EUROSMART
The Voice of the Smart Security Industry

INTERNET OF TRUST

SECURITY AND PRIVACY IN THE CONNECTED WORLD

November 2016

FOREWORD

Back in November 2009, Eurosmart published a white paper on the Smart M2M module. At that time, the association was anticipating a massive deployment of connected devices in several sectors of the industry, and claimed that our industry had the technologies to solve the security and privacy challenges at hand.

We can now see that these forecasts are becoming a reality, with more than 3 billion devices already connected and 20 to 30 billion to be connected by 2020.

Our position regarding security and privacy has not changed over the years, and the recent cyber-attacks have further increased our will to be even more proactive in the field of IoT security.

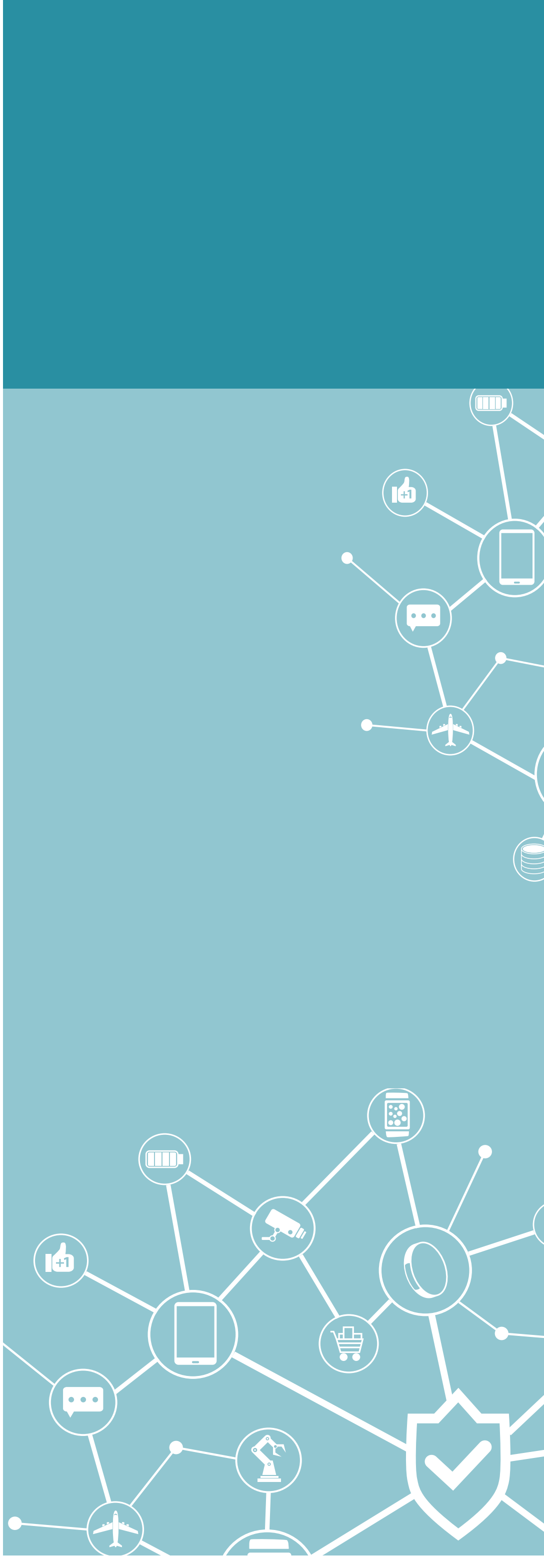
The Eurosmart IoT committee has been working on this position paper in order to share our view on the IoT world, to stress once again the importance of security and privacy within this new technological revolution, and to remind readers that solutions might not be that far off.

I hope you will enjoy reading this document and perhaps even join us in the exciting world of IoT!

Didier Sérodon
President of Eurosmart

EXECUTIVE SUMMARY

KEY MESSAGES FROM EUROSMART



- By connecting billions of devices, the IoT will change our lives and have an impact on society, the economy and the environment;
- Reinforced trust in the system is needed to ensure broad acceptance of IoT;
- Efficient security and privacy mechanisms throughout the system, from the device to the cloud, will be key enablers of trust;
- Security is not yet a priority in IoT systems, and cybersecurity attacks are proliferating. This has prompted Eurosmart to focus on end-to-end security as a matter of urgency;
- Digital security technologies combining secure hardware and secure firmware have proven their efficiency over the years in Telecoms, Banking and ID applications;
- Eurosmart and its members will employ their experience and skills to achieve a safer IoT;
- Eurosmart is also supporting initiatives which aim to create an European IoT Trust Label.

POSITION PAPER

1. IOT DEFINITION AND ECOSYSTEM DESCRIPTION

1.1 DEFINITION

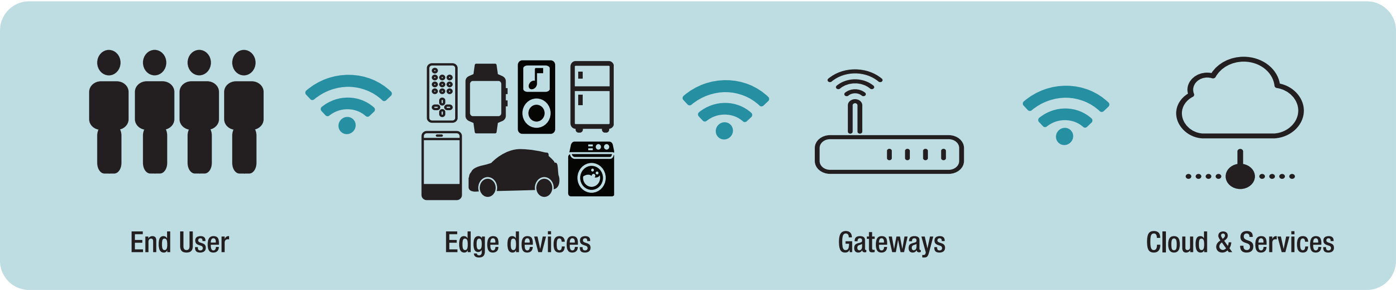
The IoT is an ecosystem made up of interconnected physical devices with the capabilities to detect, collect, communicate and interact through one or several different networks.

This ecosystem acts as the foundation for the creation of new value-added services that leverage existing and future infrastructures requiring security and privacy.

The IoT ecosystem incorporates several intelligence mechanisms that are used either at the edge or at the core to provide valuable services.

1.2 ECOSYSTEM DESCRIPTION

IoT Communication Network



2. IOT MARKET ENVIRONMENT

2.1 FACTS AND FIGURES

No longer just a vision, the Internet of Things and the rise of M2M ecosystems is now becoming a reality. This situation was anticipated by Eurosmart several years ago.

According to market analysts (Machina Research, Cisco, Gartner, ABI Research, etc.), the number of connected devices in use as part of the IoT is expected to reach between 20 and 50 billion units by 2020. Eurosmart's forecasts are in alignment with those of IC Insights, which estimate that 3.5 billion MCUs will be embedded into IoT devices by 2020. Eurosmart also agrees that there will be somewhere in the range of 10,000 IoT projects in the world.

Most applications will be supported by short-range technologies (Wi-Fi, BLE, LPWAN, ZigBee etc.), while cellular networks will continue to be used. The expected deployment of 5G is likely to be a major milestone for IoT connectivity.

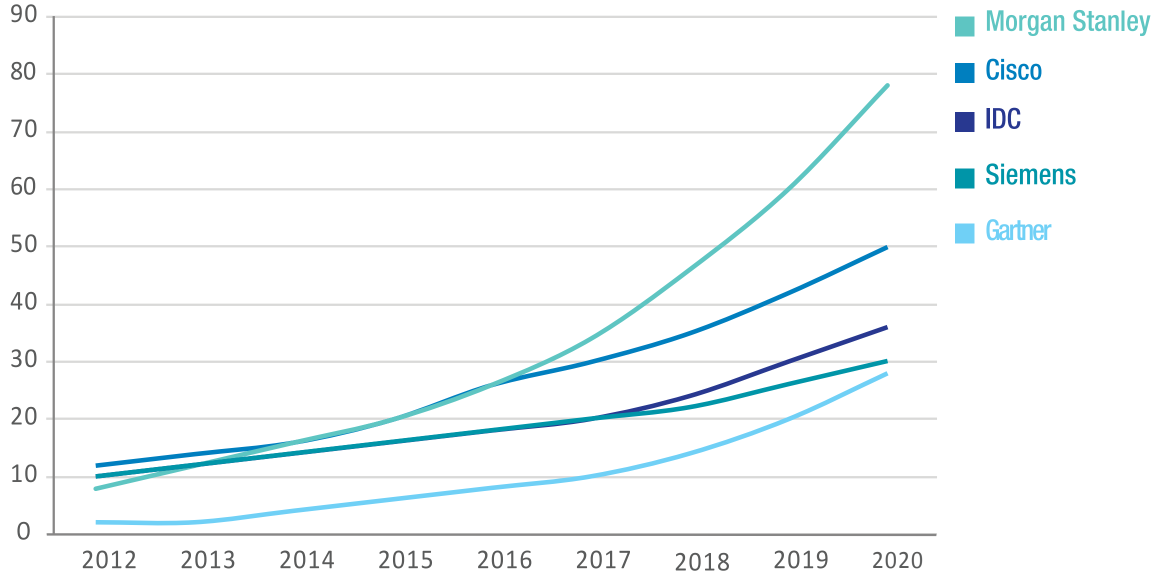
IoT is not just a technological revolution: it will have societal, economic and environmental impacts as well. It will change our lives and the way we interact with the digital world.

> ***"At Eurosmart, we believe that trust in the IoT ecosystem will be a critical factor for broader acceptance among consumers, companies and governments.***

Among other things, this means being able to trust in the device we are interacting with, and trust in the communication and management of our personal data.

Cumulative connected devices

in billon units



2.2 MARKET CHARACTERISTICS

The key learnings from past IoT market analyses and current projects include the following:

Market fragmentation:
The IoT market is a fragmented market, characterized by 8-10 different verticals, and a wide range of applications and use cases that are supported by various connectivity options. According to mapping comparisons, there are more than 60 different applications.

Market standardization:
It is likely that we will have a range of different technologies and connectivity solutions in the first stage of IoT deployment, followed by some degree of harmonization and standardization at a later stage. There are currently about 50 different standardization bodies and institutions working on IoT.

However, Eurosmart believes that market standardisation is not an obstacle for the deployment of security technologies.

Security and Privacy:
Extensive market research studies have revealed that security is often a lesser priority than time-to-market. The root causes of the recent massive cyber-attacks recently reported in Europe and the USA were connected devices (e.g. IP cameras, connected lighting etc.) with no security protection.

The table below is a good illustration of the security and privacy issue. In 2016, only 10% of IoT edge devices are equipped with a security mechanism, and only up to 30% will have such a mechanism by the end of 2018!

2.3 EDGE DEVICE CHARACTERISTICS

Edge devices in the IoT network have certain specific characteristics compared to other connected devices such as smartphones, tablets or computers:

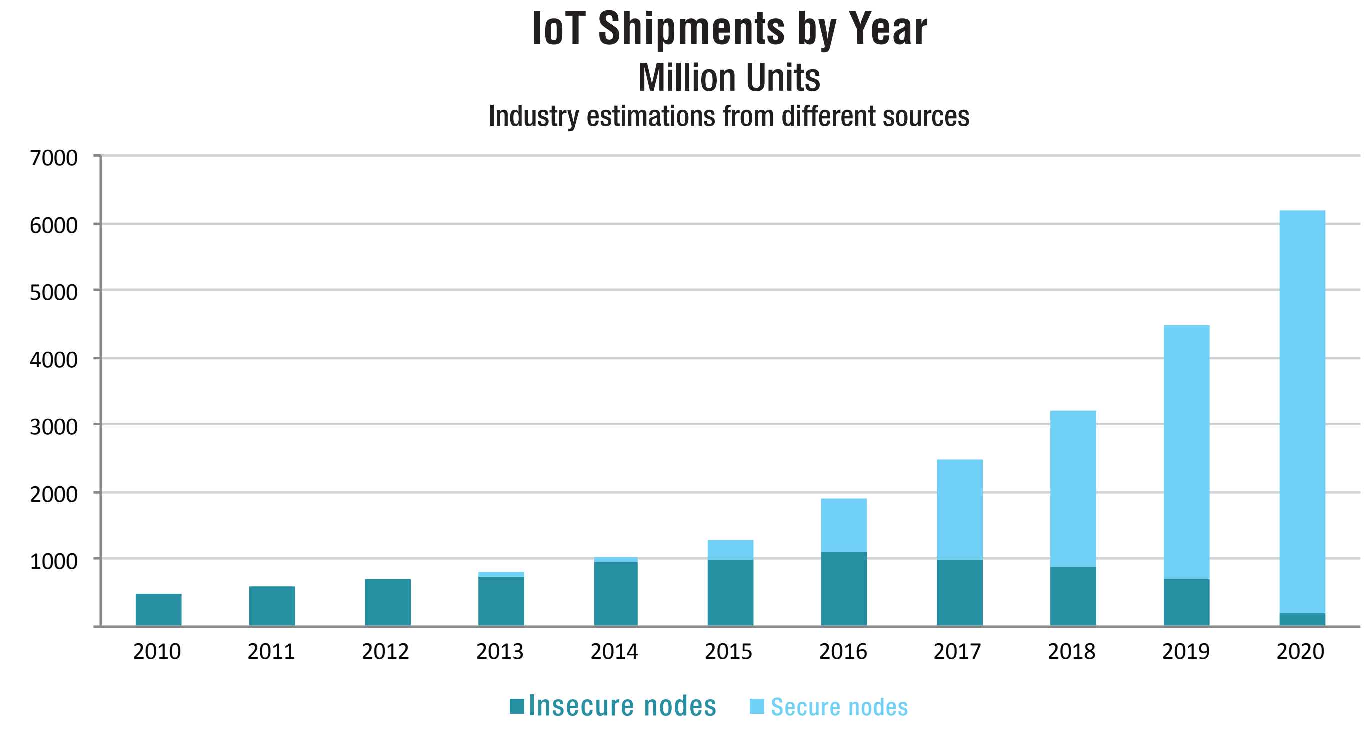
- They are always “on”;
- There is no human interaction with the device;
- They require 10 years or even more battery life;
- They have limited computer capabilities;
- Their footprint must be as small as possible;
- The connectivity bandwidth must be as broad as possible.

It is therefore important to take the above characteristics into account when considering the options for security technologies.

2.4 MARKET SEGMENTATION

As mentioned above, the numerous different IoT applications can be categorized into 8 market segments as per our suggestion below:

- **Consumer Electronics:** tracking, wellbeing, watches etc.
- **Connected cars:** emergency calls, entertainment, diagnostics, navigation, assistance etc.
- **Connected homes and buildings:** energy, appliances, safety & health, automation etc.
- **Smart cities:** lighting, traffic, environment
- **Smart manufacturing (Industry 4.0):** processing, storage, retail goods
- **Smart transit and tracking:** traffic assistance, vehicle tracking
- **Connected healthcare:** telemedicine, assisted living etc.



3. KEY ISSUES FOR IoT DEVELOPMENT AND ACCEPTANCE

3.1 CONNECTIVITY AND INTERCONNECTIVITY

To achieve a broad deployment of connected devices, network infrastructures must be installed in all geographical areas. For instance, a connected car cannot be “disconnected” due to the absence of network infrastructure.

Developing all the necessary protocol translations remains a difficult task, especially with such a wide range of protocols and networks.

3.2 SECURITY & PRIVACY

All market research studies point to the fact that security and privacy are key issues for IoT users. Conversely, security is not yet the priority in most IoT projects. This situation is now coming to the attention of the authorities, including the European Commission, and is likely to lead to strong awareness among all actors in the ecosystem, including edge device providers, service providers, network providers etc.

3.3 POSITION ABOUT AN EUROPEAN IoT TRUST LABEL

Eurosmart advocates for an IoT Trust Label or security certificate for every IoT device provider, covering not only the data protection but also the network that IoT device providers are using.

What is required to get the Trust Label will depend on the target level:

- Self-assessment;
- Self-certification;
- External assessment;
- External certification.

Eurosmart is a founding member of the European Cybersecurity Organisation (ECSO) which contribute to meet the challenge of IoT security. Hence, Eurosmart has several objectives:

- To provide IoT device suppliers with a self-assessment;
- methodology to evaluate the risk their devices are facing with;
- To work closely with the European Commission to implement an IoT trust label that can easily and conveniently be implemented by end-users.

4. SECURITY OF THE IOT

4.1 PERIMETER

Would you be surprised to find out that a connected LED lamp could reveal your WIFI password? This happened a few years ago, and the potential for it to happen was recently demonstrated again by the Weizmann Institute of Technology and the Dalhousie University (New York Times, November 2016).

LED lamps are connected to the home Wi-Fi network and make use of the network password. The password is encrypted and secured by a key. But in this case, the key was not properly protected.

This problem reveals the vulnerable nature of increasing connectivity. It also serves as a reminder that the required protection level is not defined by the value of the device, as you would not consider an LED light as something needing protection, but by the potential threat to your home network.

IoT is everywhere. It is built on different semiconductor technologies, with different types of applications needing varying levels of performance and security requirements.

As soon as sensitive data are trans ferred over the IoT, there is a risk of device manipulation, data and identity theft, data falsification, IP theft and even server/network manipulation.

4.2 RISK ASSESSMENT METHODOLOGY

There are three main categories in the field of security in IoT: confidentiality, authenticity and data integrity.
The main task is to ensure that consumers, their identities and data as well as the devices and infrastructures are protected.

The security industry has been aware of the security mechanisms needed to protect the IoT for many years now:

Authenticity:
The identities and authenticity of users as well as connected objects must be protected by strong identification and authentication methods.

Confidentiality:
Access to sensitive data (transferred or stored) and services must be protected by strong authentication methods and cryptography to guarantee confidentiality.

Integrity:
All elements of the IoT system must be protected against manipulation – this is known as integrity.

An IoT system is generally composed of clouds (storage of device information, processing etc.), networks (firewalls, services, communication etc.), intelligent devices (sensors, processors, actuators etc.) with data collection, data analysis, and initiation of actions etc.

This IoT system may have several layers depending on the use cases:

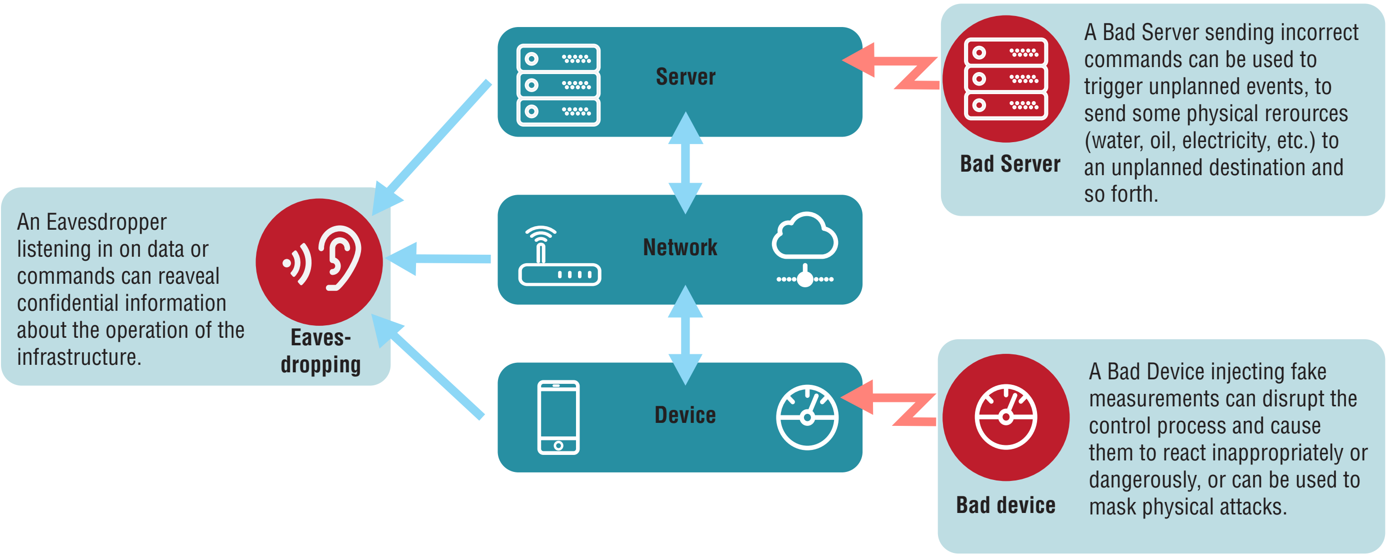
- **A typical industrial manufacturing system** has different levels including the plant level, where there are servers, control computers, central communication hubs etc., the supervisory level which includes industrial PCs, and the field level which includes actuators, sensors, motor control, robots etc.
- **A connected car** is not an isolated entity: internet connection enables new services, local connections can be made to smartphones or tablets, Car2Car communication options are available etc. This broad connectivity makes the car a target for attackers, which, in the worst-case scenario, may also affect the safety of the car.
- **Smart homes** are made up of network cameras, smart lockers, home monitor systems, centralized control lighting, thermostats etc.

To be able to measure and manage the security risk, the IoT ecosystem limits need to be clearly defined.

The risk assessment should take these questions into consideration:

- What do you want to protect?
- What is the value of the items you want to protect?
- What type of attack should be prevented?
- What kind of security level do you want to achieve (i.e. resistance to attacks from an attacker with a given potential)?
- What are the methods andcountermeasures to prevent these attacks?
- What are the potential secondary effects of the protection measures (e.g. on performance)?
- How can security be maintained throughout the lifetime of the equipment?

Risk evaluation


Server
Network
Device
Bad Server
A Bad Server sending incorrect commands can be used to trigger unplanned events, to send some physical rerources (water, oil, electricity, etc.) to an unplanned destination and so forth.
Bad device
A Bad Device injecting fake measurements can disrupt the control process and cause them to react inappropriately or dangerously, or can be used to mask physical attacks.
Eaves-
dropping
An Eavesdropper listening in on data or commands can reaveal confidential information about the operation of the infrastructure.

4.3 EXAMPLES OF SURFACE ATTACKS

An attack can be defined as follows: “An attacker (with a given attack potential) will try to exploit one or several vulnerabilities of a given IoT product (or system). This attack will allow the attacker to obtain assets as discussed in the previous chapter. Depending on the vulnerability type and the attacker’s potential, several attack techniques could be considered.”

Vulnerabilities can be divided into 4 categories:

- **Specification vulnerabilities:** The system specification is weak and could be exploited by an attacker. (e.g.: lack of encryption for communication, storage etc.).
- **Design vulnerabilities:** The system architecture and design are weak and could be exploited by an attacker. (e.g.: insecure cloud interface, insecure device interface).
- **Implementation vulnerabilities:** i.e.Software/firmware/hardware not secured.
- **Misuse vulnerabilities:** The operational guidelines for the product/system are not respected, due to insufficient authentication/authorization (default username/password, weak password etc.) or a lack of network restrictions stopping devices from accessing sites that they are not supposed to access.

IoT systems are based on local and external communications. A lack of communication encryption allows data to be read easily when transferred over networks. In a local wireless network, anyone in the range of this network can potentially read all exchanges between the end-device and the server.

The authentication process identifies the people and the system. Authentication can determine whether the user or device is who or what it is claiming to be.

Identification of users and devices is the first step towards ensuring only authorized people and trustworthy devices can access the network.

In a smart home environment, the endpoint protection afforded by security software is generally good. Most people nowadays know how to protect a computer from viruses, create a strong password, and upgrade security levels through automatic patch updates. But is this enough if other devices are connected to your network?

For instance, network storage devices could be entry points for a hacker. These devices might be compromised and turned into a backdoor for entry into the network. Malicious software can remain undetected if there is no protection against it, and it cannot be deleted if the user does not have permission to access the file system on the device. This type of attack is a clear risk to companies as hackers can access the network without infecting a laptop, workstation or server, all of which are usually protected by firewalls, intrusion prevention systems and existing antivirus software.

Another well-known example is the hacking of a connected car where the Internet-connected computer that controls the vehicle’s entertainment and navigation systems was the entry point for an attack. After gaining entry, malware is silently rewritten to enable the transmission of commands through the car’s internal computer network (CAN bus) to its physical components (engine, transmission, wheels etc.).

Because of their computation capabilities combined with their network connection, IoT devices naturally become easy targets for cyber-attacks. The first cyber-attack involving “smart” objects was carried out against connected refrigerators, and was analysed by California security firm Proofpoint Inc. According to the firm, hackers managed to penetrate network routers, connected multimedia centres, televisions and refrigerators to create a botnet. This type of “zombie” machine network was then used as a platform for sending malicious mail and spam, or coordinating several attacks against critical infrastructures.

This happened again recently to hosting provider OVH, which faced a 1Tbps DDoS (Distributed denial of service) attack launched by a botnet made up of at least 150,000 IoT devices, including cameras and DVRs (source: Security affairs, Sept 27 2016).

Generally speaking, the end user does not receive information from the IoT object when it becomes the target of an attack. This vulnerability will force developers to build secure connected objects, with real time status on their integrity. Without this security barrier, IoT systems could become the silent carriers of massive cyber-attacks.

“

CONCLUSION

Protection levels are not defined by the value of the IoT device, but by the potential threat to the network infrastructure. Devices therefore need to be carefully designed to tackle this threat and equipped with the correct scalable security level. Monitoring the lifecycle and behaviour of IoT devices must be part of this security environment, so that changes can be tracked, especially within critical infrastructure. Lastly, updates to security protections should also be carefully managed by the system, in an automatic and regular manner, whenever possible.

5. EUROSMART RECOMMENDATIONS

IoT requires a comprehensive security framework and processes to provide a security assurance model, applicable across verticals in a homogenous manner. This security assurance model will help to establish the ground rules for devices, users, service providers and integrators on how each party engages within the ecosystem.

A risk management-based approach should be promoted. The security framework should include scalable security technical requirements to adapt to the various threats and security needs.

5.1 GENERIC, BEST PRACTICES

Standardization, which encompasses a broad set of concerns including connectivity, security and privacy, will play a key role in the uptake of IoT. Since many of the benefits of IoT will occur once widespread adoption has been achieved, connected devices should provide trusted functionality and secure communication regardless of the manufacturer, OS or device technology.

A common framework should be used that establishes a baseline with common requirements for security and privacy for connected devices, operating systems, interfaces and communications to the cloud.

A common, standardized security process for the different sectors should be promoted: for each application, a solutions provider could produce an architectural model, review policies and procedures, and perform a risk assessment and a privacy impact assessment, before developing the security requirements. The security of the IoT solution will then rely on security functions that can be expressed as technical requirements and security levels.

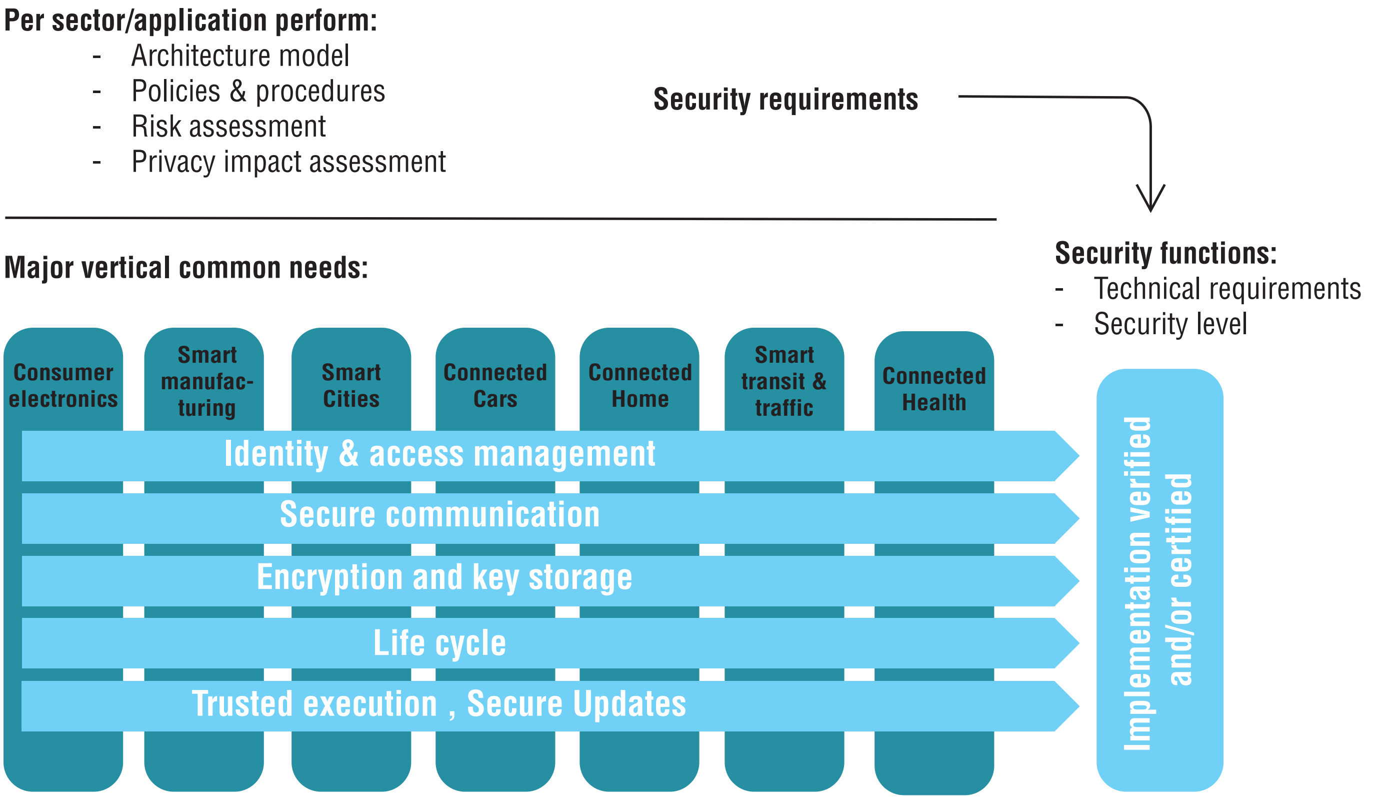
Common technical security requirements should also be developed for all vertical sectors. These should be based on international standards and support relevant security functions such as identity and access management, secure communication, encryption and key storage, life cycle management, trusted execution and secure updates.

An administration framework for IoT devices should include product life-cycle, including credential provisioning, ownership management, device installation and activation, trusted firmware updates, device end-of-life etc. Standardized services will reduce the efforts required to provide users with guidance and result in improved acceptance from end-users.

For each product or service, it is crucial to identify whether security is achievable and requirements are in line with costs.

To adapt to different risk levels, scalable security can be achieved thanks to adequate product selection:

- Activating the security features included in almost all microcontrollers, microprocessors or SoC such as memory access control, memory protection units, firewalls, lock tests, mode locks etc. ensures a very basic level of protection.
- Selecting microcontrollers, microprocessors or SoC with embedded, dedicated security IPs, such as RNG (Random Number Generators), cryptoprocessors, tamper detection, environment monitoring and internal control, TEE (Trusted Execution Environment) etc. provides more developer-friendly tools for mitigating software and non-invasive hardware attacks.
- To mitigate more sophisticated attacks, such as secret key extraction by side channel analysis or differential power/electromagnetic analysis, dedicated cryptographic implementations should be selected.
- The highest level of security involves using specially designed chips to mitigate more sophisticated and state-of-the-art attacks, including chip decapsulation, reverse engineering and microprobing, FIB (Focus Ion Beam) product
- modification, fault injection etc. These mitigation techniques are available on dedicated companion chips, secure elements, or TPMs (Trusted Platform Modules).



Per sector/application perform:

- Architecture model
- Policies & procedures
- Risk assessment
- Privacy impact assessment

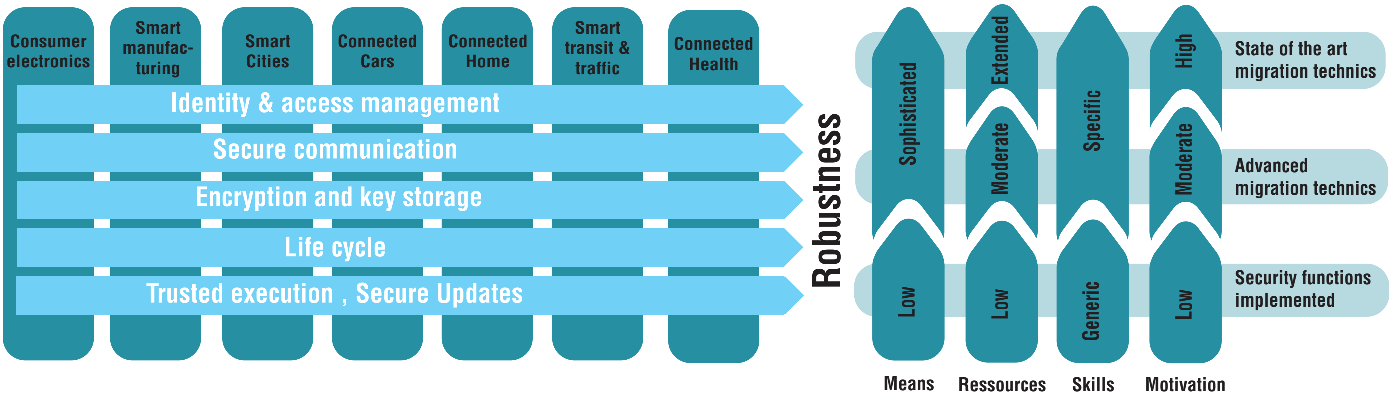
Security requirements

Security functions:

- Technical requirements
- Security level

Major vertical common needs:

Evaluation vs Attack potential



The robustness of security functions depending on the potential of the attacker in methods, resources, skills and motivation should be evaluated.

Security implementation at product level must be tested, evaluated and confirmed in the following procedures:

- **Self-assessment or security checklists** provided by suppliers do not offer sufficiently impartial and reliable assurance of the trustworthiness of a product.
- **Independent evaluation by a third party** is a minimum requirement.
- **IT security certification** is the most common way of accurately assessing the real security level of a product. In Europe, the certification process is based on a jointly agreed upon and internationally recognized procedure entitled The Common Criteria Standards, published as ISO/IEC 15408 and 18045. For customers not requesting full Common Criteria certification, lightweight certification should be used, which is more flexible, cost-effective and compatible with stringent time-to-market constraints.

Standardized classification of security levels based on independent evaluation and certification procedures could be the baseline of IoT security labelling. A European IoT Trust label for cyber-security products would provide clear visibility of the security and privacy achieved by the product at different levels, providing scalable security.

The use of standardized security foundations allows for the creation of synergies across various sectors (e.g. energy, health, transport, finance etc.) as well as the re-use of security evaluations and certifications. For developers, this provides greater accuracy and trustworthiness in the development schedule, reducing costs and time-to-market.

Selling complete platforms or reference designs for IoT devices, along with appropriate training and support tools, could help to increase security pervasion in IoT without jeopardizing time-to-market.

5.2 KEY APPLICATIONS

The common security framework needs to be flexible enough to allow the integration of sector-specific operational issues, and the addition of dedicated application constraints.

Industrial sector:

Security countermeasures, should not cause the loss of essential services and functions, including emergency procedures. Identifying which services and functions are truly essential for operations should therefore be a key step in the risk assessment process.

In IACS (Industrial Automation and Control Systems), standards such as the IEC 62443 series provide a flexible framework for addressing current and future vulnerabilities and applying necessary mitigations in a systematic, defensible manner. It combines the security requirements for IT systems with the strong availability requirements necessary for IACS. System integrators define security zones and target security levels for these zones, distributing these technical security requirements and security levels to product suppliers. Security requirements such as identification and authentication, system integrity, data confidentiality etc. are defined according to a security level based on attack potential. The standards define four security levels, and recognize the Common Criteria highest vulnerability assessment levels (AVA-VAN5) for the levels 3 and 4.

Several national and regional initiatives such as Industry 4.0 (DE), Smart Industry (NL), Catapults (UK) and Industrie du Futur (FR) have developed comprehensive standardization plans and started working on reference architecture. However, since markets and value chains are global, these initiatives must be brought to the European and global level. The European Commission will promote the development of interoperability standards and reference architecture as well as cross-sectorial platforms including for experimentation, validation, interoperability testing facilities and trusted

Automotive sector:

The automotive industry is rapidly evolving. The introduction of innovative technologies such as advanced driver assistance systems (ADAS), as well as V2X communications, is transforming cars into 'high performance computers on wheels'. Wireless interfaces connect the in-vehicle systems to external networks, increasing the attack surface. Use case scenarios for V2X communications have shown a very complex attack environment of real-time and ad-hoc interactions between on-road stakeholders.

Traditionally, the automotive sector has maintained a focus on safety and cost. Nowadays, the increasing amount of electronic and software in vehicles requires security to prevent attacks from hackers and protect user privacy, with significant real-time constraints.

Incorporating security into such firmly established automotive architectures is no small challenge. To address these challenges, developers will propose long-term solutions for protecting cars comprehensively, but should also invest in nearer-term efforts that can produce results for car manufacturers, dealers and customers much sooner. Secure elements are already widely deployed in several vertical segments, with proven solutions for credential provisioning for several device types, demonstrating embedded security solutions for brand protection, communication, smart metering etc. Such security solutions are relatively new to the automotive industry, and will certainly need adaptation.

flexibility necessary for sector specific adaptation. Common principles should be developed, based on scalable robustness requirements, reference security architectures, basic functionalities, and security certification and labelling.

A good example of the evolution of already deployed solutions to meet the needs of the automotive sector is the TPM (Trusted Platform Module). The TCG (Trusted Computing Group) has derived a TPM profile for the automotive sector. This specification describes how a TPM can provide security benefits to the information technology systems in a vehicle. Typical benefits that a TPM can provide include integrity reporting of software and cryptographic key creation, storage, management and use. In the automotive vehicle context, this specification describes scenarios of using TPMs for proving the identity of an Electronic Control Unit (ECU), reporting on the software in use, and remote deployment of maintenance updates.

Another example is the re-use of already widely deployed eSIM for emergency calls from vehicles.

Health:

The great majority of eHealth security challenges are common to any critical infrastructure IT security, but in healthcare systems, services and applications are considered a major concern due to the high privacy and confidentiality requirements of sensitive healthcare data.

Mobile health (mHealth) is a rapidly developing sub-segment of eHealth that is used in medical and public health practices and supported by mobile devices, including the use of mobile communication devices for health and well-being services and information purposes as well as mobile health applications.

In eHealth applications, authorized professionals need continuous access to critical health information in order to ensure the best healthcare services. This systems availability requires secure networks and secure data storage.

Effective and secure health services require a high level of interoperability, as the information needs to be transmitted safely through individual information systems to health service institutions, healthcare providers and patients.

eHealth services (patient summaries, electronic prescriptions, e-referrals, billing etc.), which are usually considered as the most critical areas for security and privacy, have security requirements such as:

- Service availability via component redundancy
- Data format standardisation
- Secure communication and end-to-end security for data exchange
- Reliable and effective electronic identification system that provides the appropriate level of assurance for both medical staff and patients
- Auditable way to record and track the individual operations that make up overall data processing;
- In emergency situations, any access should be logged and subject to audit.

Authentication and access control are key security features in eHealth infrastructures:

- Authentication guarantees the user's identity. Re-use of biometric authentication techniques already deployed in governmental ID should be recommended.
- Access control is one of the main safeguards for ensuring data privacy and integrity. Authorization to access the system is based on role administration. An access control policy should be used to define the information level that authenticated users are allowed to view or share for organizational purposes.

“

CONCLUSION

Synergies across various sectors should be enforced by a common security framework, compatible with the flexibility necessary for sector specific adaptation.
Common principles should be developed, based on scalable robustness requirements, reference security architectures, basic functionalities, and security certification and labelling.

6. OTHER SECURITY INITIATIVES

Through its political initiative, the European Union plans to back the take-off of the IoT. The European Commission is undertaking numerous initiatives in this field. IoT has been recognised as one of the 5 building blocks of the EU strategy for the Digital Single Market. In its communication of 19 April 2016 regarding ICT standardisation priorities, the European Commission stated its intention to foster an interoperable environment for the IoT, involving close collaboration between SDOs and under the umbrella of the Alliance for Internet of Things Innovation.

The European Commission aims to establish reference architectures, protocols and interfaces, promote open APIs, and support the development of missing interoperability standards. The emphasis will be placed on open systems for object identifications and authentications. With the support of the AIOTI, the European Commission is assessing the possibility of developing guidelines and principles, including standards, for trust, privacy and end-to-end security, i.e. a “European IoT Trust label”.

The Multi-Stakeholder Platform (MSP) for ICT standardisation provides advice to the European Commission, based on this expertise. A rolling plan for ICT Standardisation is published annually. The 2016 rolling plan identifies 3 major priorities: firstly, understanding the demands of users with regard to standardisation in the IoT context - including accessibility needs of users - is an top requirement; secondly, establishing cooperation amongst SDOs working on standards landscaping and gap analysis in order to leverage on the results and reduce duplication of work and efforts; and thirdly, addressing the semantics of standards for better data interoperability.

6.1 EUROPEAN TELECOMMUNICATIONS STANDARDS INSTITUTE (ETSI)

ETSI is a non-profit organization with more than 800 member organizations worldwide which produces globally applicable standards for ICT. ETSI is officially recognized by the EU as a European Standards Organization.

ETSI conducts many global activities in the domain of IoT standardisation. It is very active in developing customised technologies for the Internet of Things (such as the DECT ULE, a wireless technology with ultra-low power consumption for Home Automation and Industry Automation applications).

With the support of the Commission, ETSI has developed the SAREF standard (ETSI TS 103 264 V1.1.1), which is the first ontology standard in the IoT ecosystem and provides a template and foundation for the development of similar standards for the other verticals, in order to unlock the full potential of IoT.

6.2 ALLIANCE FOR INTERNET OF THINGS INNOVATION (AIOTI)

The Alliance for Internet of Things Innovation (AIOTI) was launched by the Commission to develop dialogue among the various IoT stakeholders and to promote interoperability and convergence between standards. The AIOTI assists the Commission and plays a role in designing IoT Large Scale Pilots (which will be funded by the Horizon 2020 Programme). Eurosmart is a member of the AIOTI and closely monitors the activities of the WG3, focusing on standardisation, and the WG4, which is currently working to develop an IoT trust charter label.

6.3 THE EUROPEAN CYBERSECURITY ORGANISATION (ECSO)

ECSO is the industry-led contractual counterpart to the Commission for the implementation of the Cyber Security Contractual Public-Private Partnership (cPPP). The cPPP aims to stimulate the competitiveness and innovation capacities of the digital security and privacy industry and ensure a sustained supply of innovative cybersecurity products and services in Europe. A key member of ECSO, Eurosmart is part of the Board of Directors and Partnership Board, and is vice-chair of the WG1 focusing on Standardization, Certification and Labelling.

EUROSMART
The Voice of the Smart Security Industry

ABOUT EUROSMART

Eurosmart is an international non-profit association located in Brussels and representing the Smart Security Industry for multisector applications. Founded in 1995, the association is committed to expanding the world's Smart Secure Devices market, developing Smart Security standards and continuously improving the quality of security applications.

Members are manufacturers of smart cards, semiconductors, terminals, equipment for smart cards system integrators, application developers and issuers who work in dedicated working groups (security, electronic identity, communication, marketing).

Members are largely involved in research and development projects at the European and international levels.

Eurosmart members are companies : **Gemalto, Giesecke & Devrient, GS TAG, Imprimerie Nationale, Infineon Technologies, Inside Secure, Linxens, Nedcard, NXP Semiconductors, Oberthur, +ID, Real Casa de la Moneda, Safran Identity and Security, Samsung, Sanoïa STMicroelectronics, Toshiba and Trusted Objects**, laboratories: **CEA-LETI**, research organisations **Fraunhofer AISEC**, associations: **Pôle SCS, Smart Payment Association, Mobismart, Danish Biometrics**.

Eurosmart is acknowledged as representing "the Voice of the Smart Security Industry".

For more information, please visit www.eurosmart.com

EUROSMART
Rue du Luxembourg 19-21
B-1000 Brussels

eurosmart@eurosmart.com
Tel.: +32 2 506 88 38
Fax.: +32 2 506 88 25