [A05] Peer trust management systems, Intelligent UI, Advanced 2D/3D Visualization Portal [A01], DLT Service [A02], eVDB Admin Module [A07], DLT Service [A02], System .

Stakeholders	Interest
eVDB Admin Module [A07]	Store the forensic evidences.
Intelligent UI	Receive alerts on device risk changes, especially for devices risk level is above some critical level
Infrastructure owner	Protect other devices from attacks coming from devices with high risk level

Pre-conditions
Register to the cyber-trust system; Cyber-attack, malware infection, abnormally behavior; low trust level of device;

Trigger conditions
Manual/on demand; Automatically from the Cyber-Trust system;

Post-conditions
In case of automatic triggering raise alert for the user, that network data that may contain forensic evidences (data packets, protocol information etc.) are been collected.

Cyber-Trust Consortium. All rights reserved.

Frequency of use
N/A

Non-functional requirements
Policy; National Legislation;

Related use cases
UCG-02-02; UCG-02-01; UCG-01-01-01; UCG-08-01; UCG-06-01; UCG-06-02; UCG-08-02; UCG-09-04; UCG-16-02; UCG-10-05; UCG-14-06; UCG-12-02; UCG-12-04; UCG-12-05;

Traceability to
Figure 1.1 - Detailed view of Cyber-Trust project

Example
After the detection of an attack, malware infection, abnormally behavior or low score of devices [A03, A04, A05], Cyber-Trust system is automatically collecting network data that may contain forensic evidences. The alternative is that the owner chooses to manually run the process and collect this data. In both cases the collected data is stored in the Forensic Evidence eVDB [A07] and the hash value is stored in the DLT ([A02]) in order to validate the evidences. The user is able to explore the evidences and visualize the respective information.

Main scenario

Step	Actor	Action
1	System	The forensic evidence collection is triggered
1	Actor	The actor decides to trigger the forensic evidence collection process
2	System	Collection of relevant data such as, data packets, log files, traffic analysis, protocol, information deriving from the DPI
3	System/Forensic Evidence eVDB	Storage of the data in the Forensic evidence eVDB
4	Forensic Evidence eVDB	Once the data is stored in the respective eVDB notification is send to the ISP as well as the hash value of the stored data, respective time stamps, owner of the data etc. in order to store the information in the DLT

Extension scenarios

After step 4

Cyber-Trust Consortium. All rights reserved.

1	ISP	The ISP is responsible to store the information of Step 4 in the DLT.
2	DLT Device	Explore forensic evidences
3	DLT Device	Visualize forensic evidences
4	DLT Device	Export forensic evidences

UCG-12-01: Export Trusted logs

Name: Export Trusted logs.

Description: Describe the steps involved in gathering and returning trusted logs previously stored into the DLT [A02].

Type: Business use case

Primary Actor: [O3] LEA

Supporting/Secondary actors: System

Stakeholders	Interest
[O3] LEA	Export the logs for his investigations
System	Give user access to the logs he asks for

Pre-conditions
A user has already registered itself and register one or more device. And logs from this device have been saved inside the DLT. The user needs to have the rights to access the logs.

Trigger conditions
A user requests the logs of a device.

Post-conditions
The user gets trusted logs of the device.

Minimum guarantees
A web page

Frequency of use
Once a user requests the logs of a device.

Related use cases

Cyber-Trust Consortium. All rights reserved.

UCG-12-03, UCG-14-05

Traceability to
Figure 1.1 - Detailed view of Cyber-Trust project

Example
As a (Actor: [O3]) Police officer I want to get trusted logs of a specific device own by a specific user in order to investigate on it. [A02].

Main scenario

Step	Actor	Action description
1	[O3] LEA	The actor goes to the personal page of the device's owner he wants to investigate on. He can view all the devices own by the owner.
2	[O3] LEA	The actor selects the device. He clicks on get the 'Download Trusted logs button'.
3	System	The system sends the information via a file to the user.

UCG-12-02: Export Forensic evidence

Name: Export Forensic evidence.

Description: Describe the steps involved in gathering and returning forensic evidence previously stored into the DLT [A02].

Type: Business use case

Primary Actor: [O3] Police officer

Supporting/Secondary actors: System

Stakeholders	Interest
[O3] Police officer	Get forensics evidence from the DLT.
System	Provide the user the forensic evidence he asks

Pre-conditions
A user has already registered itself and register one or more device.

Trigger conditions

Post-conditions

Cyber-Trust Consortium. All rights reserved.

The analyst gets evidences of a device.

Minimum guarantees
A web page

Frequency of use
Occasionally

Related use cases
UCG-14-04

Traceability to
Figure 1.1 - Detailed view of Cyber-Trust project

Example
As a (Actor: O3) Police officer I want to get forensic evidence of a specific device own by a specific user in order to present it to legal authority [A02].

Main scenario

Step	Actor	Action
1	[O3] Police officer	The actor goes to the personal page of the device's owner he wants to investigate on. He can view all the devices own by the owner.
2	[O3] Police officer	The actor selects the device. He clicks on get the 'Get Evidence' button.
3	System	The system sends the information via a file to the police Officer[O3].

UCG-12-03: Explore trusted logs

Name: Explore trusted logs.

Description: Use Cyber-Trust logs explorer in order to explore / sort / filter the logs [A01] stored by the ISP [A02].

Type: Business use case

Primary Actor: [O3] Police officer

Supporting/Secondary actors: None

Cyber-Trust Consortium. All rights reserved.

Stakeholders	Interest
[O1, 3] Administrator	Navigate through logs to identify abnormal behaviour or to get more information about an incident
System	Give user access to the logs user asks for

Pre-conditions
A user has already registered itself and register one or more device.

Trigger conditions
None

Post-conditions
The user accesses a web page with the last logs of a device.

Minimum guarantees
A web pages

Frequency of use
Occasionally

Related use cases

Traceability to
Figure 1.1 - Detailed view of Cyber-Trust project

Example
As a (Actor: O3) Police officer I want to view trusted logs [A02], [A02] of a specific device own by a specific user in order to help me in my investigation.

Main scenario

Step	Actor	Action

Cyber-Trust Consortium. All rights reserved.

1	O3 Police officer	The actor goes to the page of the device he investigates about. He then clicks the button 'Access logs.
2	O3 Police officer	He is seeing the devices trusted logs. The attack he investigates between the XX/XX/XXXX and YY/YY/YYYY. He sorts the logs on the screen to only get the logs in this timeframe.

UCG-12-04: Visualize forensic

Name: Visualize forensic

Description: Use Cyber-Trust forensics visualiser in order to see [A01] the data stored in the DLT [A02] with a user-friendly interface

Type: Business use case

Primary Actor: [O3] Police officer

Supporting/Secondary actors: ISP

Stakeholders	Interest
[O3] Police officer	Get forensics evidence from the DLT.
System	Provide the user the forensic evidence she asks

Pre-conditions
A user has already registered itself and register one or more device.

Trigger conditions

Post-conditions
The user accesses a web page with the last logs of a device.

Minimum guarantees
A web pages

Frequency of use
Occasionally

Related use cases

Cyber-Trust Consortium. All rights reserved.

Traceability to
Figure 1.1 - Detailed view of Cyber-Trust project

Example
As a (O3) Police officer want to visualize the forensic stored on the DLT [A02], in order to help me in my investigation by seeing who own the data stored off-chain [A02].

Main scenario

Step	Actor	Action
1	[O3] Police officer	The actor goes to the blockchain explorer of the DLT. He can filter/sort the metadata store by the type of device, timestamp, company that own the data.

UCG-12-05: Validate evidence block

Name: Validate evidence block

Description: Describe the block validation process by the DLT [A02] and the block propagation inside of the DLT.

Type: System use case

Primary Actor:

Supporting/Secondary actors: None

Stakeholders	Interest
System	Systems validate the blocks
Pre-conditions	

Trigger conditions
UCG-14-06

Post-conditions
The block created on UCG-14-06 is now propagated on the DLT

Minimum guarantees

Cyber-Trust Consortium. All rights reserved.

Frequency of use
Occasionally

Related use cases

Traceability to
Figure 1.1 - Detailed view of Cyber-Trust project

Example
A block of forensic has been created ([A02]). The block is not validated and propagated yet. After that process, the block will be part of the DLT.

Main scenario

Step	Actor	Action
1	System	A new forensic evidence appears on the memory pool. The data of the evidence is valid and ready to be inserted inside the system. Once enough evidence has accumulated the node begins the process of creating a new block and adding it to the chain.
2	System	The system will find a valid hash in order to pass the cryptographic proof and add it to the blockchain.
3	System	The node where the block has been validated will now propagate it to the other nodes of the blockchain.
4	System	End of the process, the blockchain has been updated.

UCG-13-01: Retrieve trust level from TMS

Name: Retrieve trust level from TMS

Description: The TMS receives and honors a request for retrieving the trust level of a specific device or a group of devices [A05].

Type: system use case

Primary Actor: <none; this use case is triggered from other use cases>

Supporting/Secondary actors: -

Stakeholders	Interest

Cyber-Trust Consortium. All rights reserved.

Intelligent UI user	Obtain a view of the trust levels of the devices within the infrastructure
Infrastructure owner	Exploit the trust level of the device to protect other assets

Pre-conditions
None

Trigger conditions
Retrieval of the trust level of devices is requested

Post-conditions
-

Frequency of use
Hundreds of times per day

Non-functional requirements
None

Related use cases
UCG-13-02 Compute device trust level
Traceability to
Figure 1.1 - Detailed view of Cyber-Trust project

Example
The TMS ([A05]) receives a request from the intelligent UI user for the trust level of the DEV12345. The TMS ([A05]) extracts this information from the TrustDB ([A08]) and returns the device trust level.

Main scenario

Step	Actor	Action description
1	System	The retrieval of the trust level of devices is requested, specifying the criteria of devices to retrieve. These may be a list of devices (device ids) or an upper and a lower bound of trust levels.

Cyber-Trust Consortium. All rights reserved.

2	System	The system uses a query based on the specifications of the request and retrieves the requested trust levels from the TrustDB.
3	System	The requested information is returned.

UCG-13-02: Compute device trust level

Name: Compute device trust level

Description: The trust module collects all needed information [D5] and recomputes the trust level of the device [A05, D5].

Type: system use case

Primary Actor: <none; this use case is triggered from other use cases>

Supporting/Secondary actors: [A16] Network architecture and assets repository, [A05] Trust Management System

Stakeholders	Interest
TrustDB administrator ([A08])	Keep the contents of the TrustDB up to date
Intelligent UI user	Receive alerts on device trust changes, especially for devices whose trust has been demoted below some critical level
Infrastructure owner	Protect other devices from attacks coming from devices with low trust level

Pre-conditions
None

Trigger conditions
Changes to the device profile, including presence of new vulnerabilities, attack/tampering detection or remediation of an attack, are made; Trust level reports are received from peers; a network attack in which the device is involved is detected.

Post-conditions
Trust DB has been updated to reflect the new trust level of the device. The intelligent UI user is notified about devices with demoted or restored trust.

Frequency of use
Hundreds of times per day

Cyber-Trust Consortium. All rights reserved.

Non-functional requirements
None

Related use cases
UCG-15-02 Compute device risk level (extension, upon update of device trust level)

Traceability to
Figure 1.1 - Detailed view of Cyber-Trust project

Example
After a new broken access control vulnerability has been discovered for device type DT001 [D6], the device profile of device DEV12345 [D5] is updated in the device profile service to reflect this type of vulnerability. Then, the device profile repository ([A17]) informs the trust management ([A05]) module to commence recomputation of the trust level of DEV12345. The trust management module ([A05]) collects the device profile of DEV12345 [D5] , information about device-level security defenses of DEV12345 from the network architecture and assets repository (default passwords have been changed), a list of network-level security defenses ([A04]) from network architecture and assets repository (a port/service filtering firewall) [D5] and a trust assessment from peer trust management module ([A05, D5]) regarding the trust level of DEV12345. The IRS is also queried whether DEV12345 is involved in a current attack [D5, D6], and replies negatively. All this information is used to compute the new trust level of DEV12345 [D5], which is found to be 0.25. Since this is lower than the “Critical’ threshold, the intelligent UI user is notified accordingly [D5].

Main scenario

Step	Actor	Action description
1	System	The device trust level precomputation is triggered
2	System	The system retrieves from the device profile repository the data regarding the device health. This may include detailed information, including tampering of critical files, OS and firmware, device vulnerabilities and relevant technical impacts, as well as network behaviour. Alternatively, this would be a device self-assessment of its own trust level.
3	System	The system requests from the Network architecture and assets repository data regarding the device-level security defenses applicable on the examined device.
4	Network architecture and assets repository	The Network architecture and assets repository returns the requested data.

Cyber-Trust Consortium. All rights reserved.

5	System	The system requests from the Network architecture and assets repository data regarding the network-level security defenses applicable on the examined device.
6	Network architecture and assets repository	The Network architecture and assets repository returns the requested data.
7	System	The system retrieves from the Trust DB information about the current device trust level and the method that has been used to set it (manually vs. computed).
8	System	The system, based on the collected information, computes the new device trust level and stores it in the Trust DB.
9	System	The system retrieves settings regarding rules for notifying the intelligent UI user notifications upon device trust change
10	System	The overall trust level is computed.

Extension scenarios

After step 7	Actor	Retrieve information about the device trust level from Peer trust management systems *Condition: Peer trust management systems are registered*
1	System	The system requests from Peer trust management systems information about the trust level of the device
2	Peer trust management systems	The peer trust management systems return the requested data.

After step 9	Actor	Notify the intelligent UI user about the trust change *Condition:* The criteria for notifying the intelligent UI user are met
1	System	The system notifies the intelligent UI user regarding the new device trust level

UCG-14-01: Update device critical OS files [D5] /vulnerabilities

Name: Update device critical OS files [D5] /vulnerabilities

Description: In case a legitimate update is performed on the OS, firmware or any device critical files [D5], key device parameters are recalculated and updated to the central database [A07]. Then the process of detecting vulnerabilities is also performed [A04].

Type: System Use case

Primary Actor: [P2] A Smart Device owner

Cyber-Trust Consortium. All rights reserved.

Supporting/Secondary actors: [P1] Smart Home Owner, [O2] ISP, [O4] IoT SP

Stakeholders	Interest
Smart Device Agents [A12]	The smart device agent [A12] is responsible for the monitoring of device[A03] OS files [D5] / vulnerabilities
Cyber-defense Service [A04]	Detection of suspicious content triggers backend services for threat detection and mitigation.
Monitoring Service [A03]	The monitoring of device [A03] critical OS files [D5] and host vulnerabilities constitute device monitoring [A03] activities; Abnormal activity on device profiling

Pre-conditions
The monitored device is Cyber-Trust eligible and the smart device agent [A12] is activated.

Trigger conditions
Smart device agent [A12] is activated

Post-conditions
The intelligent UI and backend services are triggered for DPI analysis.

Frequency of use
Continuous operation

Non-functional requirements
None

Related use cases
UCG-07-01 Checking Device Patching Status UCG-07-02 Host based Vulnerability Scanning UCG-14-01 Update device critical OS files/vulnerabilities

Traceability to
Figure 1.1 - Detailed view of Cyber-Trust project

Example

Cyber-Trust Consortium. All rights reserved.

A Cyber-Trust enabled device is active and connected to the Cyber-Trust user profile. Upon registration of the device to Cyber-Trust [A06], information related to the type, make and characteristics of the device are provided. The Cyber-Trust device [A06] repository system interfaces with the patch database and the MUD services and therefore instructs the Cyber-Trust device agent [A06] on the critical OS files [D5] and vulnerabilities the device is susceptible. The indicated files are continuously monitored, while the relevant rules are set up to allow scanning for vulnerabilities [A04]. A patch becomes available and the Patching Database prompts for the updating of the device with the new patch. Upon the completion of this operation, the list of critical OS files [D5] and vulnerabilities are updated to match the characteristics of the new patch.

Main scenario

Step	Actor	Action description
1	System	A patch becomes available and the Patching Database prompts for the updating of the device with the new patch,
2	Cyber-Trust User	The Cyber-Trust end user is prompted to update their device through the UI portal.
3	Smart Device Agent [A12]	An image of the device firmware is secured and stored for future reference
4	System	Automated firmware updating is triggered by the device information repository
5	System	The device information record is updated to contain the current device information
6	Smart Device Agent [A12]	The smart device agent [A12] checks the integrity of the installed firmware

Extension scenarios

<4>a	Actor	The device does not support for automated firmware updating
1	Cyber-Trust User	The user is prompted to manually install the new patch.
2	Cyber-Trust User	The user confirms the patch update

UCG-14-02: Manage available patch databases

Name: Manage available patch databases

Description: For each type of registered device [A06] the Patch database contains information related to the latest security fixes of the firmware as well as the relevant binaries. Hash information is also securely stored [A02] to ensure the integrity of the vanilla patch versions.

Cyber-Trust Consortium. All rights reserved.

Type: System Use case

Primary Actor: System

Supporting/Secondary actors: [O6] Smart Device Manufacturer

Stakeholders	Interest
Cyber-defense Service [A04]	Detection of suspicious content triggers backend services for threat detection and mitigation.
Smart Device Agents [A12]	The smart device agent [A12] is responsible for the monitoring of device [A03] related aspects.

Pre-conditions
Available information on current patching status and updates need to be available by the manufacturer or firmware provider.

Trigger conditions
Whenever new information become available by the manufacturer or firmware provider and when new devices are registered to the Cyber-Trust infrastructure.

Post-conditions

Frequency of use
Dependent on the trigger

Non-functional requirements

Related use cases
UCG-09-01 Monitor device critical OS files [D5] /vulnerabilities UCG-07-01: Check device patching status UCG-17-01 Remediate Device

Traceability to

Cyber-Trust Consortium. All rights reserved.

Example
A Cyber-Trust enabled device is actively monitored [A03] with a healthy status in the visualisation portal. The MUD service indicates that a new security patch has been released. The patching database retrieves the new binary and hash information and register this to the blockchain as well. The new entry is added to the patch database, a read only database where no Cyber-Trust user is able to alter any information.

Main scenario

Step	Actor	Action description
1	External Resource	The MUD service indicates that a new security patch has been released.
2	Patch Database	The patching database retrieves the new binary and hash information
3	DLT[A02]	The new data are registered on the blockchain
4	Patch Database	The new entry is added to the patch database

UCG-14-03: Curate mitigation policy database

Name: Curate Mitigation Policy Database

Description: Trust DB administrator[O1], curates mitigation policy database; a new class of products for Smart Homes is released, namely smart door locks.

Type: System Use Case

Primary Actor: TrustDB administrator [O1]

Supporting/Secondary actors: -[A08] TrustDB Admin Module, System

Stakeholders	Interest
TrustDB administrator [O1]	Keep TrustDB up to date

Pre-conditions
Trust DB administrator is logged into the Cyber Trust system

Trigger conditions
New Device is released

Post-conditions
TrustDB [A08] has been updated to reflect the new health status of the device.

Frequency of use

Cyber-Trust Consortium. All rights reserved.

Multiple times per day

Non-functional requirements
None

Related use cases
UCG-04-03

Traceability to
Figure 1.1 - Detailed view of Cyber-Trust project

Example
John, a Trust DB administrator noticed a new smart door locks is released, he scheduled a meeting with other security officers and they conclude that even medium-level vulnerabilities for this class of devices should be considered as critical, because if they are exploited they can lead to either uncontrolled access to the area they protect or inability to access the area. To this end, John curates the mitigation policy database to enter a policy rule that reflects the decision reached.

Main scenario

Step	Actor	Action description
1	Trust DB administrator [O1]	The Trust DB administrator [O1] access the Trust DB and selects the “Find device” functionality.
2	System	The system presents a form to allow the Trust DB administrator to enter search criteria.
3	Trust DB administrator [O1]	The Trust DB administrator [O1] enters the search criteria and submits the form.
4	System	The system retrieves from the Trust DB device records that match the criteria.
5	System	The system presents the device information to the Trust DB administrator.
6	Trust DB administrator [O1]	The Trust DB administrator [O1] selects the device to be updated and submits this information.
7	System	The system presents a detailed record of the device trust status and appropriate controls to allow the Trust DB administrator to enter a policy rule.

Cyber-Trust Consortium. All rights reserved.

8	Trust DB administrator [O1]	The Trust DB administrator enters a policy rule; additional information may be entered to document the reason for adding this policy rule.
9	Trust DB administrator [O1]	The Trust DB administrator submits the information.
10	System	The system validates the completeness and validity of the information.
11	System	The system updates the Trust DB[A08] and registers additional information in the device history.
12	System	The system informs the Trust DB administrator that the policy has been added.

Extension scenarios

After step 4	Actor	No device matches the criteria
1	System	The system notifies the user that no devices were retrieved
2	System	Control returns to step #2

After step 10	Actor	The information submitted by the user is incomplete/erroneous
1	System	The system informs the Trust DB administrator regarding the errors or omissions
2	System	Control returns to step #8

*a	Actor	The Trust DB administrator cancels the process (at any step)
1	Trust DB administrator [O1]	The Trust DB administrator [O1] cancels the process
2	System	The system terminates the procedure and destroys the Trust DB management form

UCG-14-04: Curate forensic evidence database

Name: Curate forensic evidence database

Description: The forensic evidences are stored in the Forensic Evidences eVDB (off-chain) [A07] while the hash values of these data, time stamps regarding the data, information regarding the owner of the data etc. will be stored in the DLT (on-chain) [A02]. Thus, this UC will show how the forensic data stored in the evidence DB will be annotated, organised and presented in the blockchain (e.g. hashes of the actual evidences, chain of custody etc.).

Cyber-Trust Consortium. All rights reserved.

Type: Business use case

Primary Actor: [O2] ISP

Supporting/Secondary actors: [A16] Network architecture and assets repository, [A01] Visualisation Portal, Peer trust management systems [A05], Intelligent UI, [A01] Advanced 2D/3D visualization, [A02] DLT Service, [A07] eVDB Admin Module, System.

Stakeholders	Interest
DLT Service [A02]	Store the forensic evidences.
Intelligent UI	Receive alerts on device risk changes, especially for devices risk level is above some critical level
Infrastructure owner	Protect other devices from attacks coming from devices with high risk level

Pre-conditions
Data is stored in the Forensic Evidence eVDB; The ISP stored the hashes, and all the relevant information of the data in the DLT.

Trigger conditions
N/A

Post-conditions
Forensic is stored off-chain and metadata have been sent to UCG-14-06

Frequency of use
N/A

Non-functional requirements
Policy; National Legislation;

Related use cases
UCG-02-02; UCG-02-01; UCG-01-01-01; UCG-11-01; UCG-11-02; UCG-14-06; UCG-12-02; UCG-12-05;

Traceability to
Figure 1.1 - Detailed view of Cyber-Trust project

Cyber-Trust Consortium. All rights reserved.

Example
After a device attack the society ISP (Actor O2) stores off-chain Forensic Evidence DB the data they collect during the attack. ISP will also store data on the DLT [A02] to refer the data stored off-chain.

Main scenario

Step	Actor	Action description
1	ISP	The actor stores data on its Forensic database.
2	System	The system computes the hash of the metadata relative to the data inserted in Step #1. The system also includes helpful information for the user of the DLT like the timestamp of the attack, the type of the device.
3	System	

UCG-14-05: Store trusted logs.

Name: Store trusted logs.

Description: Describe the steps involved into storing devices' logs into the DLT[A02].

Type: System use case

Primary Actor: System

Supporting/Secondary actors:

Stakeholders	Interest
System	Take consideration of new logs and add them inside the DLT.

Pre-conditions
A user has already registered itself and register one or more device. The device is active and have the permission given by the user to write into the DLT.

Trigger conditions
The device writes logs.

Post-conditions
The new logs are saved inside the DLT.

Minimum guarantees
A back-end rules triggered by the production of logs by one of the devices

Cyber-Trust Consortium. All rights reserved.

Frequency of use
Once a device produces trusted logs.

Related use **cases**
UCG-12-03,UCG-12-01,UCG-12-05

Traceability to
Figure 1.1 - Detailed view of Cyber-Trust project

Example
A home security system is being deactivated. It writes this action to its logs [A02]. The platform is being notify of the presence of the logs. The logs are being saved.

Main scenario

Step	Actor	Action description
1	System	The system is being notified of new logs for a registered device on the platform.
2	System	The device sends its new logs to the platform.
3	System	The platform saves incrementally the new logs

UCG-14-06: Store Forensic evidence.

Name: Store Forensic evidence.

Description: Describe the steps involved in adding data into the DLT [A02] after that entries have been stored off-chain on the Forensic eVDB [A07]

Type: System use case

Primary Actor:

Supporting/Secondary actors: None

Stakeholders	Interest
System	System activate the procedure to store Forensic evidence in the database

Pre-conditions
A new forensic entry has been added off-chain.

Trigger conditions

Cyber-Trust Consortium. All rights reserved.

UCG-14-04

Post-conditions
Data of forensic have been added on the memory pool waiting to be added on the DLT

Minimum guarantees
A back-end rule

Frequency of use
Occasionally

Related use cases
UCG-14-04, UCG-12-04

Traceability to
Figure 1.1 - Detailed view of Cyber-Trust project

Example
The system receive metadata relative to a new forensic add off-chain. The system begins the procedure of storing this metadata in the DLT [A02] This metadata will be available after the block have been validated and propagated inside the DLT.

Main scenario

Step	Actor	Action
1	System	Forensic have been stored off-chain. A back-end rule triggers this UC. The owner of the off-chain data sends the meta-data relative to the data he has just added off-chain.
2	System	The system places the given data to an unconfirmed block of evidence. It informs the actor which add data off-chain of the success of the operation.

UCG-14-07: Notify about updates and security-related issues

Name: Notify about updates and security-related issues.

Cyber-Trust Consortium. All rights reserved.

Description: The device profile is matched against the contents of the eVDB [A07] to retrieve vulnerabilities (and other related information) that pertain the device [D1, D5, D6]

Type: business use case

Primary Actors: [P1, P2] user, [O2] Security officer (Tom) working at an ISP – telecom operator [O1] Cyber-Trust Service Provider CISO (Bob), [O1] Vulnerability assessment expert (John), [O2] Security officer working at the SOC of the telecom operator (Sarah)

Supporting/Secondary actors: -

Stakeholders	Interest
Intelligent UI user	Receive information according to user's profile

Pre-conditions
User is logged into the Cyber-Trust system The profile of the users is inserted EVDB is properly populated and validated

Trigger conditions
User request

Post-conditions
None

Frequency of use
Many times, per day.

Non-functional requirements
None

Related use cases
UCG-06-04 Query and retrieve information from eVDB UCG-02-05 Register to the eVDB sharing service UCG-16-04 Crawl the clear/deep/dark web and update the eVDB UCG-06-05 Review and validate eVDB entries UCG-19-04 Tune the crawling parameters and evaluate existing seeds UCG-06-06 Provide feedback/rating on sources of vulnerabilities UCG-14-08 Match device profile with eVDB contents

Cyber-Trust Consortium. All rights reserved.

Traceability to
Figure 1.1 - Detailed view of Cyber-Trust project

Example
[P1, P2] user, [O2] Security officer (Tom) working at an ISP – telecom operator, [O1] Cyber-Trust Service Provider CISO (Bob), [O1] Vulnerability assessment expert (John), [O2] Security officer working at the SOC of the telecom operator (Sarah), receive information whenever a new intelligence is entered into the eVDB ([A07]) that matches their profiles [D1, D5, D6].

Main scenario

Step	Actor	Action description
1	System	The system receives new information in the eVDB or a device profile is updated.
2	System	The system identifies new matches between the eVDB and the device profiles.
3	System	The system identifies the users and the security officers that monitor the devices
4	System	The system notifies the corresponding users.

UCG-14-08: Match device profile with eVDB content

Name: Match device profile with eVDB content

Description: The device profile is matched against the contents of the eVDB [A07] to retrieve vulnerabilities (and other related information) that pertain the device [D5, D6].

Type: business use case

Primary Actor: <none; this use case is triggered from other use cases>

Supporting/Secondary actors: [A17] Device profile repository, [A09] eVDB Sharing Service

Stakeholders	Interest
Intelligent UI user	Access eVDB information
Infrastructure owner	Ensure cyber-threat intelligence sharing to the different modules of the Cyber-Trust infrastructure

Pre-conditions
None

Cyber-Trust Consortium. All rights reserved.

Trigger conditions
System request

Post-conditions
None

Frequency of use
Thousands of times per day

Non-functional requirements
None

Related use cases
UCG-06-04 Query and retrieve information from eVDB UCG-02-05 Register to the eVDB sharing service UCG-14-07 Notify about updates and security-related issues

Traceability to
Figure 1.1 - Detailed view of Cyber-Trust project

Example
A Cyber-Trust user buys a new smart device and before even physically installing it in her home, she decides to use Cyber-Trust's eVDB [A07, D5, D6**]** to search for any security issues that pertain to her newly acquired device. She uses an appropriate user interface to search ([A09, D5, D6]) the eVDB [A07] to do so the system issues a request to match the device profile and additional match criteria specified by the user against the contents of the eVDB [A07, D5, D6] at the moment, nothing comes up. She then decides to subscribe to the publish/subscribe service that is offered by the Cyber-Trust platform to be promptly notified about any updates and security-related issues that may rise in the future. She is able to tune the information she would like to receive from Cyber-Trust platform (e.g., type of updates/alerts, desired level of alert confidence, desired impact threshold). While on operation, the Cyber-Threat discovery module surfaces information about a new zero-day vulnerability, and a new request to match the new vulnerability against the device profiles that are registered [A06, D5, D6] in the publish/subscribe module is generated.

Main scenario

Step	Actor	Action description
1	System	A request to match a device profile against the contents of the eVDB arrives. The request contains the match criteria.

Cyber-Trust Consortium. All rights reserved.

2	System	The system requests from the device profile repository the data (such as the OS and firmware) regarding the device profile.
3	Device profile repository	The device profile repository returns the requested data.
4	System	The system, based on the device profile, the criteria specified, and the information stored in the eVDB computes the matching.
5	System	The system returns the result of the computation to the module that triggered the use case.
6	System	The system terminates the procedure.

Extension scenarios

3a	Actor	No data are available for the device
1	Device profile repo-sitory	The device profile repository notifies that there are no data that match the requested device profile.
2	System	Control goes to step #6

5a	Actor	No eVDB entries match the device profile and specified criteria
1	System	The system notifies the module that triggered the use case that no eVDB entries matched the specified profile and criteria.
2	System	Control goes to step #6

UCG-15-01: Compute cyber-attack graphical security model

Name: Compute cyber-attack graphical security model

Description: Create an attack graph that presents how *exploits* relate to *security conditions.* In doing so, information about the exploits [D4, D5] is retrieved by the eVDB [A07].

Type: System type

Primary Actor: [O2] Security officer

Supporting/Secondary actors: [A09] eVDB Sharing Service, [P3] Cyber-attacker, [A16] Network architecture and assets repository.

Stakeholders	Interest
Security officer [02]	Acquires a clear view of the possible attack paths an attacker could follow.
iIRS [A13]	Takes the cyber-attack graphical security model or an abstraction of it, as input upon which, the decision-making process will take place.

Cyber-Trust Consortium. All rights reserved.

Pre-conditions
Knowledge of the network configuration, security conditions and their relations, as well as, the available exploits, the network configuration is updated and reflects the current situation.

Trigger conditions
Need for security analysis; Change in network configuration, security conditions or their relations and exploits.

Post-conditions
Creation of the cyber-attack graphical security model.

Frequency of use
Initially for the security analysis task. If network configuration changes. If there is a change in security conditions and/or in their relations. If a new exploit is discovered.

Non-functional requirements
None

Related use cases
UCG-15-02 Compute device risk level UCG-13-01 Retrieve trust level from TMS UCG-06-04 Query and retrieve information from eVDB UCG-14-08 Match device profile with eVDB contents UCG-13-02 Compute device trust level UCG-04-03 Define mitigation actions' impact

Traceability to
Figure 1.1 - Detailed view of Cyber-Trust project

Example
Security officer ([O2]) wants to create the cyber-attack graphical security model related to Mary's network. She acquires the system security conditions and their relations, along with the exploits [D4, D5] (consults the eVDB ([A07]) for obtaining this information) which compromise these security conditions. After that, Sarah ([O2]) has two options. The first option is to give as input the aforementioned information to a cyber-

Cyber-Trust Consortium. All rights reserved.

attack graphical security model engine. The cyber-attack graphical security model tool provides as output the attack model which is required by the iIRS ([A13]) to operate. Sarah's ([O2]) second option is to create the cyber-attack graphical security model manually. However, this option applies only to small-scale networks.

Main scenario

Step	Actor	Action description
1	Security officer	The security officer initiates the cyber-attack graphical security model computation
2	System	The system retrieves the network configuration from the Network architecture and assets repository
3	System	The system displays a user interface for allowing the security officer to enter and document network attributes
4	Security officer	The security officer enters the network attributes through the user interface and submits the information to the system
5	System	The system accepts and validates the network attributes
6	System	The system displays a user interface for allowing the security officer to enter and document the security conditions
7	Security officer	The security officer enters the security conditions through the user interface and submits the information to the system
8	System	The system accepts and validates the security conditions
9	System	The system displays a user interface for allowing the security officer to enter and document the relations between security conditions
10	Security officer	The security officer enters the relations between security conditions through the user interface and submits the information to the system
11	System	The system accepts and validates the relations between security conditions
12	System	The system retrieves available exploits from the eVDB.
13	Security officer	The security officer uses the available graphical security tool to build representation of graphical security model.

Cyber-Trust Consortium. All rights reserved.

14	System	The selected tool takes as input the security conditions and their relations along with the exploits (if admissible) and creates the graphical model.
15	System	The system validates and stores the cyber-attack graphical security model.
16	System	Forward GrSM to iIRS and iIRS stores the GrSM.

Extension scenarios

5a	Actor	Invalid or incomplete network attributes Condition: network attributes provided by the user are incomplete or invalid
1	System	The system displays an appropriate error message
2	System	Control is returned to step 6

8a	Actor	Invalid or incomplete security conditions Condition: security conditions provided by the user are incomplete or invalid
1	System	The system displays an appropriate error message
2	System	Control is returned to step 9

13a	Actor	Create the graphical security model automatically Condition: the security officer has chosen a automated construction of the cyber-attack graphical security model
1	System	The system presents a user interface to allow the security officer to create the cyber-attack graphical security model.
2	System	The system creates the cyber-attack graphical security model automatically connecting the security conditions and exploits and submits the information
3	System	The system validates and stores the cyber-attack graphical security model.

UCG-15-02: Compute device risk level

Name: Compute device risk level

Description: The TMS computes a new value for the risk level of a device [D5]. Information about the current device trust level, the current status of network attacks and network traffic related to the device (as

Cyber-Trust Consortium. All rights reserved.

compared with the baseline), the device vulnerabilities and their exploitability, the device health level and views of peer-level TMSs [A05] are taken into account [D5, D6].

Type: system use case

Primary Actor: <none; this use case is triggered from other use cases>

Supporting/Secondary actors: [A16] Network architecture and assets repository, [A05] Trust Management System

Stakeholders	Interest
TrustDB administrator [A08]	Keep the contents of the TrustDB up to date
Intelligent UI user; [O2] [P1, P2] user	Receive alerts on device risk changes, especially for devices risk level is above some critical level
[P1, P2] user, depending on the context	Protect other devices from attacks coming from devices with high risk level

Pre-conditions
None

Trigger conditions
Changes to the device trust level are made; Trust level reports are received from peers; A network attack in which the device is involved is detected.

Post-conditions
Trust DB has been updated to reflect the new risk level of the device. The intelligent UI user is notified about devices whose risk has been significantly elevated or demoted.

Frequency of use
Hundreds of times per day

Non-functional requirements
None

Related use cases
UCG-13-02 Compute device trust level

Traceability to
Figure 1.1 - Detailed view of Cyber-Trust project

Cyber-Trust Consortium. All rights reserved.

Example
After computing a new value for the trust level of device DEV12345 [A05, D5], the risk level for DEV12345 is reassessed. The trust management module ([A05]) collects the current device trust level from the TrustDB ([A08, D5]) and the peer trust management module TMS001 ([A05, D5]), the device's health level and its known vulnerabilities and their exploitability level from the device profile repository ([A17, D5]), data regarding the security controls that are in effect for the device from the Network architecture and assets repository ([A16, D5]), while data regarding the network architecture and the proximity of the device with other devices are again sourced from the Network architecture and assets repository ([A16, D5]). The IRS ([A13]) is queried whether there have been anomalous traffic patterns detected relating to this device and if the device is believed to be part of an ongoing attack ([D6]). The above information is used to compute the new risk level ([A05, D5]), which is found to be 0.82. Since this is higher than the "Critical" threshold, the intelligent UI user ([P1, P2]) depending on the context; additionally, [O2]) is notified accordingly.

Main scenario

Step	Actor	Action description
1	System	The device risk level recomputation is triggered
2	System	The system retrieves from the TrustDB the current device trust level.
3	System	The System requests from the Network architecture and assets repository information about other devices that can be attacked from the current device; the focus of this query is devices that are inside the same network perimeter and thus are not protected by active network-level security defenses (or have a low level of protection).
4	Network architecture and assets repository	The Network architecture and assets repository returns the requested data.
5	System	The system retrieves from the device profile repository information about information about the device whose risk level is assessed; this includes device vulnerabilities, their exploitability level and technical impact, the health status of the device, and the current network traffic & network traffic baseline.
6	System	The system retrieves from the device profile repository information about devices that could be attacked from the current device; this includes device vulnerabilities, their exploitability level and technical impact.
7	System	The TMS requests from the Network architecture and assets repository information about the network defenses that apply to the device whose risk level is assessed.

Cyber-Trust Consortium. All rights reserved.

8	Network architecture and assets repository	The Network architecture and assets repository returns the requested information.
9	System	The system requests from the network architecture and assets repository information about the device under investigation, as well as for other devices that can be attacked from the current device. For each device, this information includes the value of services and data that the device hosts and the device-level security defenses that apply to the device.
10	Network architecture and assets repository	The assets repository returns the requested information.
11	System	The system computes the device risk level
12	System	The system retrieves settings regarding the rules for notifying the intelligent UI user upon device risk level change.

Extension scenarios

After step 7		**Retrieve information about the device trust level from Peer trust management systems** **Condition: Peer trust management systems are registered**
1	System	The system requests from Peer trust management systems information about the trust level of the device
2	Peer trust management systems	The peer trust management systems return the requested data.

After step 9		**Communicate to the intelligent UI a notification about the risk level change** **Condition: The criteria for notifying the intelligent UI user are met**
1	System	The system notifies the intelligent UI user regarding the new device trust level

UCG-15-03: Compute attack's likelihood and success probability

Name: Compute attack's likelihood and success probability

Description: The Security officer consults the eVDB ([A07]) to compute the attack's likelihood and success probabilities. This information [D2, D4, D5] is vital for the iIRS [A13] to compute the best mitigation actions, because of the stochastic nature of the decision-making process of the iIRS [A13].

Type: System type

Primary Actor: [O2] Security officer (Sarah)

Cyber-Trust Consortium. All rights reserved.

Supporting/Secondary actors: [A09] eVDB Sharing Service, [A13] iIRS

Stakeholders	Interest
Security officer [02]	More accurate attack model and as a result better defense actions applied by the iIRS.

Pre-conditions
Knowledge of the cyber-network structure and configuration. Access to the eVDB.

Trigger conditions
Need for security analysis, recommendation of defence strategies, automated defence; Change of network configuration; Need of addition/removal of a security condition or change in a relation among them; A new exploit is discovered.

Post-conditions
Accurate attack models and as a result better defense action.

Frequency of use
Initially for the security analysis task. Whenever the network configuration changes. Whenever there is a change in security conditions and/or in their relations. Whenever a new exploit is discovered.

Non-functional requirements
None

Related use cases
UCG-06-04 Query and retrieve information from eVDB UCG-14-08 Match device profile with eVDB contents UCG-18-05 Compute optimal intrusion response actions

Traceability to
Figure 1.1 - Detailed view of Cyber-Trust project

Example

Cyber-Trust Consortium. All rights reserved.

Security officer Sarah ([O2]) carefully analyses the information [D2, D4, D5] ([A09]) provided by the eVDB ([A07]) to assess the cyber-attacker's ([P3]) likelihood and success probability. Then, the dynamic system model which depends on the expected impact of attack actions and their success is updated and given as input to the iIRS ([A13]).

Main scenario

Step	Actor	Action description
1	Security officer	The security officer initiates computation of attack's likelihood and success probability
2	System	The system retrieves information about the available exploits and their scoring (CVSS) from the eVDB.
3	System	The system presents the retrieved information
4	Security officer	The security officer processes the presented information, assesses the cyber-attack's likelihood and success probability and computes new parameters for the system dynamics (i.e. state transition model, expected utility function)
5	System	The system displays an appropriate user interface for entering updated system dynamics parameters
6	Security officer	The security officer enters updated system dynamics and submits the information.
7	System	The system accepts and validates the submitted system dynamics parameters
8	System	The system forwards this information as input to the iIRS.

UCG-15-04: Compute a belief on current security status

Name: Compute a belief on current security status

Description: The iIRS [A13] uses the alerts provided by the intrusion detection system to update the belief it has about the system security state. The belief is a probability distribution over the possible security states, which are comprised of the system security conditions. These conditions denote system attributes (e.g. active services (and the associated vulnerabilities), network connectivity, trust relationships between hosts, and attacker privileges on hosts) and represent attacker's capabilities.

Type: System type

Primary Actor: [A13] iIRS

Supporting/Secondary actors: [A11] IDS, [O2] Security officer (Tom)

Stakeholders	Interest
iIRS [A13]	More accurate belief of the true system security state.

Cyber-Trust Consortium. All rights reserved.

Security officer	Knowledge of the system security state.

Pre-conditions
Knowledge of the cyber-network structure and configuration to define the state space. Operating IDS system.

Trigger conditions
Initially, when the system state is defined, and the initial belief is formed based on prior knowledge; Change of network configuration; Need of addition/removal of a security condition or change in a relation among them; An alert is generated by the intrusion detection system.

Post-conditions
A new belief over the system security state is formed.

Frequency of use
Initially for the security analysis task using prior knowledge on system security state; Periodically after the alert generation by the IDS.
Non-functional requirements
None

Related use cases
UCG-16-03 Receive intrusion detection system(s) alerts UCG-18-05 Compute optimal intrusion response actions

Traceability to
Figure 1.1 - Detailed view of Cyber-Trust project.

Example
During the course of an attack, alerts are being generated by the IDS ([A11]) and sent to the iIRS ([A13]). The iIRS ([A13]) uses its former knowledge on the system state and the newly generated alert to update the belief it possesses over the system security state. Optionally, the security officer ([O2]) Tom is informed about this change.

Main scenario

Step	Actor	Action description
1	iIRS [A13]	A security status belief update is triggered.

Cyber-Trust Consortium. All rights reserved.

2	iIRS [A13]	The iIRS retrieves alerts, information about the current belief, and data related to the graphical security model (vulnerabilities, exploits, etc.).
3	iIRS [A13]	The iIRS interprets the alerts and determines the set of exploits that could have caused them, possibly along with other information (e.g. the type of the attacker utilizing such exploits)
4	iIRS [A13]	Based on the collected information, the iIRS updates the belief over the system's current security state.
5	iIRS [A13]	The belief is updated.
6	iIRS [A13]	The belief is stored locally for future reference.

Extension scenarios

6a	Actor	Security officer notification Condition: security officer requires to be notified
1	iIRS [A13]	Informs the security officer about the new belief of the system security state.

UCG-16-01: Determine device firmware and software through remote detection

Name: Determine device firmware and software through remote detection

Description: A backend service runs between the device and central device profile database to identify device's firmware and software thereby building and updating the central database with all firmware. As a result, the system can be able to generate metrics such as vulnerability and trust.

Type: System Use case

Primary Actor: System

Supporting/Secondary actors: Smart Device Agent [A12]

Stakeholders	Interest
Trust Management System [A05]	The trust score of a device is heavily dependent on the integrity of its operating firmware.

Pre-conditions
Available information on current firmware status and updates need to be available by the manufacturer or firmware provider.

Trigger conditions
Firmware and software

Cyber-Trust Consortium. All rights reserved.

Post-conditions
Triggering of relevant services for the updating of the central device profile database.

Frequency of use
Dependent on the trigger

Non-functional requirements
None

Related use cases
UCG-09-01: Monitor device critical OS files/vulnerabilities UCG-07-01: Check device patching status UCG-07-03: Ensure Device firmware integrity

Traceability to
Figure 1.1 - Detailed view of Cyber-Trust project
Example
A Cyber-Trust enabled device is active and connected to the Cyber-Trust user profile [A17]. Upon registration of the device to Cyber-Trust [A06], information related to the type, make and characteristics of the device are provided. The Cyber-Trust device repository system interfaces with the patch database and the MUD services and therefore instructs the Cyber-Trust device agent[A06] on the critical OS files and vulnerabilities the device is susceptible. The indicated files are continuously monitored, while the relevant rules are set up to allow scanning for vulnerabilities.

Main scenario

Step	Actor	Action description
1	Smart Device Agent [A12]	The list of critical OS files and vulnerabilities related to the device type are retrieved from the Patch Database
2	Device Information Management System [A05]	The monitoring services [A03] continuously compare the hash information from the device's critical files and the values provided by the device information management system[A05].
3	System	The system continuously updates the central device profile database with new device's firmware.

Extension scenarios

Cyber-Trust Consortium. All rights reserved.

<#>a	Firmware detection fails	
1	System	The firmware check fails on a device
2	System	The device information management system [A05] is notified

UCG-16-02: Discover Network

Name: Discover Network

Description: The exploitation of the Cyber-Trust device profiles conjoined with location information to allow for support to visualization capabilities [A01], wither via dynamic (flow) or static (GID) graphs.

Type: System

Primary Actor: [A03] Monitoring Service

Supporting/Secondary actors: [A04] Cyber-defense Service, [A11] Smart Gateway Agent, [A12] Smart Device Agent

Stakeholders	Interest
System	Provides data for visualization

Pre-conditions
Monitoring Service is active, and network is live

Trigger conditions
Devices registered on the Cyber-Trust network

Post-conditions
Dynamic and static device visualization

Frequency of use
Continuous Operation

Non-functional requirements
None

Related use cases
UCG-04-01 Private IoT Device Profile Generation UCG-05-06 Visualize network traffic

Cyber-Trust Consortium. All rights reserved.

UCG-02-03 Register device into Cyber-Trust platform

Traceability to
Figure 1.1 - Detailed view of Cyber-Trust project

Example
Device profile generates the overall device picture, covering common IP, ports, traffic load, CPU and memory usage as well as the location of the device on the network (obscuring personal data of the owner). As part of this, the discover network capability acts as the flow meter for the device-connected network(s) to profile dynamic and static data for visualisation [A01].

Main scenario

Step	Actor	Action description
1	System	New device is registered on the network
2	Network Profiling	Flow meters installed on the HIDS and NIDS gather data
3	System	Network & Device Scans DB stores profile data

Extension scenarios

After step 1	Actor	The device is scanned for vulnerabilities
1	System	The system retrieves intelligence form the Enriched eVDB
2	System	The system locates the list of devices to be scanned
3	System	The System retrieves devices profile information
4	System	The System performs vendibility scan on the devices
5	System	The System issues a scan report to the security officer with the details of the vulnerability scan results.

UCG-16-03: Receive intrusion detection system(s) alerts

Name: Receive intrusion detection system(s) alerts

Description: In case of an attack discovery, or a false alarm event, the intrusion detection system is activated and generates alerts [D2, D4] and informs the iIRS [A13]. The iIRS evaluates the generated alerts in order to infer the true system security state, by considering the possible mis-detections and false alarms.

Type: System type

Primary Actor: [A11] Intrusion detection system (IDS)

Supporting/Secondary actors: [A13] iIRS, [P3] Cyber-attacker, [O2] Security officer

Stakeholders	Interest
iIRS [A13]	Forms a more accurate view of the true system security condition.

Cyber-Trust Consortium. All rights reserved.

Pre-conditions
Operating intrusion detection systems on smart gateway agents. Connectivity of these devices with the iIRS.

Trigger conditions
An attack is performed, and it is correctly detected; False alarm of the devices.

Post-conditions
The iIRS computes the probability distribution of the system security state.

Frequency of use
Periodically.

Non-functional requirements
None

Related use cases
UCG-08-02 Capture and classify network packets (DPI) UCG-18-03 Apply network security defense rule UCG-15-04 Compute a belief on current security status

Traceability to
Figure 1.1 - Detailed view of Cyber-Trust project

Example
A cyber-attacker [P3) is attempting to compromise multiple devices with firmware vulnerabilities in the network. While the bot is trying to replicate itself in the network through telnet/FTP/SSH default logins such attempts are successfully detected by the IDS [A11] and a specific alert is generated [D2, D4]. This alert is sent to the iIRS [A13].

Main scenario

Step	Actor	Action description
1	Intrusion detection system	The Intrusion detection system detects an attack and notifies the Cyber-Trust system

Cyber-Trust Consortium. All rights reserved.

2	System	The system forwards this information to the iIRS for further handling
3	System	The system creates a notification to be displayed to the intelligent UI user

UCG-16-04: Identify and prioritize cyber-threats.

Name: Identify and prioritize cyber-threats.

Description: The cyber-threats that affect the protected assets [A05], taking into account the vulnerability characteristics (including technical impact, exploitability etc.), the business impact/value of the assets, and the characteristics of the threat agents. Finally, the threats are ordered in descending order of their score. The complete list of threats, the top-K ones or the threats surpassing a risk threshold may be returned, depending on the parameters within the request.

Type: system use case

Primary Actor: <none; this use case is triggered from other use cases>

Supporting/Secondary actors: -

Stakeholders	Interest
Security officer [02]	Obtain a view of threat levels for the infrastructure.
Infrastructure owner [A04]	Allocate resources for threat mitigation to the most appropriate targets.

Pre-conditions
None

Trigger conditions
Retrieval of cyber threat identification and prioritization is requested.

Post-conditions
-

Frequency of use
Few to tens of times per day.

Non-functional requirements
None

Related use cases

Cyber-Trust Consortium. All rights reserved.

UCG-15-02 Compute device risk level

Traceability to
Figure 1.1 - Detailed view of Cyber-Trust project

Example
Cyber threat identification and prioritization is requested. The system retrieves from the device profile repository [A17] the profiles of devices [D5]; the vulnerable devices are a surveillance camera CAM001 is which has a data stream leakage vulnerability exploitable from devices within the network perimeter, and a Smart TV, STV002, which has a device takeover vulnerability, exploitable from any location [D5]. No device-level security defenses [A04] are identified for these devices. The impact of Smart TV takeover is rated as medium, while the impact of camera data stream leakage is rated as severe [D5]. No peer-level TMSs [A05] are found to be registered. Taking the above into account, the system computes a priority of 0.8 [D5] for the “Exploitation of the STV002 takeover vulnerability” threat and a priority of 0.67 [D5] for the “Exploitation of the CAM001” threat; the “Exploitation of the STV002 takeover vulnerability” reaches a higher score since (a) it directly affects STV002 and (b) once this threat is realized, CAM001 can also be attacked.

Main scenario

Step	Actor	Action description
2	System	The system retrieves from the device profile repository the profiles of devices, including the vulnerabilities for each device, their technical impact and their exploitability.
3	System	The system requests from the Network architecture and assets repository the information about the value of the services that the device hosts and the device-level security defenses that apply to each device.
4	Network architecture and assets repository	The Network architecture and assets repository returns the requested information.
5	System	The system requests from the Network architecture and assets repository the security defenses that apply to each device.
6	Network architecture and assets repository	The Network architecture and assets repository returns the requested information.
7	System	The system computes the risk level that each threat poses to the infrastructure directly, considering the potential for direct attacks from the attack sources (external network; untrusted insiders; currently compromised devices within the network perimeter).
8	System	The system computes the risk level that each threat poses indirectly, considering the potential for attackers to exploit successful threat realizations to attack other devices/assets;

Cyber-Trust Consortium. All rights reserved.

		this particularly concerns the potential of attackers to firstly compromise devices within the network perimeter, and then use these devices to attack other devices within the network perimeter that either have a higher business value/impact or can be used for the formation of botnet armies.
9	System	The system synthesizes a comprehensive score for each risk, taking into account both direct and indirect risk levels associated with the threat, formulating the result list
10	System	The system returns the list of risks coupled with their ratings.

Extension scenarios

After step 9		Prune threat list result by risk threshold Condition: A risk threshold is specified in the request
1	System	The system removes from the result list threats whose risk level is lower than the designated threshold

After step 9		Prune threat list result by number of results Condition: A specification of the maximum number of threats to be returned is included in the request
1	System	The system retains on the result list only the top-K threats, with respect to their risk level.

UCG-16-05: Crawl the clear/deep/dark web and update the eVDB

Name: Crawl the clear/deep/dark web and update the eVDB

Description: The Cyber-Trust system continuously crawls popular social media streams, popular security-related websites and deep/dark web forums and marketplaces [A10, D6]. Cyber-Trust searches for cyber-threat information including zero-day vulnerabilities, exploits, signatures, executables, and other related information. The collected data will update the eVDB [A07, D6]

Type: system use case

Primary Actor: [O1] Cyber-Trust Service Provider CISO (Bob)

Supporting/Secondary actors: [P1, P2] user, [O2] Security officer (Tom) working at an ISP – telecom operator [O1] Vulnerability assessment expert (John), [O2] Security officer working at the SOC of the telecom operator (Sarah), [A09] eVDB Sharing Service

Stakeholders	Interest
Intelligent UI user	Receive information according to user's profile

Pre-conditions
None

Cyber-Trust Consortium. All rights reserved.

Trigger conditions
None

Post-conditions
The eVDB is updated.

Frequency of use
Two to four times per day.

Non-functional requirements
None

Related use cases
UCG-06-04 Query and retrieve information from eVDB UCG-02-05 Register to the eVDB sharing service UCG-14-07 Notify about updates and security-related issues UCG-06-05 Review and validate eVDB entries UCG-19-04 Tune the crawling parameters and evaluate existing seeds UCG-06-06 Provide feedback/rating on sources of vulnerabilities UCG-14-08 Match device profile with eVDB contents

Traceability to
Figure 1.1 - Detailed view of Cyber-Trust project

Example
The Cyber-Trust system continuously monitors popular social media streams, popular security-related websites and deep/dark web forums and marketplaces [D6]. Cyber-Trust searches for cyber-threat information including zero-day vulnerabilities, exploits, signatures, executables, and other related information [D6]. The collected data will be inserted into the eVDB ([A07]). To this end, Cyber-Trust uses an ensemble of state-of-the-art data and knowledge processing and machine learning techniques to identify the (clear/deep/dark) web pages that should be crawled ([A10]) and to extract and contextualize all relevant threat information. The collected data may refer to a new threat that has to be inserted into the eVDB ([A07]), or new information about known threats (e.g., exploits) that will update the eVDB entries and enrich the stored intelligence. New information is initially added to the eVDB with a low level of confidence in the existence of the vulnerability (as it has possibly not been validated yet by security experts) and the credibility of the known technical details [UCG-06-05]. The function of the cyber-threat discovery module is supervised by an IT expert (Bob [O1]) that is responsible to add, annotate, and approve

Cyber-Trust Consortium. All rights reserved.

the crawling of new seeds [A10] (i.e., websites of interest), tune the crawling parameters that enable their discovery, and evaluates existing seeds in terms of usefulness [UCG-19-04].

Main scenario

Step	Actor	Action description
1	System	The system read the available seeds.
2	System	The system crawls the web using the seeds as starting point.
3	System	The system extends the search using state-of-the-art methods.
4	System	The system pinpoints new or altered pages.
5	System	The system processes the pinpointed pages using state-of-the-art Machine Learning and Knowledge Extraction methods.
6	System	The system updates existing and adds new information into the eVDB.

UCG-17-01: Remediate Device

Name: Remediate Device

Description: This use case is responsible for restoring a device to a healthy state. Remediation takes place once the detection of an attack is confirmed meaning that either abnormal device behaviour is detected or the existence of fraudulent content is identified. The remediation process involved the isolation of affected files and their recovery to a previous healthy state or the notification of the end user about advised actions

Type: System Use case

Primary Actor: [P2] A Smart Device owner

Supporting/Secondary actors: [P1] Smart Home Owner, [O2] ISP, [O4] IoT SP, [O6] Smart Device Manufacturer

Stakeholders	Interest
Cyber-Defense Service [A04]	Cyber-Defense Service [A04] work collaboratively with the remediation services to effectively protect the monitored device..
Visualization Portal [A01]	The status of remediation of a device is displayed on the portal

Pre-conditions
A threat had been identified, the remediation policy for the device’s restoration might occur due to device monitoring [A03] aspects or mitigation policies emerging as the result of decision making at network level.

Trigger conditions

Cyber-Trust Consortium. All rights reserved.

Post-conditions
The remediation policy on the device may result in the isolation of the device from the remaining network. In the case of remediation, the updating of device critical OS files [D5] and patching information might be required.

Minimum guarantees

Frequency of use
Ad Hoc

Non-functional requirements

Related use cases
UCG-09-01 Monitor device critical OS files [D5] / vulnerabilities
UCG-07-01 Check device patching status
UCG-07-02 Host based vulnerability scanning
UCG-09-02 Monitor activity on device
UCG-07-03 Ensure Device firmware integrity

Traceability to
Figure 1.1 - Detailed view of Cyber-Trust project

Example
A Cyber-Trust enabled device that is actively monitored suddenly detects [A03] that its firmware has been altered due to a malware that is trying to adjust its communication practices. The smart device agent [A12] has recognised that critical OS files [D5] have been altered. The smart device agent [A12] instructs for the dumping of the current device firmware to a secured container and instructs the storage of key information in the blockchain. The vanilla version of the firmware is retrieved from the Patching Database (if available) and installed on the device. The smart device agent [A12] runs checks on the health status of the device again and recognises the correctness of the firmware hashes and the integrity of the device.

Main scenario

Step	Actor	Action description

Cyber-Trust Consortium. All rights reserved.

1	NIDS	A Cyber-Trust enabled device that is actively monitored suddenly detects that its firmware has been altered due to a malware that is trying to adjust its communication practices.
2	Smart Device Agent [A12]	The smart device agent [A12] checks for the integrity of critical OS files [D5]
3	Smart Device Agent [A12]	The smart device agent [A12] instructs for the dumping of the current device firmware to a secured container
4	DLT	Relevant information is stored in the blockchain
5	Patch Database	The vanilla version of the firmware is retrieved from the Patch Database and installed on the device
6	Smart Device Agent [A12]	The smart device agent [A12] runs checks on the health status of the device again and recognises the correctness of the firmware hashes and the integrity of the device

Extension scenarios

<5> a	Actor	The Patch database does not contain information related to the new patch
1		The user is prompted to update the firmware themselves

<6> b	Actor	The health check fails
1		The smart device agent [A12] cuts off communication with other Cyber-Trust monitored devices [A03]
2		The smart device agent [A12] checks for firmware integrity and when this is confirmed communication to other Cyber-Trust devices is restored.

UCG-18-01: Apply Mitigation Policy on Device

Name: Apply Mitigation Policy on Device

Description: At device level the decisions taken at network level are applied. This use case is relevant with full functionality for Cyber-Trust enabled devices and when the system runs with full capabilities. Functionality is also offered on Cyber-Trust enabled devices when operating with partial capability.

Type: System Use case

Primary Actor: [P2] A Smart Device owner

Supporting/Secondary actors: [P1] Smart Home Owner, [O2] ISP, [O4] IoT SP

Stakeholders	Interest

Cyber-Trust Consortium. All rights reserved.

Network Modelling [A16]	The detection of abnormal and suspicious activity at network level may determine the mitigation policy to be applies at device level.; The network profiling of a service produces key findings to allow the effective detection and identification of the acquired cyber-threat.
Cyber-Defence Service [A04]	This service involves the decision making at defending the Cyber-Trust system and limiting the impact of the imposed threat; The detection and mitigation center depending on the findings of the analysis determines the most appropriate mitigation policy to be taken at device level.
Smart Gateway IRS Application [A13]	The incident response module at the smart gateway level [A13]

Pre-conditions
A threat had been identified, the mitigation policy for its elimination or isolation is being determined at network level.

Trigger conditions

Post-conditions
The mitigation policy on the device may result in the isolation of the device from the remaining network. A post-condition for this use case might also be the initiation of a remediation operation.

Minimum guarantees

Frequency of use
Ad hoc

Non-functional requirements

Related use cases

Traceability to
Figure 1.1 - Detailed view of Cyber-Trust project

Cyber-Trust Consortium. All rights reserved.

Example
A Cyber-Trust enabled device is actively monitored [A03] and at healthy state. During operation malicious traffic goes through the device originating a network device. The mitigation strategy constructed at network level instructs the smart device agent [A12] to cut off communication with connected devices and raise an alert to the visualisation portal [A01]. The device will be instructed to go back online when the issue at network level is resolved.

Main scenario

Step	Actor	Action description
1	System	During operation malicious traffic goes through the device originating a network device
2	System	The mitigation strategy constructed at network level instructs the smart device agent [A12] on the action set
3	Smart Device Agent [A12]	The smart device agent [A12] is performing the instructed tasks
4	Smart Device Agent [A12]	An alert is raised to the visualisation portal

UCG-18-02: Retrieve mitigation policy information

Name: Retrieve mitigation policy information

Description: Retrieve mitigation policy from database for the threat detected. If the database [A08] does not maintain mitigation, then default measure it to block connectivity until received from Intelligence mitigation module.

Type: System

Primary Actor: Trust Management System [A05]

Supporting/Secondary actors: Mitigation policy database

Stakeholders	Interest
Trust Management System [A05]	Query the mitigation policy database
TrustDB Admin Module [A08]	Provides specifications to be followed

Pre-conditions
Mitigation policy information exists in the database.

Trigger conditions
Device risk level is changed

Post-conditions

Cyber-Trust Consortium. All rights reserved.

mitigation policy is retrieved

Frequency of use
Multiple times per day

Non-functional requirements
None

Related use cases
[UCG-15-02]

Traceability to
Figure 1.1 - Detailed view of Cyber-Trust project

Example
The system retrieves the mitigation policy information from mitigation policy database.

Main scenario

Step	Actor	Action description
1	TMS	The risk level related to the current status of the device is changed
2	TMS	The TMS sends the vulnerable device details along with risk updated level and profile information to the mitigation policy database.
3	System	The System analyses the given information using [UCG-18-01] and retrieved the recommended policy.
4	The mitigation policy database	The mitigation policy database sends Retrieve mitigation policy information TMS.

UCG-18-03: Apply network security defense rule

Name: Apply network security defense rule

Description: Network security combines multiple rules and layers of defenses [A04] at the edge and in the network and as such represents the decision implementation element of the intersection of vulnerability (built from trust, threat and DLT-assured device profiles [A02]). These include access control, application security, Intrusion prevention system, firewall and many more.

Type: System

Cyber-Trust Consortium. All rights reserved.

Primary Actor: Cyber-Defense Service [A04]

Supporting/Secondary actors: Smart Gateway Agent [A11]

Stakeholders	Interest
System	Manage the traffic via the network

Pre-conditions
Apply all security rules

Trigger conditions
Network traffic

Post-conditions
network is protected

Minimum guarantees

Frequency of use
Multiple times per second

Non-functional requirements

Related use cases
Monitor the network traffic

Traceability to

Example
Depending on the detected attack, the appropriate network defense rule will be applied.

Main scenario

Step	Actor	Action description

Cyber-Trust Consortium. All rights reserved.

1	System	The system applies network access control (NAC) to recognize each user and each device by allowing only authorized devices to get access to the network.
2	System	The system uses application security to close holes, or vulnerabilities, that attackers can use to infiltrate the network.
3	System	The system uses intrusion prevention system (IPS) to scan network traffic to actively block attacks.
4	System	System uses VPN to encrypt the connection from an endpoint to a network.
5	System	System uses the firewall to put up a barrier between a trusted internal network and untrusted outside networks.
6	system	System uses IDS to compare the packets information with known attack signatures to identify threats to the network.

UCG-18-04: Notify of device compromise

Name: Notify of device compromise.

Description: Describe the procedure the system will use in case of a comptonization of a device.

Type: System use case

Primary Actor: System

Supporting/Secondary actors: [P1, P2] user, [O2] A security officer (Tom) working at an ISP – telecom operator.

Stakeholders	Interest
[P1, P2] user. [O2] A security officer (Tom) working at an ISP – telecom operator.	Get notify when one of his/her device is being compromised.

Pre-conditions
A user has already registered itself and register one or more device.

Trigger conditions
A security issue is registered to the Cyber-Trust platform.

Post-conditions
The user and organization are being alerted by the system.

Minimum guarantees
A back-end rule which alert user impacted by the addition of a new security issue in the system.

Cyber-Trust Consortium. All rights reserved.

Frequency of use
Once per security issue.

Related use cases

Non-functional requirements
None

Traceability to
Figure 1.1 - Detailed view of Cyber-Trust project

Example
As an ISP security officer [O2] I want to get notify of a potential security issue in order to protect my devices and my clients.

Main scenario

Step	Actor	Action description
1	System	A new security issue is added to the system for a specific device. The system will alert the fabricant of the device and every registered user of this device.

UCG-18-05: Compute optimal intrusion response actions

Name: Compute optimal intrusion response actions

Description: The iIRS [A13] computes the suitable defence action based on the information it possesses about the system security state and the attacker's profile. Optionally, it suggests an action to security officer, before applying it automatically.

Type: System type

Primary Actor: [A13] iIRS

Supporting/Secondary actors: [O2] Security officer (Sarah)

Stakeholders	Interest
[P1, P2] user	The defense actions applied enhance the smart home security.

Cyber-Trust Consortium. All rights reserved.

Security officer [02]	In case the iIRS informs the security officer, it helps her to make better decisions regarding the security actions to be applied.

Pre-conditions
Formalization of the decision-making module of the iIRS (I.e. state space and observation model, information about the attacker and its admissible strategies, utility functions).

Trigger conditions
None.

Post-conditions
A suitable defense action is either applied or suggested to the security officer.

Frequency of use
Periodically (at predefined decision epochs).

Non-functional requirements
None

Related use cases
UCG-18-01 Apply Mitigation Policy on Device UCG-18-03 Apply network security defense rule UCG-18-06 Define applicable mitigation actions

Traceability to
Figure 1.1 - Detailed view of Cyber-Trust project.

Example
At the predefined decision epochs (periodically), the iIRS [A13] based on the belief it has computed [UCG-15-04], defines its applicable actions [UCG-18-06] and decides on the best available action. Alternatively, the iIRS [A13] informs the security officer Sarah [O2] about the best suggested action and she decides on the defense action [A04].

Main scenario

Step	Actor	Action description

Cyber-Trust Consortium. All rights reserved.

1	iIRS [A13]	At every decision epoch iIRS updates its local information (incl. the available mitigation actions).
2	iIRS [A13]	Computes the belief about the current system security state.
3	iIRS [A13]	Internally stores the computed belief.
4	iIRS [A13]	Decides on the best defense action to be taken.
5	iIRS [A13]	The chosen defense action is communicated to the Cyber-Defence service [A04]

Extension scenarios

5a		Clearance by security officer Condition: The decision of the enforcement of the defense action requires approval by the security officer.
1	System	The system displays the computed defense action and asks the security officer for clearance on whether the action should be performed
2	Security officer	The security officer provides a response
3	System	If the response is positive, the action is taken

UCG-18-06: Define applicable mitigation actions

Name: Define applicable mitigation actions

Description: The Security officer consults the cyber-attack graphical security model, which contains the system's security conditions and the available exploits, as well as their relations, and defines the mitigation actions which are at the iIRS [A13] disposal.

Type: System type

Primary Actor: [O2] Security officer (Sarah)

Supporting/Secondary actors: [A09] eVDB Sharing Service, [A13] iIRS

Stakeholders	Interest
Security officer [02]	Accurate construction of the iIRS defense model.

Pre-conditions
Cyber-attack graphical security model. Access to the eVDB and the existence of information on mitigating vulnerabilities.

Trigger conditions

Cyber-Trust Consortium. All rights reserved.

Need for security analysis, recommendation of defence strategies, automated defence; Change of network configuration; New exploit discovery.

Post-conditions
iIRS admissible mitigation actions are defined.

Frequency of use
Initially for the security analysis task. If network configuration changes. If there is a change in security conditions and/or in their relations. If a new exploit is discovered.

Non-functional requirements
None

Related use cases
UCG-15-01 Compute cyber-attack strategy's model UCG-18-05 Compute optimal intrusion response actions UCG-04-03: Define mitigation actions' impact

Traceability to
Figure 1.1 - Detailed view of Cyber-Trust project

Example
The security officer Sarah [O2] consults the cyber-attack graphical security model to see which exploits the iIRS [A13] can block to secure the various security conditions. If a new exploit is discovered by the eVDB [A09], Sarah [O2] is informed and she updates the available mitigation actions in the iIRS [A13] model.

Main scenario

Step	Actor	Action description
1	Security officer	The security officer initiates the process of defining/updating the applicable mitigation actions
2	System	The system retrieves the cyber-attack graphical security model.
3	System	The system retrieves updated information on the available exploits from the enriched eVDB also containing information on mitigation or workarounds.

Cyber-Trust Consortium. All rights reserved.

4	System	The system displays a user interface for allowing the security officer to define the applicable mitigation actions
5	Security officer	The security officer selects the applicable mitigation actions for each exploit.
6	System	The system validates and stores the applicable action set for each exploit.

Extension scenarios

1a	Actor	Automated definition of mitigation action(s) Condition: the graphical security model has just been created
1	System	The system triggers the definition of applicable mitigation actions
2	System	Control is returned to step #2

After step 3	Actor	Define default mitigation action(s) Condition: explicit information on the mitigation actions is not available on the enriched eVDB
1	System	The system displays a warning message
2	System	The system populates the list of applicable actions with a system-wide default mitigation action.
3	System	Control is returned to step #4

After step 6	Actor	Communicate mitigation updates Condition: change in action(s) set
1	System	The updated action set is sent to the user's iIRS.
2	iIRS	The iIRS receives and stores locally the updated mitigation options.

UCG-19-01: Update baseline traffic statistics

Name: Update baseline traffic statistics

Description: the baseline network should be updated in order to gain insight into how the network is being used. This leads to know overall health of the network by statistics that are provided.

Type: System

Primary Actor: Cyber-Defense Service [A04]

Supporting/Secondary actors: Monitoring Service [A03]

Stakeholders	Interest

System	Manage the traffic via the network
Monitoring Service [A03]	Analyses and tracks inbound and outbound packets

Pre-conditions
Packet Sniffer has been installed.

Trigger conditions
Network traffic

Post-conditions
The baseline has been updated

Minimum guarantees

Frequency of use
Multiple times per minute

Non-functional requirements

Related use cases
Monitor the network traffic

Traceability to

Example
The baseline network is updated in order to gain insight into how the network is being used.

Main scenario

Step	Actor	Action description
1	System	The system retrieves baseline database

Cyber-Trust Consortium. All rights reserved.

2	System	The system will check each packet passing through network
3	System	The system uses Packet Sniffer to capture the entire stream of network data.
4	Packet Sniffer	IDS use a network probe to capture raw packet data.
5	System	System checks what the users are actually doing on the network.
6	Packet Sniffer	Packet Sniffer determines users and the specific applications that consume the most bandwidth within the network.
7	System	The system updates the baseline network statistics.

Extension scenarios

After step 5	Actor	If the captured traffic belongs to new device
1	System	The system creates new profile to store the gathered stats.
2	System	The System checks match any followed stats with the newly created profile.

UCG-19-02: Choose data sharing level.

Name: Choose data sharing level.

Description: Define the procedure for changing the amount of data a user will expose to the Cyber-Trust platform.

Type: Business use case

Primary Actor: [P1, P2] user.

Supporting/Secondary actors: System

Stakeholders	Interest
[P1, P2] user	Change the data sharing level to improve the security of her devices or improve her privacy
System	Take consideration of the user choice.

Pre-conditions
A user has already registered itself and the device he wants to change data sharing level

Trigger conditions
The user clicks the ‘Change the data sharing of my device’ button.

Post-conditions
The data sharing level have been changed.

Cyber-Trust Consortium. All rights reserved.

Minimum guarantees
Web page with a table of all user's devices and their data sharing level.

Frequency of use
Once per user request.

Related use cases
UCG-10-06

Non-functional requirements
User experience.

Traceability to
Figure 1.1 - Detailed view of Cyber-Trust project

Example
As a user [P1, P2]. I want to change the data sharing level of one my device in order to protect my personal data or collaborate to the overall safety of the connected device.

Main scenario

Step	Actor	Action description
1	[P1, P2] user	Mary, a user, connects to the Cyber-Trust web site and successfully log on the platform. She already registered her device. She goes to the data table where is listed the devices, she wants to share more data.
2	[P1, P2] user	On the device's row, she goes to the column data sharing level. The element is a drop-down list. She chooses the 'Maximum' element in it.
3	System	The system validates the change and notify the user by a message on the screen.

UCG-19-03: Change Device configuration.

Name: Change Device configuration.

Description: A user wants to change the configuration of a device that he previously registers [A06, A15] on the platform.

Type: Business use case

Cyber-Trust Consortium. All rights reserved.

Primary Actor: [O3] LEA.

Supporting/Secondary actors: System

Stakeholders	Interest
[O3] Police officer	Change configuration of a device to stop an attack
System	Acknowledge and apply the change ask by the user

Pre-conditions
A user has already registered itself and register one or more device. He is logged in and on the page of the device he wants to change the configuration of. The user also has the right to perform the operation.

Trigger conditions
The user clicks on the button 'Change configuration' next to the device he wants to get information about.

Post Conditions
The actor changes configuration of a device.

Minimum guarantees
A web pages

Frequency of use
Once per request of the user

Related use cases
UCG-18-04

Traceability to
Figure 1.1 - Detailed view of Cyber-Trust project

Example
As a Police officer. (Actor: O3) I want to change the configuration of a device in order to stop an attack.

Main scenario

Step	Actor	Action description

Cyber-Trust Consortium. All rights reserved.

1	[O3] LEA	The actor goes to the page of the device he investigates about. He then clicks the button 'Change configuration'. A pop-up opens.
2	[O3] LEA	The actor changes the information (shutting down the device / closing one port of the device) and validate the form.
3	System	The system saves the change, close the pop-up and notify the user of the success of the operation by a message on the screen.

Extension scenarios

After step 2	Actor	The information given by the user via the form is incorrect
1	System	The system does not validate the form and write a message under each incorrect field to help the user to understand what happened.

UCG-19-04: Tune the crawling parameters and evaluate existing seeds

Name: Tune the crawling parameters and evaluate existing seeds

Description: The function of the cyber-threat discovery module is supervised by an IT expert that is responsible to add, annotate, and approve the crawling of new seeds [A10] (i.e., websites of interest), tune the crawling parameters that enable their discovery, and evaluates existing seeds in terms of usefulness [D6].

Type: business use case

Primary Actor: [O1] An IT expert acting as a cyber-threat discovery module supervisor (Bob)

Supporting/Secondary actors: [A09] eVDB Sharing Service

Stakeholders	Interest
IT expert [01]	Ensure that Cyber-Trust monitors credible and information-rich sources
Infrastructure owner	Protect registered devices through reliable and up-to-date cyber-threat intelligence

Pre-conditions
IT expert is logged into the Cyber-Trust system

Trigger conditions
When crawl quality drops or periodically

Cyber-Trust Consortium. All rights reserved.

Post-conditions
Crawl parameters have been tuned to improve crawl quality. New seeds have been added, approved and annotated. Existing seeds have been evaluated.

Frequency of use
Periodically (a few times per month) or when crawling quality is observed to drop.

Non-functional requirements
None

Related use cases
UCG-16-04 Crawl the clear/deep/dark web and update the eVDB UCG-06-06 Provide feedback/rating on sources of vulnerabilities

Traceability to
Figure 1.1 - Detailed view of Cyber-Trust project

Example
The cyber-threat module has identified a number of new seeds for crawling ([A10], [D6]) and all this information is presented to the IT expert ([O1]). He uses an appropriate UI to get access to the new seeds and inspects them with regard to a number of aggregated/anonymised parameters (like top-ranked terms/tags, recently extracted –anonymised- text snippets, extracted vulnerability information, or annotations per seed) that are presented to him. He approves the most promising ones, while he manually inspects some others (e.g., by visiting the relevant webpage/forum/marketplace) to get more insight on the seed content and quality. After approving and annotating the most promising seeds, and rejecting the rest, he also adjusts the crawling ([A10], [D6]) parameters to reflect the changes he made. This is done by entering login credentials and CAPTCHA information for the newly approved seeds and by setting the crawl frequency and the crawl frontier size.

Main scenario

Step	Actor	Action description
1	IT expert	The IT expert selects "Tune crawling" functionality.
2	System	The system presents an editable list of current crawl parameters and a form to allow the IT expert to enter seed search criteria.
3	IT expert	The IT expert enters the seed search criteria and submits the form.

Cyber-Trust Consortium. All rights reserved.

4	System	The system retrieves the seeds that match the search criteria alongside relevant information (such as top-ranked terms/tags, recently extracted text snippets, extracted vulnerability information, annotations) for each seed.
5	System	The system presents the information to the IT expert.
6	IT expert	The IT expert selects the seed to be updated and submits this information.
7	System	The system presents a detailed record of the seed and appropriate controls to allow the update, including “approve”, “annotate”, “evaluate”, “delete”.
8	IT expert	The IT expert selects and performs the desired update.
9	System	The system validates the completeness and validity of the updated information.
10	System	The system updates the information of the affected seed.
11	System	The system informs the IT expert that the update has been performed.

Extension scenarios

4a	Actor	No seed matches the criteria
1	System	The system notifies the IT expert that no seeds were retrieved
2	System	Control returns to step #2

9a	Actor	The information submitted by the IT expert is incomplete/erroneous
1	System	The system informs the IT expert regarding the errors or omissions
2	System	Control returns to step #7

*a	Actor	The IT expert cancels the process (at any step)
1	IT expert	The IT expert cancels the process
2	System	The system terminates the procedure and destroys the Trust DB management form

7 Legal, ethical and privacy/data protection dimensions

UCG-07-01; UCG-07-02; UCG-14-01; UCG-10-03; UCG-07-03; UCG-14-02; UCG-09-03; UCG-09-04; UCG-06-03; UCG-19-01; UCG-14-03; UCG-05-01; UCG-05-02; UCG-05-03; UCG-05-04; UCG-05-05; UCG-05-06; UCG-05-07; UCG-05-08; UCG-05-09; UCG-15-01; UCG-15-02; UCG-13-01; UCG-16-03; UCG-15-03; UCG-06-04;

Cyber-Trust Consortium. All rights reserved.

UCG-02-05; UCG-14-07; UCG-16-04; UCG-06-05; UCG-14-08; UCG-13-02; UCG-15-04; UCG-06-07; UCG-04-02; UCG-04-03: No particular issues or only minor concerns were identified at this stage in relation those Use Cases, either because personal data is not envisaged to be processed at all or because it is not yet clear whether personal data is going to be processed. If personal data is processed, the processing must take place in accordance with the relevant data protection and privacy laws, as discussed in D3.1 - Part B, i.e. a legal base for such processing should be identified, the data controllers/processors must comply with the data protection principles and the data subjects´ rights should be respected to the fullest.

UCG-17-01; UCG-11-01; UCG-11-02; UCG-14-04; UCG-14-05; UCG-12-01; UCG-12-02; UCG-14-06; UCG-12-03; UCG-12-04; UCG-12-05: These Use Cases are related to the collection, handling and storage of information which may contain evidentiary material. Up until today, there is no comprehensive international or European legal framework in relation to electronic evidence. The collection and preservation of electronic evidence relies upon the national law, in particular the criminal law and the criminal procedural law of each Member State. The relevant provisions of national legislation must be taken into consideration when forensic evidence is gathered, in order to increase the likelihood for forensic evidence to be admissible in the Court of Law. Moreover, in the European Union the legal framework with regard to cross-border judicial and police cooperation, including the exchange and transfer of electronic evidence, is under intense reform. The legal use of electronic evidence, as well as data protection and privacy concerns and recommendations with regards to Distributed Ledger Technologies are discussed further in D3.2.

UCG-02-01; UCG-02-02; UCG-02-03; UCG-02-04; UCG-03-01; UCG-03-02; UCG-03-03; UCG-03-04: Those Use Cases relate to the registration or un-registration of a user, organisation or device to the Cyber-trust platform. In this context, personal data may be processed, such as full names, email addresses or data relating to a device. It must be ensured that a legal base for such processing exists, data processing principles are entirely implemented and data subject´s rights are fully communicated to the registering users. Users must be able to understand the implications of their registration to the platform and for that purpose, a detailed data protection and privacy statement should be easily accessible, including information about which types of data is collected, for which time-period, how it is stored, who has access to it. The storage and transmission of data collected must be safeguarded and accuracy of data must be established, for instance by establishing a pro-registration verification system and offer the post-registration possibility for incorrect data to be corrected. Moreover, only the least amount of information should be collected with regards to the specific purpose pursued. Legal entities are not protected under GDPR. Nevertheless, if personal data is involved (e.g. registering specific employees of a given entity), then all the data protection principles and data subject´s rights must be taken into account. When unregistering a user or a device, it must be ensured that all associated data is deleted.

UCG-16-05; UCG-19-04: These Use Cases are related to the use of the web crawler. Since the amount of information being crawled is enormous, the theoretical possibility that some of this information contains personal data cannot be excluded. In the case personal data is processed, as well as in case of doubt, the controller will need to ensure that the processing is compliant with the relevant data protection legislation. Furthermore, when crawling takes place on restricted access sources will most likely require a kind of authorisation, sometimes by the owner of the source. Although there is no specific law against web crawling or using publicly available information which has been obtained through the use of automated web crawling tools, the owner of a website may have a claim against the user if the scraping and subsequent use of the scraped information infringes the website owner’s intellectual property rights or, if the user violates the terms of use of the specific website. All these implications have been taken into consideration in D3.1, Section 6.4.1.

UCG-18-01; UCG-18-02; UCG-18-03; UCG-18-04; UCG-18-05; UCG-18-06: Those Use Cases relate to the selected defense tools or mitigation policies. The optimal solutions selected must always be proportional and necessary for the purpose pursued. The purpose, in turn, must be legitimate. The least intrusive methods should be always preferred, if they can lead to the same result as more intrusive methods. The impact on an

Cyber-Trust Consortium. All rights reserved.

individual´s privacy should be always assessed on a case-by-case basis. The tools should be only activated by certain incidents that are more likely to correlate to criminal activity. Different measures should be selected depending on whether they are intended to tackle serious crime (e.g. cyber-attacks on critical infrastructure) or petty criminality (e.g. small-scale cyberthreats with minor or uncertain impact). This dimension is further discussed in D3.1, Section 3.4.2.2.

UCG-01-01; UCG-01-02; UCG-10-05: These Use Cases relate to the activation and deployment of the device agent. Some considerations also apply to the network traffic filtering. The Terms of Services must be drafted in accordance to the data protection principles and fully implement data subject´s rights, by giving him/her control over his/her data, in full compliance with GDPR as depicted in D3.1, Part B. According to Article 4(11) of the GDPR, consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. The GDPR conditions for obtaining valid consent are also applicable in cases which fall within the scope of the e-Privacy Directive concerning the confidentiality of electronic communications, which may be relevant in the case of Cyber-trust. Caution is needed from the data controller when a contract, which may include the provision of a specific service has a request for consent to process personal data tied to it. If consent is bundled up as a non-negotiable part of terms and conditions, presumably it has not been provided freely by the data subject.

Moreover, data protection and privacy must be guaranteed by design and by default, and users must be provided with information about how their data is going to be collected, used and processed, as well as their rights and relevant risks and implications. For that cause, a data protection and privacy statement in clear and plain language and must be made available and easily accessible on the user interface. Emphasis should be given to the parts where the user has the chance to explicitly opt-in or opt-out. Practices which can be characterised as particularly intrusive and include great degree of monitoring should be an opt-in, rather than an opt-out.

UCG-09-01; UCG-09-02; UCG-10-01; UCG-10-05: These Use Cases relate to monitoring activity, critical OS files and vulnerabilities on a device or network traffic filtering. All monitoring activities, either active or passive, may be rather intrusive. It must be ensured that only the most relevant data is collected and processed and only the most appropriate and reasonable techniques are used, based on the principle of proportionality, serving a legitimate purpose. Monitoring should never be excessive, because it would risk amounting to digital surveillance, and thus resulting in an interference with individuals´ privacy, as seen in detail in D3.1, Section 3.4.2.2. Even though the user may choose between partial and full monitoring, data protection and privacy options should always be the default settings. Hiring and consulting a DPO would be indispensable provided the big quantities of data collected and processed for achieving the cybersecurity purposes. It must be kept in mind as well, that special categories of data (i.e. "sensitive" data) require higher levels of protection. The issues, related to UCG-10-01, are further discussed in D3.1, Section 6.4.2.

UCG-10-04; UCG-19-03: These Uses Cases relate to the curation or change of a device configuration. Since the responsibility lies with the owner of the device to change the status of the device, when inactive, it is important that a mechanism for the prevention of false positives is in place, given the consequences a false positive may have to an individual´s privacy (e.g. use of rather intrusive methods), as seen in D3.1, Section 8.1.3.

UCG-10-06; UCG-06-06: Those Use Cases relate to access rights. It must be ensured, that only persons with the right authorisation can access information, which might include personal data. The participation of external entities/parties to the platform and their access rights must be elaborated accordingly, so as to minimise the possibility of false positives or the likelihood of access to a user´s data without the right authorisation. External entities/parties must only have access to anonymised/aggregated information and their contributions/expertise must be assessed with the necessary caution, given the adversary results false positives may have upon individuals.

Cyber-Trust Consortium. All rights reserved.

UCG-10-02; UCG-16-01; UCG-06-01; UCG-06-02; UCG-04-01; UCG-16-02: These Use Cases relate to anonymised, pseudonymised and special types of data. Anonymised data do fall out of the scope of the data protection legislation, but data subjects may still be entitled to protection under other legal instruments, for instance the confidentiality of their communications. Anonymisation solutions should be decided on a case-by-case basis, with the use of a combination of different techniques and methods and taking into account that anonymised data may still pose residual risks to data subjects. Practical recommendations are developed in the Article 29 Working Party Opinion 05/2014 on Anonymisation Techniques. As discussed in D3.1 and D3.2, encrypted data is personal data since it can still be accessed with the correct key and thus, it becomes evident that encryption does not make the data irreversibly unidentifiable, as required by GDPR in order to be regarded as anonymised. Thus, encrypted data still lays inside the Regulation´s scope. Furthermore, personal data which has been processed through a hashing function, continue to qualify as personal data under GDPR, as well. Although a hash process that cannot be reverse-engineered offers stronger data protection guarantees than encryption, the Article 29 Data Protection Working Party has clearly stated that hashes constitute pseudonymised data and not anonymised, as it is still possible to link the data to the data subject. Only the persons with the right authorisation may have access to this data.

Even if an individual is not directly identified from a piece of information, it is necessary to consider whether this individual is still identifiable, directly or indirectly. In order to assess that, the data controller must take into consideration the processed information with all the means reasonably likely to be used by either the data controller himself/herself or any other entity. For the data to be considered personal, it must also relate to an individual, taking into account the content of the information, the purpose of the processing or the impact of such processing on an individual. For instance, a piece of information may be personal data for one controller´s purposes, but non-personal data for another´s controller´s purposes. Even when additional information may be needed for the identification of an individual, the individual may still be identifiable, regardless of whether this additional data is already at the controller´s disposal or must be obtained from another source. The issue has been further discussed in D3.1.

Location data relating to individuals is very likely to be able to identify them. Hence it constitutes personal data, and sometimes it may include special types of data. Data controllers must minimise the amount of such data collected, processed and retained due to risks posed by linked location data. Therefore, informed consent appears to be the most appropriate basis for collecting and processing location data in most cases. More information may be found in the Article 29 Working Party Opinion 13/2011 on Geolocation services on smart mobile devices.

UCG-19-02: This Use Case relates to data sharing options and thus, it is essential to be well designed because it implies hundreds of thousands of inter-connected devices which contain personal data and may interfere with individual´s privacy. For instance, if the smart home surveillance system of a user is activated, this could imply that the user is out of his/her home at that specific time. It is of paramount importance that the highest level of privacy enhancement and security measures are in place, whenever monitoring activities entail the risk of being exploited by an adversary or an unauthorised third party to gain access to special types of data or information which can expose patterns or other specific aspects of an individual´s life. The possible damages caused by such an exploitation can impact both the psychological and physical spheres of a user and interfere with her/his right to privacy. Hence, the information collected should always be the minimum necessary for the purpose pursued, the purpose should be legitimate, and the methods used assessed under the principle of proportionality. All data protection principles must be safeguarded, and in particular, privacy and data protection by design and by default should ensure that the least intrusive available means will be implemented. Data security measures should make sure that the data will not be accessed by unauthorised

Cyber-Trust Consortium. All rights reserved.

entities internally or externally, as opposed to the individual´s will and even in the case of a breach incident, the data must be in such a way technically engineered, that it would render it unexploitable in the hands of a third unauthorised party. A detailed overview of the risks and implications of a user´s choices with regards to data sharing must be easily accessible, intelligible, written in plain and clear language. Moreover, it must be clear that the user can revoke her/his consent at any time. This is important for seeking a valid informed consent from the user. These issues have been discussed in detail in D3.1 – Part B.

Hereinafter a table is included with all the considerations regarding privacy and data protection, as well as other legal and ethical implications per Use Case. For some issues may not be straightforward, a more in-depth analysis of the applicable frameworks, at European and national level, can be found in Deliverable 3.1 (D3.1) - Regulatory Framework Analysis and Deliverable 3.2 (D3.2) - Legal analysis of the use of evidence material.

UC ID	UC Name	Legal, ethical and privacy/data protection dimensions
UCG-01-01	Activate device agent	The privacy policy must be drafted in accordance to the data protection principles and fully implement data subject´s rights, by giving him/her control over his/her data, in full compliance with GDPR as depicted in D3.1.A lawful basis for processing is in place, if you enter into a contractual relation with an individual and processing their personal data is necessary so as to comply with your obligations under the contract. If the processing is not necessary for the performance of the contract, meaning that there are other reasonable and less intrusive means to satisfy one´s contractual obligations then another legal basis must be considered, for instance the consent of the data subject. According to Article 4(11) of the GDPR, consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. The GDPR conditions for obtaining valid consent are also applicable in cases which fall within the scope of the e-Privacy Directive concerning the confidentiality of electronic communications, which may be relevant in the case of Cyber-trust. Caution is needed from the data controller when a contract, which may include the provision of a specific service has a request for consent to process personal data tied to it. If consent is bundled up as a non-negotiable part of terms and conditions, presumably it has not been provided freely by the data subject. Data protection and privacy must be guaranteed by design and by default, and users must be provided with information about how their data is going to be collected, used and processed, as well as their rights and relevant risks and implications. For that cause, a data protection and privacy statement in clear and plain language and must be made available and easily accessible on the user interface.

Cyber-Trust Consortium. All rights reserved.

UCG-01-02	Deploy Cyber-Trust device agent	The conditions for the use of the platform and its tools must be clearly-written in an intelligible way, that can be understood by an average user - not necessarily tech savvy. Emphasis should be given to the parts where the user has the chance to explicitly opt-in or opt-out. Practices which can be characterised as particularly intrusive and include great degree of monitoring should be an opt-in, rather an opt-out.
UCG-02-01	Register user into Cyber-Trust platform	Personal data is involved here such as a name and the email address (registration data) used to register. It must be ensured that a legal base for such processing exists, data processing principles are entirely implemented and data subject´s rights are fully communicated to the registering users. Users must be able to understand the implications of their registration to the platform and for that purpose, a detailed data protection and privacy statement should be easily accessible, including information about which types of data is collected, for which time period, how it is stored, who has access to it. The storage and transmission of data collected must be safeguarded and accuracy of data must be established, for instance by establishing a pro-registration verification system and offering the post-registration possibility for incorrect data to be corrected. Moreover, only the least amount of information should be collected with regards to the specific purpose pursued.
UCG-02-02	Register organization into Cyber-Trust platform.	Legal entities are not protected under GDPR. Nevertheless, if personal data is involved (e.g. registering specific employees of a given entity), then all the data protection principles and data subject´s rights must be taken into account.
UCG-02-03	Register device (including device class) into Cyber-Trust platform.	Personal data is involved here such as the name and the class of the device registered. Same as in UCG-02-01.
UCG-02-04	Log on to the Cyber-Trust platform	Personal data is involved here such as the name and the class of the device registered. Same as in UCG-02-01.
UCG-02-05	Register to the eVDB sharing service	No issues identified. Collection and processing of data of registered users must be in line with GDPR.
UCG-03-01	Log out from the Cyber-Trust platform	Personal data is involved here such as the name and the class of the device registered. Same as in UCG-02-01.
UCG-03-02	Unregister User	Same as in UCG-02-01. All associated data should be deleted.

Cyber-Trust Consortium. All rights reserved.

UCG-03-03	Unregister Organisation	Same as in UCG-02-01. All associated data should be deleted.
UCG-03-04	Unregister device	Same as in UCG-02-01. All associated data should be deleted.
UCG-04-01	Private IoT Device Profile generation	This is a core data protection element to the IoT device component of the cyber-trust system. As discussed in D3.1 and D3.2, encrypted data is personal data since it can still be accessed with the correct key and thus, it becomes evident that encryption does not make the data irreversibly unidentifiable, as required by GDPR in order to be regarded as anonymised. Thus, encrypted data still lays inside the Regulation´s scope. Furthermore, personal data which has been processed through a hashing function, continue to qualify as personal data under GDPR, as well. Although a hash process that cannot be reverse-engineered offers stronger data protection guarantees than encryption, the Article 29 Data Protection Working Party has clearly stated that hashes constitute pseudonymised data and not anonymised, as it is still possible to link the data to the data subject. The optimal solution should be decided on a case -by-case basis. For a complete anonymisation process to be valid, it must be robust against identification performed by the most likely and reasonable means the data controller or any third party may employ. If a solution does not offer these guarantees, a thorough evaluation of the identification risks should be performed. Thus, the use of a combination of techniques is highly recommended to ensure that data is sufficiently de-identified, despite the fact that the Article 29 Working Party admits that there are inherent limitations in most anonymisation and pseudonymisation techniques. When selecting/implementing the techniques, all means reasonably likely to be used to identify an individual must be taken into consideration, both internally and by other third entities/individuals, especially when additional data sets could be obtained and used to lead to the identification of an individual. Keeping up with technological developments in the field of re-identification technologies and re-assessing regularly the effectiveness of anonymisation or pseudonymisation techniques used may also lead to higher protection levels.
UCG-04-02	Characterize asset's importance	No particular considerations.
UCG-04-03	Define mitigation actions' impact	No particular considerations.

Cyber-Trust Consortium. All rights reserved.

UCG-05-01	2D View Systems State	No particular considerations. If personal data is processed for this Use Case, the processing must be carried out in accordance with the relevant data protection and privacy laws, as discussed in D3.1.
UCG-05-02	3D-Virtual Reality View Systems State	Same as in UCG-05-01.
UCG-05-03	Visualize summary of eVDB contents matching an operator's devices	Same as in UCG-05-01.
UCG-05-04	Visualize network's health status	Same as in UCG-05-01.
UCG-05-05	Visualize device vulnerability levels	Same as in UCG-05-01.
UCG-05-06	Visualize network traffic	Same as in UCG-05-01.
UCG-05-07	Visualize device trust level	Same as in UCG-05-01.
UCG-05-08	Visualize known and zero-day vulnerabilities	Same as in UCG-05-01.
UCG-05-09	Visualize historical (heterogeneou s) data	Same as in UCG-05-01.
UCG-06-01	Raise alert for security officer	In this case, hashed device ID will be displayed. If the device IDs are personal data in the first place, then a hashed device ID is pseudonymous data, hence still personal data. Only the persons with the right authorisation may have access to this data. To ensure that, a secure mechanism for the authentication of the UI user must be put in place.
UCG-06-02	Raise alert for device owner	In this case, hashed device ID will be displayed. Details can be unlocked with biometrics. Same as in UCG-06-01. Even if an individual is not directly identified from a piece of information, it is necessary to consider whether this particular individual is still identifiable, directly or indirectly.

Cyber-Trust Consortium. All rights reserved.

		In order to assess that, the data controller must take into consideration the processed information with all the means reasonably likely to be used by either the data controller himself/herself or any other entity. For the data to be considered personal, it must also relate to an individual, taking into account the content of the information, the purpose of the processing or the impact of such processing on an individual. For instance, a piece of information may be personal data for one controller´s purposes, but non-personal data for another´s controller´s purposes. Even when additional information may be needed for the identification of an individual, the individual may still be identifiable, regardless of whether this additional data is already at the controller´s disposal or must be obtained from another source. The issue has been further discussed in D3.1.
UCG-06-03	Establish baseline traffic statistics	No particular issues identified. Privacy concerns have been discussed further in D3.1.
UCG-06-04	Query and retrieve information from eVDB	No particular considerations.
UCG-06-05	Review and validate eVDB entries.	No particular considerations.
UCG-06-06	Provide feedback/rating on sources of vulnerabilities.	The participation of external entities/parties to the platform and their access rights must be elaborated accordingly, so as to minimise the possibility of false positives or the likelihood of access to a user´s data without the right authorisation. External entities/parties must only have access to anonymised/aggregated information and their contributions/expertise must be assessed with the necessary caution, given the adversary results false positives may have upon individuals.
UCG-06-07	Communicate iIRS actions to the security officer	No particular considerations.
UCG-07-01	Check device patching status	This use case involves only firmware information and installed updates; this data is not related to personal data. No particular issues identified.
UCG-07-02	Host based vulnerability scanning	If this correlation of information could lead to the identification of an individual, even if personal data is not processed in the first place, then all the data processing principles must be complied with, in addition to the existence of a legal base.

Cyber-Trust Consortium. All rights reserved.

UCG-07-03	Ensure Device firmware integrity	No particular issues identified.
UCG-08-01	Monitor device at gateway (network traffic filtering)	Privacy and data protection concerns have been further discussed in D3.1 and in particular, Section 6.4.3.
UCG-08-02	Capture and classify network packets (DPI)	Data protection and privacy dimensions on this matter have been discussed in D3.1, Sections 6.4.2 and 6.4.3.
UCG-09-01	Monitor device critical OS files / vulnerabilities	All monitoring activities, either active or passive, may be rather intrusive. It must be ensured that only the most relevant data is collected and processed and only the most appropriate and reasonable techniques are used, based on the principle of proportionality, serving a legitimate purpose. Monitoring should never be excessive, because it would risk amounting to digital surveillance, and thus resulting in an interference with individuals´ privacy, as seen in detail in D3.1, Section 3.4.2.2.
UCG-09-02	Monitor activity on device	Same as in UCG-09-01.
UCG-09-03	Perform vulnerability scanning	No issues identified, as long as no personal data is displayed on the dashboard or can be accessed through it, unless with the right authorisation.
UCG-09-04	Detect network attacks	If data related to an individual may be contained in those alerts, it must be ensured that only persons/entities with the right authorisation will have access to them, and no-one else. To that end, oversight mechanisms must be put in place.
UCG-10-01	Device Profiling	It is crucial that there is always a legal base for the collection of this information, as long as personal data is concerned. In the context of that use case, informed, specific and explicit consent given by the data subject is required, when registering himself/herself to the platform and his/her devices. Principles related to the data processing, in particular the principle of data minimisation (the least possible amount of personal data shall be collected), must be guaranteed and the data subject´s rights alike. Since these techniques may be quite intrusive, the operators of the Cyber-trust platform must always keep in mind that the collection and processing of personal data and other information relating to the private sphere of an individual should be proportional to the pursued legitimate purpose. Always the least intrusive method should be chosen from the available methods that could lead to the same result and additional

Cyber-Trust Consortium. All rights reserved.

		technical and organisational measures must be taken to assess any risks pertaining to such processing. In other words, the collection of all possible data, simply because they are available, is to be avoided. Even though the user may choose between partial and full monitoring, data protection and privacy options should always be the default settings. Hiring and consulting a DPO would be indispensable provided the big quantities of data collected and processed for achieving the cybersecurity purposes. It must be kept in mind as well, that special categories of data (i.e. "sensitive" data) require higher levels of protection.
UCG-10-02	Data Anonymisation	Anonymised data do fall out of the scope of the data protection legislation, but data subjects may still be entitled to protection under other legal instruments, for instance the confidentiality of their communications. Anonymisation solutions should be decided on a case-by-case basis, with the use of a combination of different techniques and methods and taking into account that anonymised data may still pose residual risks to data subjects. Practical recommendations are developed in the Article 29 Working Party Opinion 05/2014 on Anonymisation Techniques.
UCG-10-03	Retrieve device profile information	If this information includes personal data, it is of paramount importance that a legal base for such processing has been identified, the data processing principles are implemented and data subjects´ rights are respected to the fullest.
UCG-10-04	Manually curate device profile	Since the responsibility lies with the owner of the device to change the status of the device, when inactive, it is important that a mechanism for the prevention of false positives is in place, given the consequences a false positive may have to an individual´s privacy (e.g. use of rather intrusive methods).
UCG-10-05	Gateway Network Device Profiling	Same as in UCG-01-02 and UCG-09-01.
UCG-10-06	Get Device Information	It has to be ensured, that only persons with the right authorisation can access information, which might include personal data.
UCG-11-01	Gather device forensic evidence	There is no comprehensive international or European legal framework in relation neither to evidence, in general, nor electronic evidence, in specific. The collection and preservation of electronic evidence relies upon the national law, in particular the criminal law and the criminal procedural law. Significant differences in national legislations and approaches make the handling of electronic evidence complex across jurisdictions. The relevant provisions of national legislation must be taken into consideration when forensic evidence is gathered, in order to

Cyber-Trust Consortium. All rights reserved.

		increase the likelihood for forensic evidence to be admissible in the Court of Law. The legal use of electronic evidence is analysed in detail in D3.2. In this latter deliverable, data protection and privacy concerns with regards to Distributed Ledger Technologies are also discussed.
UCG-11-02	Gather network forensic evidence	Same as in UCG-11-01. The issue has been further discussed in D3.2.
UCG-12-01	Export Trusted logs	Same as in UCG-14-05.
UCG-12-02	Export Forensic evidence	Same as in UCG-14-05.
UCG-12-03	Explore trusted logs	Same as in UCG-14-05.
UCG-12-04	Visualize trusted logs	Same as in UCG-14-05.
UCG-12-05	Validate evidence block	Make sure that the validation rules are in line with the chain of custody best practices and guidelines, as depicted in D3.2.
UCG-13-01	Retrieve trust level from TMS	No particular considerations.
UCG-13-02	Compute device trust level	If personal data is processed for this Use Case, the processing must be done in accordance with the relevant data protection and privacy laws, as discussed in D3.1.
UCG-14-01	Update device critical OS files/vulnerabili ties	No particular issues identified.
UCG-14-02	Manage available patch databases	As long as no personal data is involved in this process, no particular issues are identified.
UCG-14-03	Curate mitigation policy database	No particular issues identified.
UCG-14-04	Curate forensic evidence database	Same as in UCG-11-01. The issue has been further discussed in D3.2.
UCG-14-05	Store Trusted logs	The relevant discussion on the legal implications of the use of DLT systems for the storage of electronic evidence in D3.2 must be taken into

Cyber-Trust Consortium. All rights reserved.

		consideration. Due to the lack of ad hoc regulation with regards to DLT systems and Admissibility of evidentiary material will have to be discussed on a case-by-case base and in accordance with the relevant national law and case law of the Member State, where the criminal proceedings take place as well as other best practices and guidelines, always under the guidance of a legal expert familiar with the local legal framework and forensics specialists for each specific type of evidence.
UCG-14-06	Store forensic evidence	Same as in UCG-14-05.
UCG-14-07	Notify about updates and security-related issues.	No particular considerations.
UCG-14-08	Match device profile with eVDB contents	No particular considerations.
UCG-15-01	Compute cyber-attack graphical security model	No particular considerations.
UCG-15-02	Compute device risk level	If personal data is processed for this Use Case, the processing must take place in accordance with the relevant data protection and privacy laws, as discussed in D3.1.
UCG-15-03	Compute attack's likelihood and success probability	No particular considerations. Perhaps, to keep in mind in case a legal claim arises against cyber-trust (e.g. related to a false alarm by affected individuals), that it may be necessary to explain how this computation system worked in the specific case and in general, as seen in D3.1 in Section 5.5.7. Thus, it is important to keep all the relevant documentation and take records of all the processes, including the amount of human intervention concerning the decision-making process.
UCG-15-04	Compute a belief on current security status	No particular considerations.
UCG-16-01	Determine device firmware and software through	One-Way cryptographic functions and SMC-based data distribution will be used to ensure privacy. Given the consequences of false positives, the accuracy of the information concerning device profiles must be checked frequently and the possibility of incorrect information must be eliminated to the greatest degree possible. Encrypted data is considered pseudonymous data, and hence, still personal data as explained in D3.1,

Cyber-Trust Consortium. All rights reserved.

	remote detection	Section 5.1. Pseudonymous data is protected under the principles of personal data processing, as depicted in GDPR.
UCG-16-02	Discover network	This would be a measurement of flow, and whilst nodes will be identified, no data enabling identification of persons or location would be analysed. Location data relating to individuals is very likely to be able to identify them. Hence it constitutes personal data, and sometimes it may include special types of data. Data controllers must minimise the amount of such data collected, processed and retained due to risks posed by linked location data. Therefore, informed consent appears to be the most appropriate basis for collecting and processing location data in most cases. More information may be found in the Article 29 Working Party Opinion 13/2011 on Geolocation services on smart mobile devices.
UCG-16-03	Receive intrusion detection system(s) alerts	No particular considerations.
UCG-16-04	Identify and prioritize cyber-threats.	If personal data is being processed in this Use Case, the processing must take place in accordance with the relevant data protection and privacy laws, as discussed in D3.1. Again, it is important to mitigate the risks arising from false positives.
UCG-16-05	Crawl the clear/deep/dark web and update the eVDB.	Since the amount of information being crawled is enormous, the theoretical possibility that some of this information contains personal data cannot be excluded. In the case personal data is processed, as well as in case of doubt, the controller will need to ensure that the processing is compliant with the relevant data protection legislation. Furthermore, when crawling [A10] takes place on restricted access sources will most likely require a kind of authorisation, sometimes by the owner of the source. Depending on the country where the investigation is conducted, accessing restricted fora without authorisation could be considered an interception of content data or a seizure of computer data. Although there is no specific law against web crawling or using publicly available information which has been obtained through the use of automated web crawling tools, the owner of a website may have a claim against the user if the scraping and subsequent use of the scraped information infringes the website owner’s intellectual property rights or, if the user violates the terms of use of the specific website. All these implications have been taken into consideration in D3.1.
UCG-17-01	Remediate Device	In this use case a malicious or fraudulent file, which may contain personal data, will be deleted/removed from the device and may be retained for forensic purposes. One of the main issues in digital forensics is the management of evidence, from the moment the evidence is first identified and collected till its presentation in legal proceedings. This

Cyber-Trust Consortium. All rights reserved.

		timeline of handling constitutes the chain of custody. The chain of custody may determine the admissibility of the evidentiary material to the court. The retained malicious or fraudulent file from a device may contain evidentiary material and consequently, the appropriate forensic and legal experts must make sure that all necessary safeguards are in place, including the fact that the material was collected with means that do not infringe upon fundamental rights of individuals, and the most appropriate and up-to-date handling techniques in the field are used, as described in detail in D3.2.
UCG-18-01	Apply Mitigation Policy on Device	Depending on the mitigation policy, legal concerns may arise. Thus, it is crucial that only the most relevant data is collected and processed and only the most appropriate, reasonable and least intrusive techniques are used, based on the principle of proportionality, serving a legitimate purpose.
UCG-18-02	Retrieve mitigation policy information	Before blocking the connectivity of a device, all relevant risks and impacts must be assessed.
UCG-18-03	Apply network security defense rule	The defense tools selected must be always be proportional and necessary for the purpose pursued. The purpose, in turn, must be legitimate. The least intrusive methods should be always preferred, if they can lead to the same result as more intrusive methods. The impact on an individual´s privacy should be always assessed. The tools should be only activated by certain incidents that are more likely to correlate to criminal activity. Different measures should be selected depending on whether they are intended to tackle serious crime (e.g. cyber-attacks on critical infrastructure) or petty criminality (e.g. small-scale cyberthreats with minor or uncertain impact). This dimension is further discussed in D3.1, Section 3.4.2.2.
UCG-18-04	Notify of device compromise	Same as in UCG-18-03.
UCG-18-05	Compute optimal intrusion response actions	The optimal response should be chosen based on proportionality, on a case-by-case assessment and in accordance with best practices.
UCG-18-06	Define applicable mitigation actions	A case-by-case assessment is significant in order for the most appropriate and the least intrusive means from all the mitigation actions to be selected, with the minimum impact on the user´s freedoms and rights.

Cyber-Trust Consortium. All rights reserved.

UCG-19-01	Update baseline traffic statistics	No particular issues identified.
UCG-19-02	Choose data sharing level	This UC is essential to be well designed because it implies hundreds of thousands of inter-connected devices which contain personal data and may interfere with individual´s privacy. For instance, if the smart home surveillance system of a user is activated, this could imply that the user is out of his/her home at that specific time. It is of paramount importance that the highest level of privacy enhancement and security measures are in place, whenever monitoring activities entail the risk of being exploited by an adversary or an unauthorised third party to gain access to special types of data or information which can expose patterns or other specific aspects of an individual´s life. The possible damages caused by such an exploitation can impact both the psychological and physical spheres of a user and interfere with her/his right to privacy. Hence, the information collected should always be the minimum necessary for the purpose pursued, the purpose should be legitimate, and the methods used assessed under the principle of proportionality. All data protection principles must be safeguarded, and in particular, privacy and data protection by design and by default should ensure that the least intrusive available means will be implemented. Data security measures should make sure that the data will not be accessed by unauthorised entities internally or externally, as opposed to the individual´s will and even in the case of a breach incident, the data must be in such a way technically engineered, that it would render it unexploitable in the hands of a third unauthorised party. A detailed overview of the risks and implications of a user´s choices with regards to data sharing must be easily accessible, intelligible, written in plain and clear language. Moreover, it must be clear that the user can revoke her/his consent at any time. This is important for seeking a valid informed consent from the user. The issue has been in detail discussed in D3.1.
UCG-19-03	Change Device configuration	It has to be designed in such a way that the likelihood of false positives is eliminated.
UCG-19-04	Tune the crawling parameters and evaluate existing seeds.	Same thoughts as in UCG-16-05.

Cyber-Trust Consortium. All rights reserved.

8 Pilot Infrastructure

The execution of the pilot will be hosted by MTN. MTN is the largest private telecommunications providers in Cyprus, offering integrated telecommunications solutions for mobile, fixed telephony and broadband services, providing pioneering solutions for private and business clients, serving more than 400K residential customers and 8K business customers and enterprises. MTN's mobile network consists of more than 570 base stations supporting 2G, 3G, 4G and 4.5G technologies. MTN research laboratories are equipped with advanced testbeds for WiMAX, 3G and LTE base stations. Wireless access networks are directly connected to the corporate backbone network of MTN and to in-lab application servers, giving the opportunity to test various end-user access scenarios (fast internet, VoIP, IPTV, surveillance, location-based services, etc.). In particular, the MTN´s Measurements and Wireless Technologies infrastructure offers advanced cellular network simulators capable of realistically reproducing current cellular network deployments and topologies, thus offering a general platform for testing new technologies, protocols and models in practical scenarios. For the Cyber-Trust project, and in order to accommodate all use case scenarios that are to be executed, a dedicated testbed environment is to be setup reflecting the real-life environment and any restrictions (network or other) that are important to be taken into consideration. The two domains are to be supported as is diagrammatically depicted in Figure 8.1; part of the Mobile and Broadband networks are to be configured in particular in such a way so as isolate the test scenarios to be executed. Both the Smart Home environment setup (Domain 1) and Mobile clients (Domain 2) are to be connected via the Mobile and xDSL Networks via dedicated network configurations. The testbed is going to also accommodate the servers and equipment required to allow the Cyber-Trust platform to run as well as the virtualization of any other modules required. Via the configuration and routing that is to be done parts of the devices and/or equipment are to have access to the public internet, as required for activities demanding such access.

Cyber-Trust Consortium. All rights reserved.

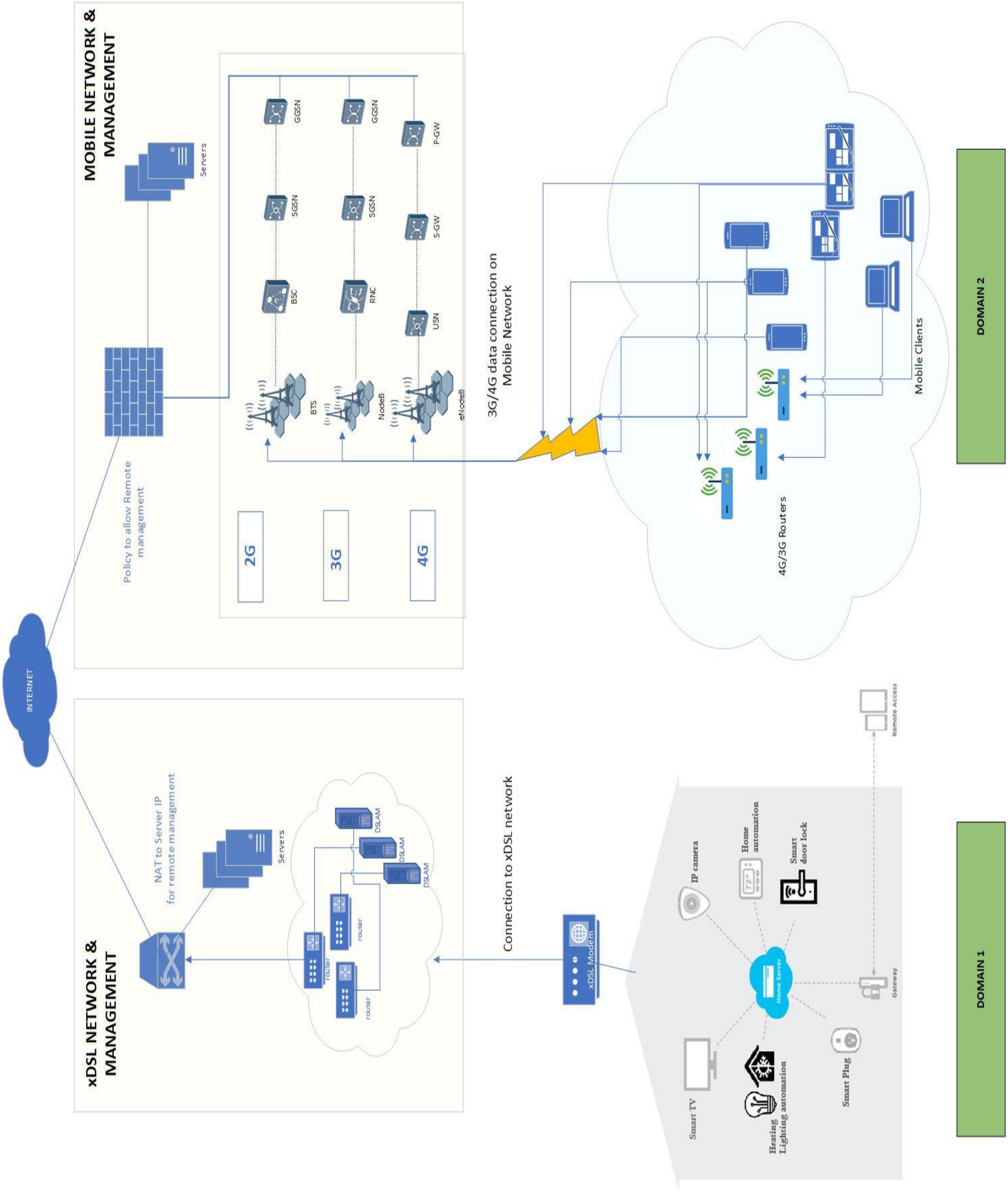

Figure 8.1: Pilot Infrastructure

Cyber-Trust Consortium. All rights reserved.

9 Conclusions

This deliverable overviewed and critically evaluated Cyber-Trust project main components behavior in two domains: Smart Homes and Mobile Devices. The two areas were mainly selected due to their prevalence and the ubiquity of devices within any typical context, from residential use to commercial and enterprise architectures relying on them. For these domains, a set of use cases and associated actors are defined, making the deliverable the stepping stone for the development of the Cyber-Trust architecture in WP4, Deliverables 4.1 and 4.4.

The purpose of the use case scenarios is to define, investigate, and evaluate how the Cyber-Trust system would react in the context of the two areas when mitigating botnet attacks targeting the protected ecosystem. From the domains in Section 4 and 5, 82 use cases were identified which provide the capabilities highlighted by the technical objectives and present a coordinated solution. It is worth noting that the design of the use cases aims to provide a comprehensive set of scenarios to conceptually stress-test the proposed system, rather than act as an exhaustive validation set. Both use cases and actors are applicable across all the scenarios, and described as part of the methodology, that also introduces specific metrics for measuring alignment with the GDPR to ensure that capabilities within the Cyber-Trust solution does not deviate from established data protection legislation and regulations within member states.

As aforementioned WP4 will translate these hypothetical scenarios into a more detailed specification that will then feed WP8 which is responsible for implementing the pilots to test and validate the Cyber-Trust platform. The Use Cases of this deliverable will be used in order to create the evaluation plans of the demonstration of the platform while more detailed use case will be created based on this deliverable in order to run the Cyber-Trust demonstration. All the components developed in WPs 5-7 will be integrated in WP8, delivering an advanced platform to better protect CIIs against cyber-attacks and provide enhanced services to their citizens as per Figure 1.1.

Further, D2.5 will consider additional aspects with respect to attackers' strategies in the domains considered in this deliverable. These considerations will build the basis for studying botnets and simulating large scale attacks in the current IoT ecosystem. We envision the use of GNS3 as well as a series of virtual machines and dockers for testbed in order to scale the Smart Home as well as the Mobile Domain, experiment and evaluate of the proposed use cases along with Cyber-Trust innovate components in realistic environment.

Cyber-Trust Consortium. All rights reserved.

10 References

[1] Kar, U. N., & Sanyal, D. K. (2017). An overview of device-to-device communication in cellular networks. *ICT Express*.

[2] Living Map, "The Internet of everything: IoT use cases," 2018. [Online]. Available: https://www.livingmap.com/technology/the-internet-of-everything-iot-use-cases/. [Accessed 30 7 2018].

[3] Dzone, "Home Automation Using IoT," 2017. [Online]. Available: https://dzone.com/articles/home-automation-using-iot . [Accessed 30 7 2018].

[4] MIPS, "Smart architectures for smart home gateways," 2017. [Online]. Available: https://www.mips.com/blog/smart-architectures-for-smart-home-gateways/. [Accessed 30 7 2018].

[5] ENISA, "Security and Resilience of Smart Home Environments: Good practices and recommendations," 2015. [Online]. Available: https://www.enisa.europa.eu/publications/security-resilience-good-practices. [Accessed 2 8 2018].

Cyber-Trust Consortium. All rights reserved.