CYBER-TRUST

ADVANCED CYBER-THREAT INTELLIGENCE, DETECTION AND MITIGATION PLATFORM FOR A TRUSTED INTERNET OF THINGS

INFOCOM WORLD 2020
Michalis Rantopoulos
mrantopoul@cosmote.gr

OTE's LAB INFRASTRUCTURE

This work is performed within the **Cyber-Trust Project** (Advanced Cyber-Threat Intelligence, Detection and Mitigation Platform for a Trusted Internet of Things), with the support of the European Commission and the Horizon 2020 Program, under **Grant Agreement No 786698**

THE FRAMEWORK PROGRAMME FOR RESEARCH AND INNOVATION
HORIZON 2020

Scope of the presenation

The ***Cyber-Trust*** *"Cyber-Threat Intelligence, Detection and Mitigation Platform for a Trusted Internet of Things"* ***software platform,***

is showcasing

how Law Enforcement Agents will be assisted in viewing and receiving information from Telecom/Internet providers and Smart Homes

that potentially holds digital evidences of specific cyber-crimes, in a timely manner.

Cyber-Trust Partners

KEMEA

UNIVERSITY OF PLYMOUTH

Vrije Universiteit Brussel

SCORECHAIN

aditess
Advanced Integrated Technology
Solutions & Services

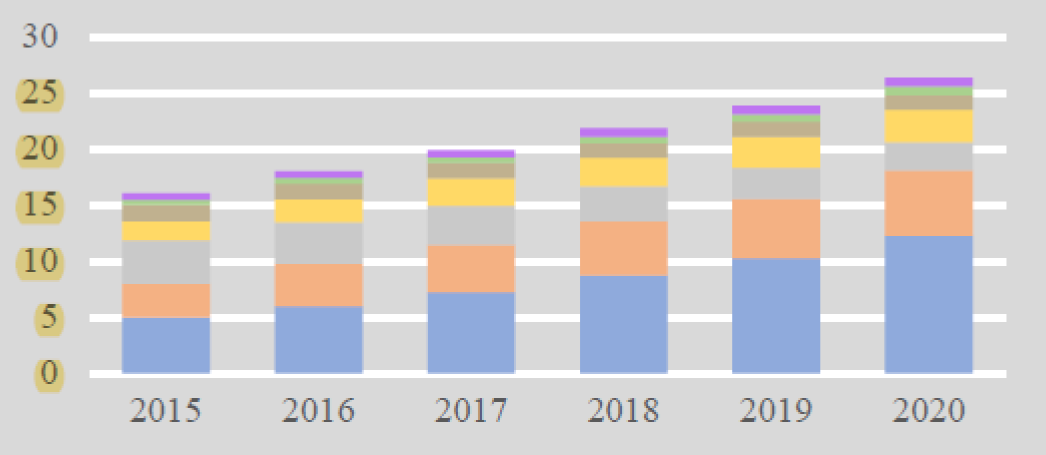
CGI

mathema

OTE
GROUP OF COMPANIES

Growing Demand for IoT Devices

- Vision of *Internet of Things (IoT)* is to establish a new eco-system comprised of heterogeneous connected devices



Global number of devices and connections growth in billions

- Number of connected IoT devices is expected to exceed the number of mobile phones

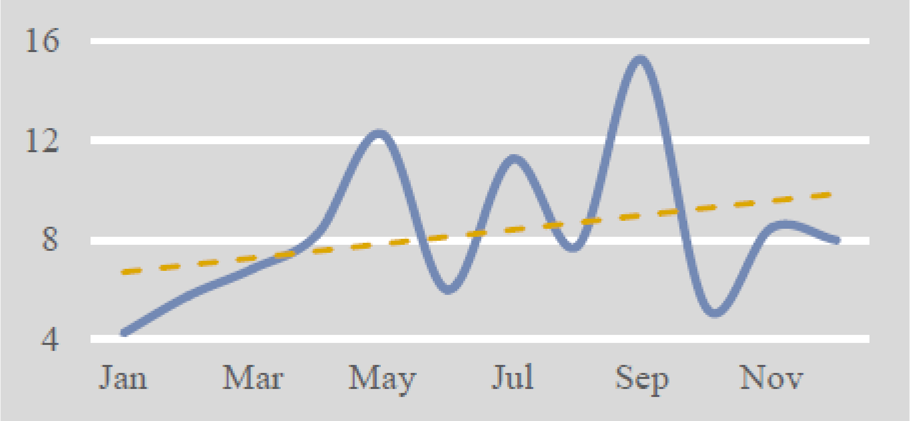
🟦	M2M	(30% → 46%)
🟧	Smartphones	(19% → 21%)
⬜	Other phones	(24% → 9%)
🟨	TVs	(11% → 12%)
🟫	PCs	(9% → 5%)
🟩	Tablets	(3% → 3%)
🟪	Other	(3% → 3%)

Such technological evolution is making our society vulnerable to new forms of threats and attacks, *therefore rendering **Cyber Security** amongst the most important aspects of a networked world.*

Threats

- The fact that the number of the intelligent things (attributed to industries, businesses, and consumers) has greatly increased in the past few years, amplifies any concerns about the security of networked applications and services;
  these may, **rather easily, become targets** of cyber-criminals that are using vulnerabilities traded in the **deepnet** to accomplish their objectives *(e.g. to take control of devices, gain access to applications, deny services to legitimate users, etc.).*

- As cyber attacks become more frequent and sophisticated they attack Internet connected appliances such as **refrigerators, televisions , cameras and cars** in order to *perform DoS (Denial of Service)* attacks



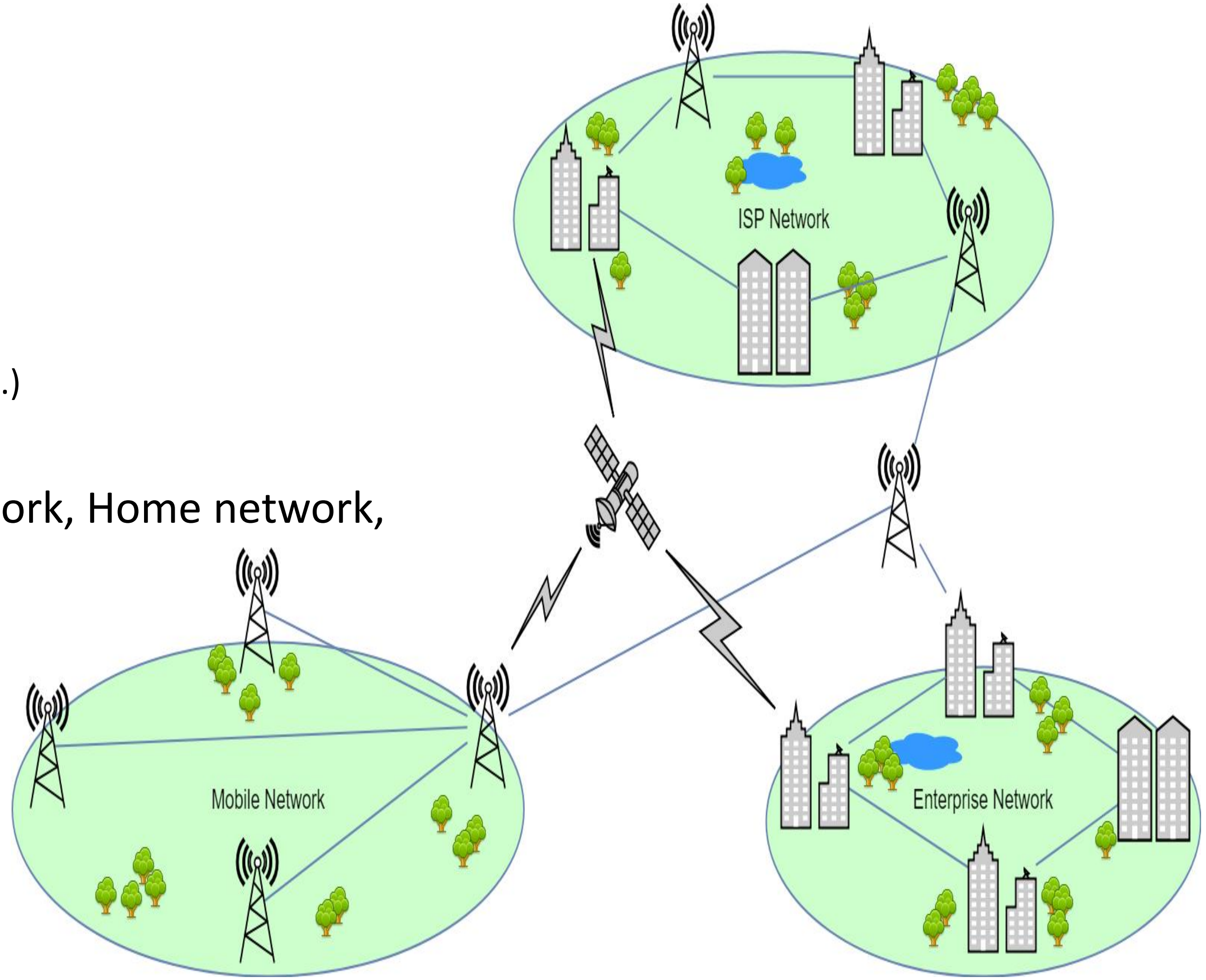
Total number for 2015 of DoS attacks in millions.

- Cyber attacks are capable of delivering anything that is remotely controlled to Cyber criminals:

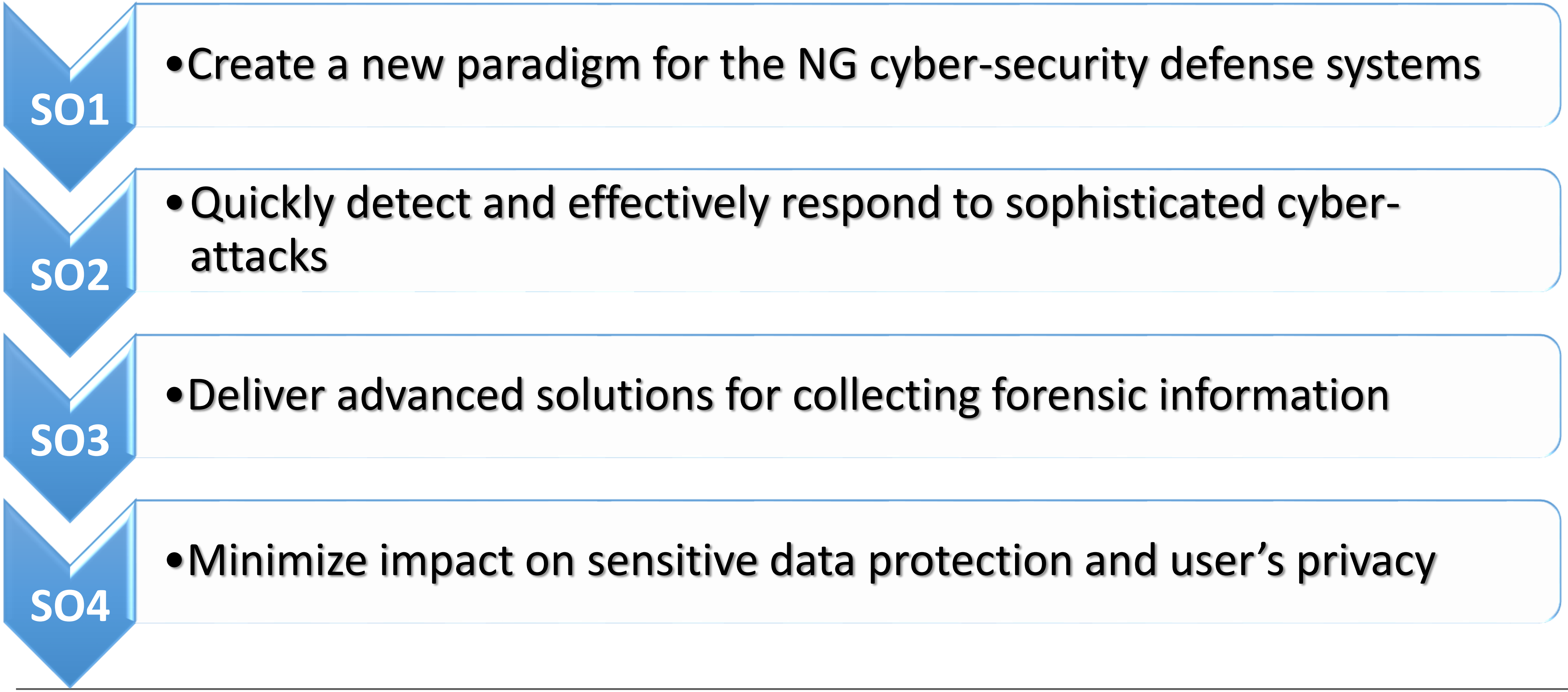
1. May access full control of Drones and Vehicles
2. Computer controlled devices in automobiles such as brakes, locks, engines, steering wheel **currently not connected to external networks
3. Potentially **deadly vulnerabilities** already found in Medical devices (e.g. insulin pumps, x-ray systems)

Cyber-Trust's Inspiration

- **The increasing number of smart devices (IoT)**
- **The increasing areas of applications**
  - ❑ Industry
  - ❑ Cars
  - ❑ Sensors (e.g.: cameras)
  - ❑ House (e.g.: fridge, air conditioner, baby monitor, thermostat etc.)
  - ❑ Wearable devices (e.g.: watches, glasses, etc.)
- **The interconnectivity between networks** (e.g.: ISP network, Home network, Business network, etc.)
- **The massive transfer of important and personal data** through multiple networks.
- **The increasing number of attacks and the appearance of zero-day vulnerabilities** in smart-devices.



Scientific objectives



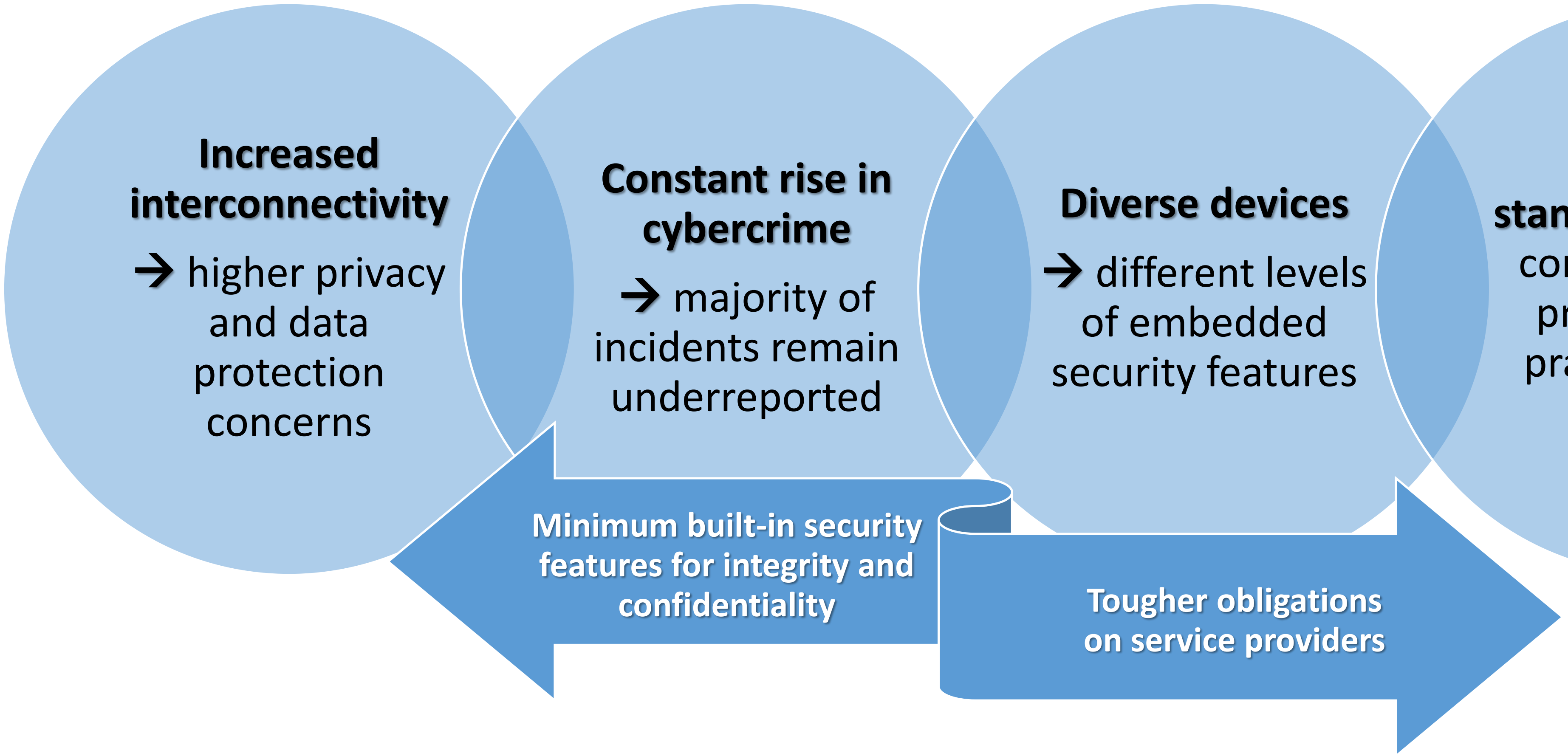
SO1
- Create a new paradigm for the NG cyber-security defense systems

SO2
- Quickly detect and effectively respond to sophisticated cyber-attacks

SO3
- Deliver advanced solutions for collecting forensic information

SO4
- Minimize impact on sensitive data protection and user's privacy

Challenges in a Smart Home environment



Increased interconnectivity
→ higher privacy and data protection concerns

Constant rise in cybercrime
→ majority of incidents remain underreported

Diverse devices
→ different levels of embedded security features

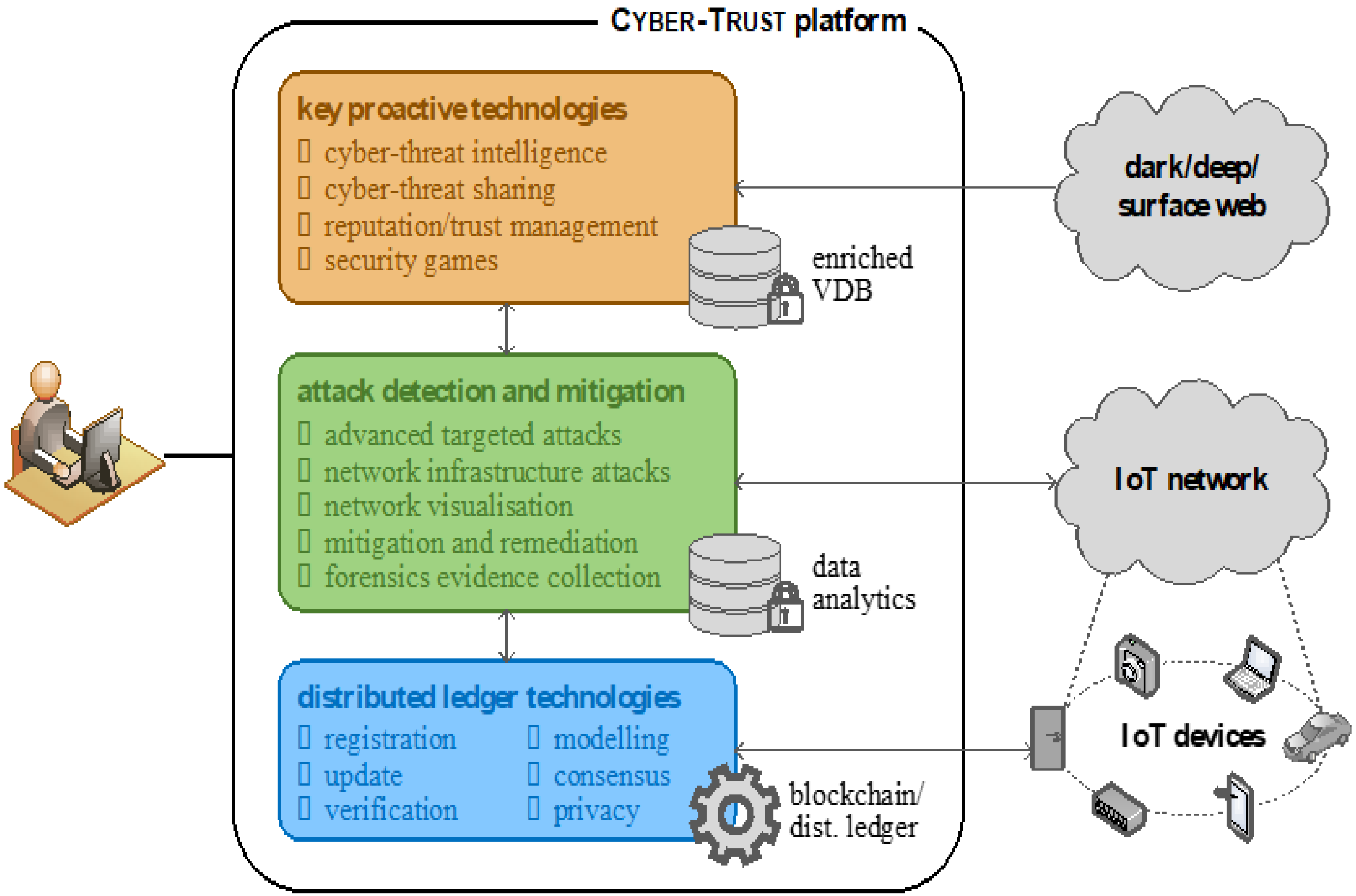
Lack of standardisation in communication protocols and practices in IoT devices

Minimum built-in security features for integrity and confidentiality

Tougher obligations on service providers

The 3 pillars of Cyber-Trust

A holistic cybersecurity solution



CYBER-TRUST platform

key proactive technologies
- cyber-threat intelligence
- cyber-threat sharing
- reputation/trust management
- security games

attack detection and mitigation
- advanced targeted attacks
- network infrastructure attacks
- network visualisation
- mitigation and remediation
- forensics evidence collection

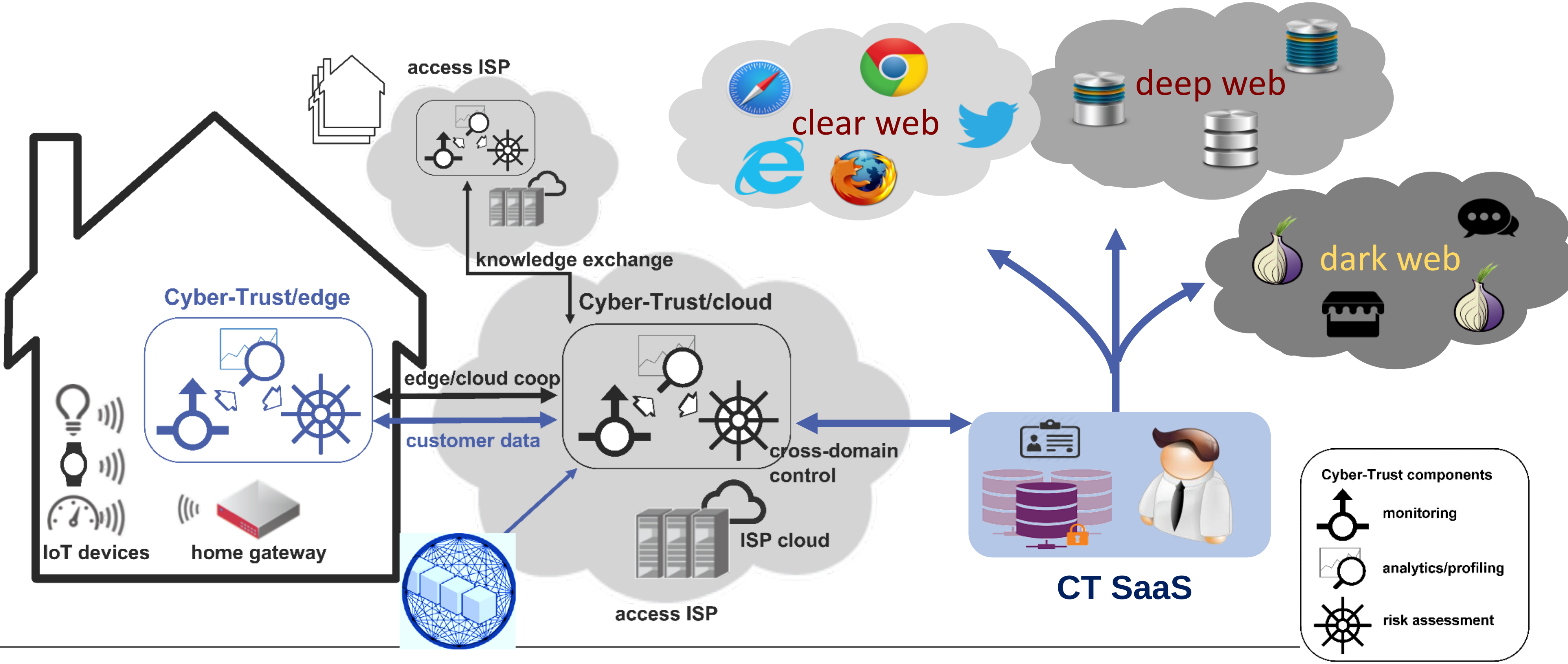
distributed ledger technologies
- registration
- update
- verification
- modelling
- consensus
- privacy

Overview

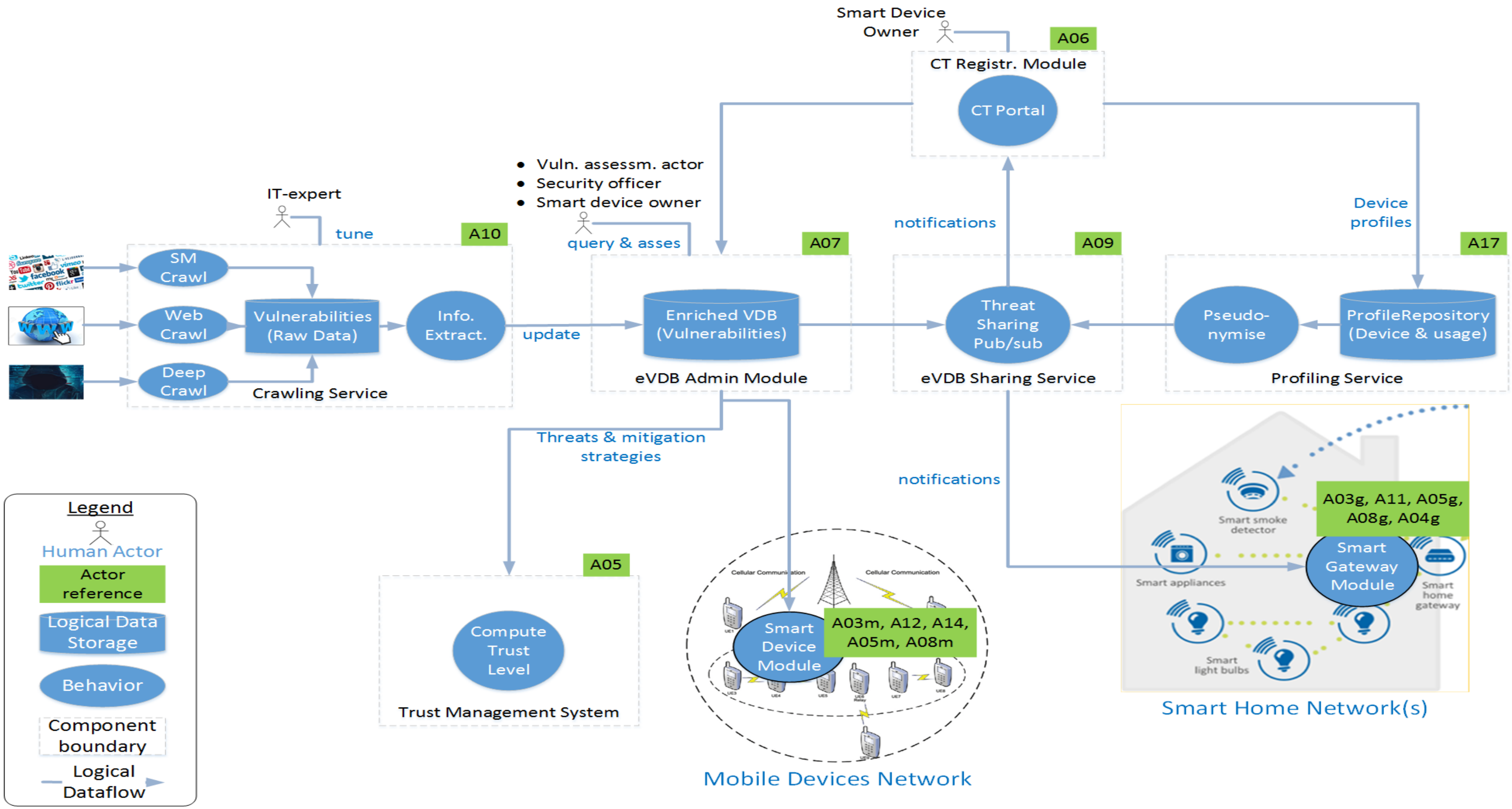
- Cyber-trust project will focus on two domains:
    - Smart Homes
    - Mobile devices in cellular carrier context

- For each domain, appropriate scenarios, capabilities and actors were designed.

- Scenarios are used to illustrate a typical attack and how the Cyber-trust environment will identify, isolate, and mitigate or eliminate the threat.



Conceptual Operational View



Main Cyber-Trust Components 1/2

- Crawling Service (A10) – lies at the Core of the Cyber-Threat Intelligence
    - collects intelligence information from social/clear/dark/web including fora, marketplaces and security related websites
    - leverage information to identify threats for IoT devices
    - storing in the eVDB (*enriched Vulnerability Database*) the leveraged information, thus making it available to the rest of the Cyber-Trust platform

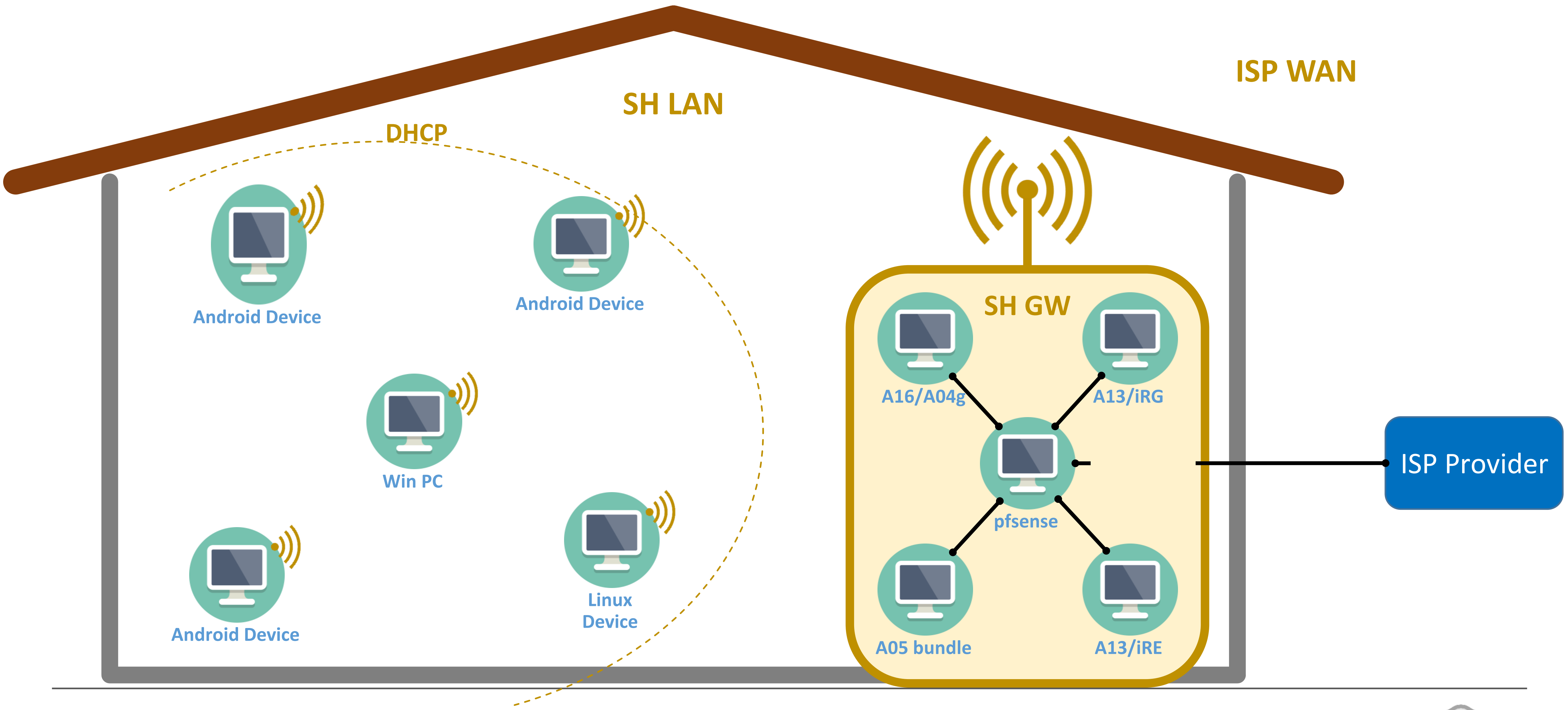
- Profiling Service (A17) – information about users and devices
- Smart Device Module (A03m, A05m, A08m, A12) – acquires information from IoT devices
- Registration Module (A06) – Admin Portal
- Trust Management Service (A05) – plays a **central role** in CyberTrust platform since it undertakes computation of risk level and trust level

Main Cyber-Trust Components 2/2

- **Intelligent Intrusion Response Smart Gateway Module (A13) –** real time monitoring of Smart Home's Security Status
- **Distributed Ledger Service (Blockchain)**
  - The greatest new advantage of Hyperledger is that it will help us to provide the proof that every type of data stored inside the DLT was not altered or corrupted since they are stored. For example, it assures that the forensic evidence was not altered since it was collected to when it comes in a court of law.

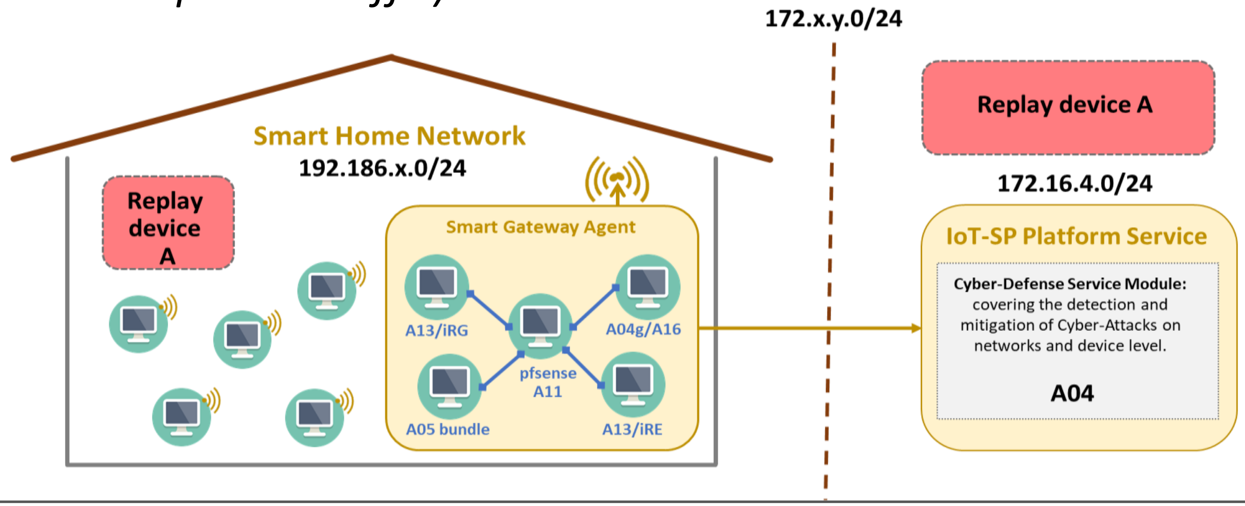
  Hyperledger will help us to assure:
  - ***Integrity****:* No entity has corrupted or altered the evidence during the transferring.
  - ***Authentication****:* The authorized entities that interact with the evidence must provide proof of their identities. For example, only an authorized LEA officer can have access to a specific log he asks access for.
  - ***Verifiability****:* Each entity that owns for a particular time the evidence must verify all the processes.
  - ***Traceability****:* Each authorized entity must be able to trace the evidence, from the moment of its creation until the moment of its elimination
- **Network Repository (A16) –** Database which contains information about topology and security defenses
- **Cyber-Defense Service (A04)** – Databases which contain information on mitigation policies and forensic evidence
- **Visualization Portal (A01) –** Network Monitoring tools (2D & 3D) , provides decision support with feedback from eVDB (A07) as primary source of data
- **enriched Vulnerability Database (A07)** – imports from various sources (free-text) or object sources from Crawler

Smart Home


ISP WAN
SH LAN
DHCP
Android Device
Android Device
Win PC
Android Device
Linux Device
SH GW
A16/A04g
A13/iRG
pfsense
A05 bundle
A13/iRE
ISP Provider

OTE's testbed Future Plans

- Simulation of **750 Smart Homes**
- **Traffic Generation** objective is to analyse and improve the performance of the Cyber-Trust Components : *Intrusion detection System (A13) and Cyber Defense Service (A04) deployed at the Gateway Level (A04g)*:
  - A testing approach has been proposed to generate and replay both dummy and malicious network traffic from PCAP files to the Cyber-Trust components, thus emulating the environment for network security testing
  - *Through a combination of tools such as **Cisco Trex , Ostinato and TCPliveplay** (realistic scenario with real captured traffic)*



CYBER TRUST

www.cyber-trust.eu

@CyberTrustEU

www.linkedin.com/groups/13627755/

@cybertrust

???
Q&A