Smart Insights

Security: the key for IoT success

In partnership with:

TRUSTECH

PAY I IDENTIFY I CONNECT & SECURE

WHITE PAPER

Table of Contents

Our market information (qualitative and quantitative) is based on a combination of primary and secondary research, along with our long-standing experience of the industry. Intelling takes no responsibility for any incorrect information supplied to us by manufacturers or users.

The information contained herein is general in nature and is not intended, and should not be construed, as professional advice or opinion provided to the user. This document does not purport to be a complete statement of the approaches or steps, which may vary according to individual factors and circumstances, necessary for a business to accomplish any particular business goal. This document is provided for informational purposes only; it is meant solely to provide helpful information to the user. This document is not a recommendation of any particular approach and should not be relied upon to address or solve any particular matter. The information provided herein is on an “as-is” basis.

Amounts are converted according to recent conversion rates known at time of publishing. The converted amounts are only a gross evaluation and are not intended to reflect accurately the variations of currency rates.

Author: Silvana Pintão - spintao@smartinsights.net

Publication date: July 2017

Published by Intelling, 9 - 13 rue Bel Air, 13006 Marseille, France
www.smartinsights.net-report@smartinsights.net

[1] Source of cover page’s image: To Increase (retrieved from https://tinyurl.com/k9v9vya 29th March, 2017)

1. Overview

The concept of IoT is relatively new, but the IoT itself has been growing for more than a decade now. Over the years, the number of monitoring and control devices has been growing significantly. IoT can be embedded into almost every imaginable type of device: automobiles, home appliances, manufacturing stations, medical devices, x-ray machines, *etc*.

With the addition of connectivity, these devices can now collect and transmit data in real-time that can be analyzed to extract valuable information. Combined with machine learning and behavioral analysis, IoT can derive meaning from data to deliver end-users seamless experiences and help organizations to reach new efficiencies.

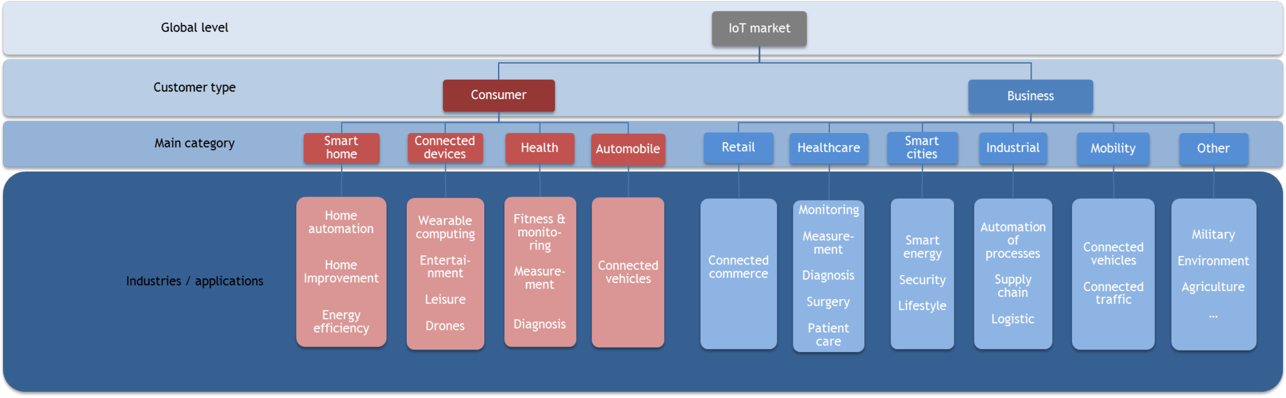
Although the potential economic benefits of the IoT may be massive, they are by no means guaranteed. Recent security breaches, whether on devices, on the cloud or on the network, have put the spotlight on the need for improving IoT and connected devices security before reaching mass adoption.

IoT solution providers must assess their security needs before deploying solutions. Strong security must be included since the solution design and along the entire value chain (end-to-end security). As there is not "one solution fits all" for security, we will see software, hybrid and hardware solutions being intensely adopted in the next years.

2. IoT segmentation

A first segmentation is possible according to the customers' type: consumers or businesses. Consumer IoT includes mainly mass-market connected devices to be used by end-users, while business IoT covers mainly IoT systems used in manufacturing, distribution, buildings and campuses management, asset management, logistics, supply chain management among others. Figure 1 illustrates IoT segmentation in more detail.

Figure 1 - IoT Segmentation



Source: Adapted from *IoT Analytics*

3. Trends and drivers

The introduction of smartphones (and their access to application stores) has revolutionized the way end-users access the internet, marking the beginning of a new era. At this point, consumers have got used to access internet everywhere whenever they want. An increasing number of devices have also been connected to the internet. This was only possible due to:

IoT startups investment

IBM announced in 2015 that it would invest US$ 3 billion (EUR 2.8 billion) to bring IoT solutions to market over the next four years.

- Decreasing production costs;
- Improvement of chip design;
- Strong adoption of consumer devices and mobile apps;
- Expanded internet connectivity;
- Benefits of big data and cloud computing development;
- Investment in IoT startups;

4. Challenges

Though IoT market is anticipated to unleash many opportunities by bringing the benefits of IT and automation to the physical world, many challenges have been preventing further market expansion. These challenges hinder IoT projects from achieving scale and additional benefits, including revenue streams. Consumer adoption is also been damaged. Main challenges preventing IoT expansion include:

- Security;
- Definition of cost effective business models;
- Challenges of big data management, including data storage management and real time business processes;
- Lack of standardization;
- Legacy systems;
- Ease of use for consumers.

IoT security attack

On October 21, 2016, a distributed denial of service (DDoS) was conducted against Dyn, a US internet infrastructure firm, forcing it offline. Consequently, major websites which Dyn is domain name provide, including Airbnb, Amazon, Spotify and Twitter, were inaccessible to users on the Eastern seaboard of the US and parts of Europe.

The attacker(s) launched a DDoS attack against Dyn by exploiting a vulnerability in large numbers of IoT devices like webcams and digital video recorders, then recruiting them all into a single botnet. The botnet bombarded Dyn with traffic, so much that it went down. And consequently, multiple websites.

5. Why we need IoT security

IoT has brought increasing connectivity to end-users. However, this increasing security has its drawbacks: the more devices and points of entry there are on a network, the more opportunities there are for cybercriminals to sneak in. IoT security is only as strong as its weakest link.

Security concerns are driven by the vast amounts and types of data that are being collected by IoT devices, which potentially represent a far greater risk to consumers. This data, in the wrong hands, could be used for nefarious purposes. IoT security includes concerns about theft, privacy, safety and productivity (in the case of business customers).

Not all IoT devices need the same security level. While medical devices, where sensitive health data is passed, may affect patient safety; telemetry units, where unauthorized access can lead to massive privacy breach. Thus, it is the responsibility of IoT device manufacturers to provide appropriate security controls. A major cyberattack may create a climate of fear that will slow down deployments of future IoT systems.

IoT security must be incorporated along the entire value chain (end-to-end security) since the solution's design (security by design). A major issue is the fact that many legacy devices are unable to support security, and new devices do not have security built in by design. From the user perspective, securing IoT depends on a secure device, network and ecosystem incorporating trusted service management, data management and compliance with regulation. Security must be adapted during the solutions' lifecycle according to current system needs and threats. The threats and risks of today are not the same of tomorrow; cybercriminals are constantly evolving and unveiling new creative attacks.

Example - IoT security attack

Nest

University of Central Florida researchers demonstrated how easily a Nest Learning thermostat can be compromised if a hacker has physical access to the device. Within 15 seconds, a hacker can remove the Nest from its mount, plug in a micro USB cable, and backdoor the device without the owner realizing. The compromised Nest can then be used to spy on its owner for example, attack other devices on the network or steal wireless network credentials.

Fitness trackers

Symantec used customized Rasberry Pi computers to draw attention to glaring security holes in fitness trackers. The security experts found that some devices could be easily tracked geographically.

Given the complexity and sophistication of IoT security architectures, stakeholders (OEMs, connectivity providers, cloud service providers, ISVs, *etc.*) must work together to ensure all components and steps in the ecosystem are secured to ensure there are no disruptions. Robust security ensures businesses can benefit from connected business continuity with customers. Partnerships should be an intrinsic part of an enterprise IoT security strategy.

5.1. Securing devices

Security is not a one-off activity, but an evolving part of the IoT ecosystem. Securing IoT devices is just the first step to build an IoT security architecture. It also includes adding a security solution to the device, but also end-of-life device decommissioning, device integration with a new cloud ecosystem or vice versa, managing secure firmware/software downloads, *etc.* Encryption, authentication, and key management are invariably the foundation of meaningfully resilient security. Additionally, secure storage and secure communications, both within and from the device, have to be assured across the network to the cloud.

Currently, devices can be protected with software (lower security), hybrid or hardware solutions (higher security). Software solutions are solutions that typically targeted to the general public, with their affordable cost and easy deployment, while hardware-based solutions with their closed environment have been required for higher levels of security. This reality may be about to change as there are new and more powerful software solutions that might prove good enough for corporations and other providers; or as hardware solutions become more flexible, they may also expand their use cases and may achieve mass deployment.

The development of different technologies has created opportunities for IoT solution providers to choose the most satisfactory solution for their needs (*i.e.* identified on their security risk assessment. These solutions must include classic security functions like encryption, authentication, integrity verification, intrusion prevention, and secure update capabilities.

Moreover, in the long-term, there is also a possibility to combine different technologies, combining the better of each one and adapting security to the user's demands.

5.1.1. Software Solutions

Software is believed to be the most deployed solution currently in the security market. Software solutions include antivirus, antimalware, encryption, firewalls, and more recently solutions in the cloud created by the opportunities of the mobile device world, such as the cloud secure element.

These solutions have lived a faster adoption due to their easy deployment and accessibility to end-users. Software solutions involve few players just, the software provider and the end-user. They are also easy to adopt, the end-user does not need to change his behavior and can easily understand how to implement and manage the solutions. No major adaptations are needed, such as alterations to the device. Software solutions also allow a high level of flexibility, being possible to apply to almost any device. Other positive point of these type of solutions is also its affordable cost.

On the other hand, software solutions are seen as weaker and more vulnerable solutions than hardware-based solutions due to how they are developed. Software solutions rely on signature and known threats, threats that were detected in the past, meaning they do not offer protection against unknown risks. However software solutions are strongly tested in laboratories and research about new threats is constant in order to keep the solutions updated. Also software solutions are not tamper resistant.

Even if these limitations are true until certain point, software offers an appropriate level of security for certain levels of risk. Security is about to choose the good compromise between the risks the user wants to face and the cost he wants to pay for it. However, as risk increases, software limitations also increase. It is necessary to understand how much risk the user wants to take with its security solution.

5.1.2. Hybrid solutions

A hybrid security solution offers an “in the middle” solution for mobile security. It combines both software and hardware in one solution, leveraging the best of these two dimensions. They offer a good compromise between security and cost for end users: it offers highest performance than software solutions, but it is easier and cheaper to implement than hardware-based solutions. Examples of hybrid solutions include Trusted Execution Environments (TEEs) or Trusted Module Platforms (TPMs).

The TEE is an isolated environment built in the main processor of the mobile device that allows processing sensitive code, data and resources separately from the main OS, software and memory on the device. The TEE offers a good solution for secure storage and processing of keys, PINs and biometric data. It is also possible to secure peripherals such as secure memory, crypto blocks, keyboard and screen to ensure they can be protected from software attack. Multiple technologies can be used to implement a TEE, and the level of security achieved varies accordingly.

The main bright point of this solution is its higher level of security compared to software only solutions, due to its hardware architecture. Also as it uses the hardware already existing in the device (the main processor), the cost to implement the solution is minimal. However there is a cost that is usually supported by the handset manufacturer. Even if the TEE is supported by hardware, the management of the TEE is made using software, offering a more convenient option for the service provider than hardware-only solutions. This freedom facilitates the deployment of the solution.

But the TEE is not a perfect solution. Because it relies on an existing processor in the device that is used for other purposes as well, TEE is not resistant to physical tampering and provides only a medium level of security. It also has limited cryptographic key storage capacity for managing access. As a result, the TEE provides good security, but not always good enough. It is not a full replacement for secure elements.

Despite the promising capacities of the TEE, this solution is not yet widely spread. Currently, most IoT devices do not have the processing capacities (or even a main processor) to integrate a TEE. Most IoT devices main capability is to collect and send data. Still, hybrid solutions, such as the TEE, offer good promises to IoT devices with more capabilities, such as connected cars.

5.1.3. Hardware Solutions

Hardware solutions are currently seen as the most secure solutions, because their physical architecture allows higher levels of trust and protection against physical attack than software or hybrid solutions. Hardware-based solutions can be embedded in the device or removable, such as removable Secure Elements (SEs). Embedded security has become the preferred option for IoT use cases due to devices’ main requirements (*e.g.* battery life, processing capabilities).

These solutions are tamper resistant and have a built in root of trust so that with appropriate cryptographic keys it can be used to set up a secure communications channel that cannot be accessed by the host OS or unauthorized applications. Hardware solutions are well-standardized solutions that support encryption, authentication, key management and OTA infrastructure to update devices. Such OTA update capabilities, including software and firmware updates are crucial to maintaining a strong security posture.

But hardware security has also disadvantages. Many IoT devices will be deployed in harsh environments and inaccessible. If compromised, IoT solution providers may be unable to access their devices to replace them. Hardware-based solutions also do not offer the appropriate architecture to migrate solutions.

Still, hardware solutions are getting more deployed and becoming more relevant as risk increases and software shows its limitations. As more flexible hardware solutions become, more application developers and users will be tempted to adopt them. For that it is necessary to bring more flexibility for this value chain and reduce constraints for the adoption of hardware solutions. Critically, as more open is the architecture, major are the dangers for security.

5.2. Securing data

Until now, most of connected devices (*e.g.* smartphones, tablets) had enough computing capabilities to pursue traditional IP-based protocols. Unfortunately, most IoT devices are low power devices with significantly less computing and less cryptographic capabilities than smartphones or laptops. For these reasons, cryptographic operations like encryption and authentication in the IoT world must support both high- and low-power devices.

Most IoT devices are likely to communicate wirelessly and in many cases to run on batteries without maintenance for 5 to 15 years depending on the use cases. Although a few IP-friendly wireless technologies such as 802.11 and cellular 3G/4G have been around for years they still fail the battery life test.

Instead, battery-friendly wireless technologies tend to favor small payloads, extended sleep time, asynchronous behavior and asymmetric communication, very often connecting to gateways with LAN (Local Area Network) connectivity such as Bluetooth, ZigBee, WmBUS, Z-Wave, Enocean, KNX, ioHomeControl, 802.15.4 or more recently without gateways with LPWAN (Low-Power Wide Area Network) technologies. Unfortunately, these IoT devices to not support the Internet Protocol (IP) standard to establish strong authentication with servers.

5.2.1. Authentication

IoT devices will need to operate over the public internet or private networks. They will shuttle data to and from the network. Indeed, it is essential to ensure the user or device is who or what it is claiming to be. Identification and authentication of users and devices is the first step towards ensuring only authorized people and trustworthy devices can access the network.

Mutual authentication is critical for end users connecting to IoT services, for devices communicating to central services, and for peer-to-peer communication between devices. Devices or gateways and back-end servers needs to be identified by each other and mutually authenticated before exchanging data or allowing remote access. Depending on the use case, it might mean:

- A device authenticates a server,
- A server authenticates a device,
- Mutual authentication.

Strong authentication is so important because accepting data from either unverified devices or unverified services can put systems at risk. Such data can corrupt or compromise devices, and give control of those devices to some malicious party who wishes to harm users. Regardless of whether a device is connecting to another device as a peer, or connecting to a remote service, such as a cloud based service, the communications must be protected. All such interactions need robust mutual authentication and trust.

This means that IoT devices and any “nodes” need to get identity and credentials for authentication. Cryptography and PKI (Public Key Infrastructure) technologies might be the best options for deploying strong authentication. Asymmetric cryptography or public key cryptography, contrary to symmetric cryptography, answers to multiple issues of dealing with credentials: storage (in software or secure hardware), issuance, provisioning, updates, suspension/revocation, *etc*.

For asymmetric encryption to deliver confidentiality, integrity, authenticity and non-repudiability, users and systems need to be certain that a public key is authentic, that it belongs to the person or entity claimed and that it has not been tampered with or replaced by a malicious third party. There is no perfect solution to this public key authentication problem. A public key infrastructure (PKI), where trusted certificate authorities certify ownership of key pairs and certificates, is the most common approach. IoT devices manufacturers and industry consortia are already embedding certificates during the device manufacturing process so that each device has a verifiable unique identity.

Moreover, Elliptic Curve Cryptography (ECC) is gaining favor with many security experts as an alternative to RSA[2] for implementing public-key cryptography. ECC is a public key encryption technique based on elliptic curve theory that can create faster, smaller, and more efficient cryptographic keys. ECC generates keys through the properties of the elliptic curve equation. To break ECC, one must compute an elliptic curve discrete logarithm, and it turns out that this is a significantly more difficult problem than factoring. As a result, ECC key sizes can be significantly smaller than those required by RSA yet deliver equivalent security with lower computing power and battery resource usage making it more suitable for IoT devices than RSA.

Many IoT applications will require absolute privacy of data, and this requirement is easily met through use of certificates and encryption protocols. However, where privacy is not a requirement, the data can be authenticated by any party if it is signed on sensor at “time of capture,” and this approach cuts the burdens of link level encryption, which can be particularly important in multi-hop architectures.

6. Privacy

Integral to the discussion of security, it is always the question of privacy and data protection. The discussion around privacy is more relevant than ever. As IoT proliferates, a larger number of players is about to have access to private data and use it to build their business models.

It is important to remember that a majority of the new IoT connected devices are low-cost devices with basic functionality that do not have the necessary security architecture to support strong security. These devices will be one more enter and exit point for data. Being easier to break, these devices may become the preferred enter point for fraudsters to access consumers’ data.

Challenges to IoT solution users’ privacy include traceability / profiling / unlawful processing; repurposing of data; loss / violation of individuals’ privacy and data protection; user lock-in; applicable law, *etc*. New regulations assessing these issues are needed.

Privacy-related policies need to ensure that users understand how their personal data may be used, exercise control over it, and be confident that it will be handled fairly and lawfully. Users should be able to limit the sharing of their data with third parties (including, among other things, for research and marketing purposes) and to revise their decisions at any time.

Therefore mechanisms are needed to ensure that no unwanted processing of personal data takes place and that individuals are informed of the processing, its purposes, the identity of the processor and of how to exercise their rights. At the same time processors need to comply with the data protection principles as data minimization, data deleting, purpose limitation, *etc*.

[2] RSA is one of the first practical public-key cryptosystems and is widely used for secure data transmission.

Indeed, the consideration of data protection requirements should become a mandatory design goal in standardization, as standards can serve as a multiplier for privacy friendly application design. Only this way "privacy by design" and "privacy by default" can become a reality. Information on how to build privacy-friendly applications needs to be provided to IT engineers, system designers and standardization bodies.

However, today, IoT standardization and related legislation are scarce. Many privacy concerns were not assessed yet by competent authorities. Nevertheless, service providers and device manufacturers are employing security solutions which are already applied in other industries, mainly in the telecommunications industry. Mobile Network Operators (MNOs) have long been protecting confidentiality of both information and communications, and therefore users' privacy, through the implementation of solutions such as encryption of communications.

Privacy and security regulations' importance become even more evident in the case of a data breach. Laws around liability from data breaches and privacy must be adopted. As we move to an industry of Internet of Everything (IoE), where not all devices will have the necessary security feature, data breaches will inevitably occur. In addition to trying to mitigate the risks of these breaches, there will be a greater need for cyber security insurance.

International organizations, such as the European Commission, are taking a role in this discussion to try to harmonize solutions and bring common rulings. A good practice being promoted is the creation of a Privacy Impact Assessment (PIA). The PIA is a decision tool used to identify and mitigate privacy risks that notifies the public: what Personally Identifiable Information (PII) data is collected; why the PII is being collected; and. how the PII will be collected, used, accessed, shared, safeguarded and stored. New solution providers must conduct a PIA before releasing their products.

7. Standardization and interoperability

Standardization plays a key role in the uptake of any system. Standardization helps to harmonize systems, making them interoperable across applications, devices and solution providers. Inherently, standardization allows the creation of synergies across various sectors and re-use of security evaluations and certifications, reducing time to market and costs for solution providers, while improving acceptance among end-users.

The promotion of common standards will allow service providers to develop common IoT solutions that can be used by stakeholders alike. Standardizing IoT means that all devices should provide trusted functionality and secure communication regardless of the manufacturer, OS or device technology.

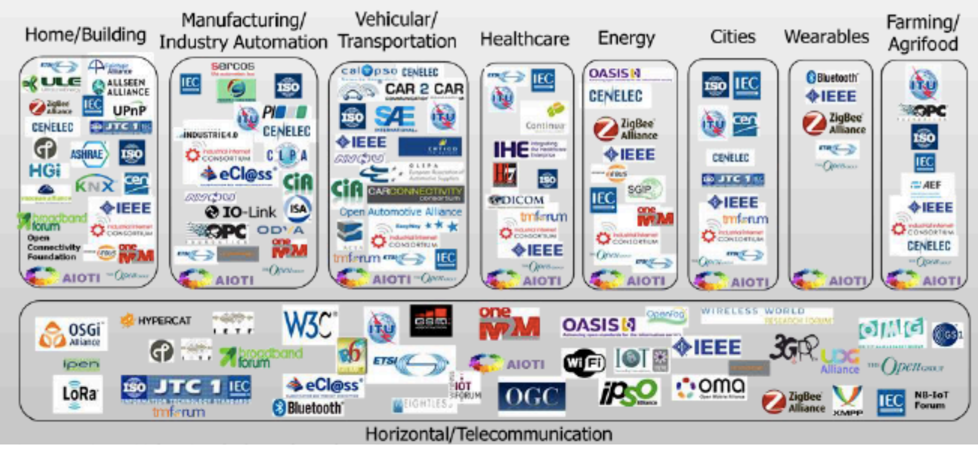
IoT standardization

oneM2M is one of the most advanced standard for an IoT service platform that integrates security services. oneM2M Release 2 supports advanced security services such as end-to-end encryption and dynamic authorization, while Release 3 is expected to further develop interworking with GlobalPlatform compliant security infrastructures. Furthermore, oneM2M enables security integration with established lower layer security standards such as those provided by 3GPP, ETSI NFV, ETSI SCP or the Trusted Computing Group.

New IoT standards must focus on security and privacy for connected devices, operating systems, interfaces and communications to the cloud. Moreover, they should support relevant security functions such as identity and access management, secure communication, encryption and key storage, life cycle management, trusted execution and secure updates.

Today, the lack of standards, official or *de facto*, are a challenge for scalability. Only widespread adoption will unveil IoT benefits. But mass deployments are only possible when interoperability is assured. If interoperability does not receive clear focus and attention, the market will continue to have fragmented ecosystems, limiting its growth. There are currently about 50 different standardization bodies and institutions working on IoT.

Figure 2 - IoT standardization bodies


Home/Building
Manufacturing/ Industry Automation
Vehicular/ Transportation
Healthcare
Energy
Cities
Wearables
Farming/ Agrifood
Horizontal/Telecommunication

Source: *AIOTI*

8. Certification

Standards-based certification testing is a basic building block for device interoperability that sets a minimum bar for product testing. IT security certification is the most common way of accurately assessing the real security level of a product.

Generally, the certification process is based on the Common Criteria (CC) standards. However, CC is frequently too complex, long and costly for smaller stakeholders. Also not all devices and applications need the type of security promoted by Common Criteria standards. For those stakeholders, lightweight certification should be used, which is more flexible, cost-effective and compatible with stringent time-to-market constraints.

Therefore, many companies have chosen to often set up their own integration and interoperability testing to further test and validate device performance. In some cases, device manufacturers buy other devices and set up their own internal testing lab to minimize consumer-facing problems.

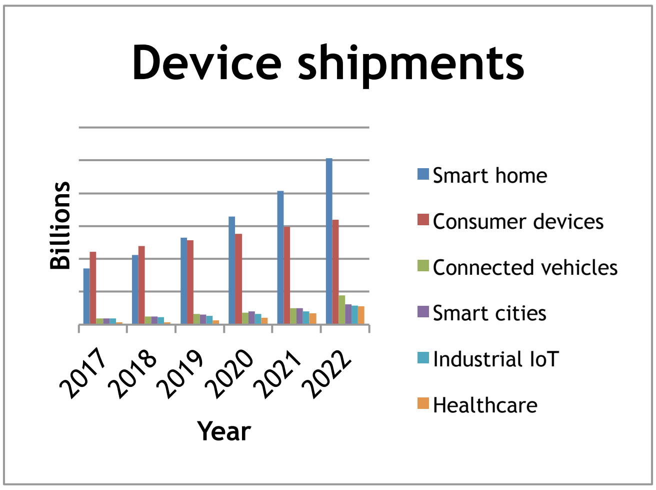
Still, independent evaluation and certification should be promoted. In that sense, multiple stakeholders, including Eurosmart, have suggested the creation of IoT security labelling. An IoT trust label for cyber-security products would provide clear visibility of the security and privacy achieved by the product at different levels, providing scalable security.

Smart Insights Report

Security solutions to expand smart IoT markets

Smart Insights Report "Security solutions to expand smart IoT markets" focuses on secure IoT opportunities in six market segments - smart home, consumer devices, automotive, smart cities, industrial IoT and healthcare. **Smart Insights** also analyzes major trends and challenges, the IoT security architecture and security solutions available, the value chain as well as the positioning and business models of the multiple stakeholders in this industry. Standardization, interoperability, regulation and privacy issues, among others, are also discussed.

This **Smart Insights Report** covers the market landscape and its growth prospects over the coming years (2017-2022). The **Smart Insights Report: "Security solutions to expand smart IoT markets,"** forecasts secure IoT device shipments and their installed base in six market segments. In each market segment, shipments are also calculated according to the type of security solution adopted (*i.e.* software, hybrid or hardware.) Moreover, product and services revenues are also computed for each segment over the forecast period.



According to **Smart Insights Report "Security solutions to expand smart IoT markets,"** by 2022, there will be 27 billion connected devices around the world. Device shipments are expected to grow at a CAGR (Compound Annual Growth Rate) of 19% during the forecast period. IoT security solution providers have an opportunity to collect EUR 21.5 billion in revenues by 2022. These revenues correspond to both sales of security solutions and the security management services jointly delivered.

Smart Insights Report "Security solutions to expand smart IoT markets" has been conducted combining Smart Insights long-standing experience and unique positioning in the secure transactions industry with interviews with key players in the IoT industry. It is an essential tool to all key stakeholders in secure transactions and IoT industries such as solution providers, hardware and software providers, system integrators, standards organizations, technology developers, *etc*.

Smart Insights Report "Security solutions to expand smart IoT markets" is available here: http://www.smartinsights.net/Smart-Insights-Reports

Glossary

API	Application programming interface
CPU	Central processing unit
CAGR	Compounded Annual Growth Rate
DaaS	Data as a Service
DDoS	Distributed Denial of Service
eSIM	Embedded SIM
ISV	Independent Software Vendor
IT	Information Technology
IaaS	Infrastructure as a service
IoE	Internet of Everything
IoT	Internet of Things
LPWAN	Low Power Wide Area Network
M&A	Merger and acquisition
MNO	Mobile Network Operator
NFC	Near Field Communication
ODM	Original Design Manufacturer
OEMs	Original Equipment Manufacturers
OTA	Over the Air
PaaS	Platform as a service
PIA	Privacy Impact Assessment
PKI	Public Key Infrastructure
R&D	Research and Development
RoT	Root of Trust
SaaS	Security-as-a-service
SoC	System on Chip
TEE	Trusted Execution Environments
TPM	Trusted Module Platform
VC	Venture Capital

Published by:
Intelling, 9-13 rue Bel-Air, 13006 Marseille, France
www.smartinsights.net -report@smartinsights.net

Publication date: July 2017