Positioning paper

IoT Cybersecurity vision 2018-2019

Trusted partner for your **Digital Journey**

Atos

Contents

IoT Security Present and Future

The emergence of IoT – the networked connection of people, process, data and things – is expected to significantly grow the number of connected devices worldwide, from billions of units we have today, to tens of billions of units expected to be deployed in the coming years as stated by several analysts:

- IDC[1] states that "By 2018, cloud, mobile, and IoT services providers will own/operate 30% of IT assets in edge locations and micro data centres".
- Gartner[2] predicts that "By 2020, IoT technology will be in 95% of electronics for new product designs (…). While security challenges need to be sorted".
- Forrester[3] recently ranked the Internet of Things the number 1 tech trend from 2018 to 2020.

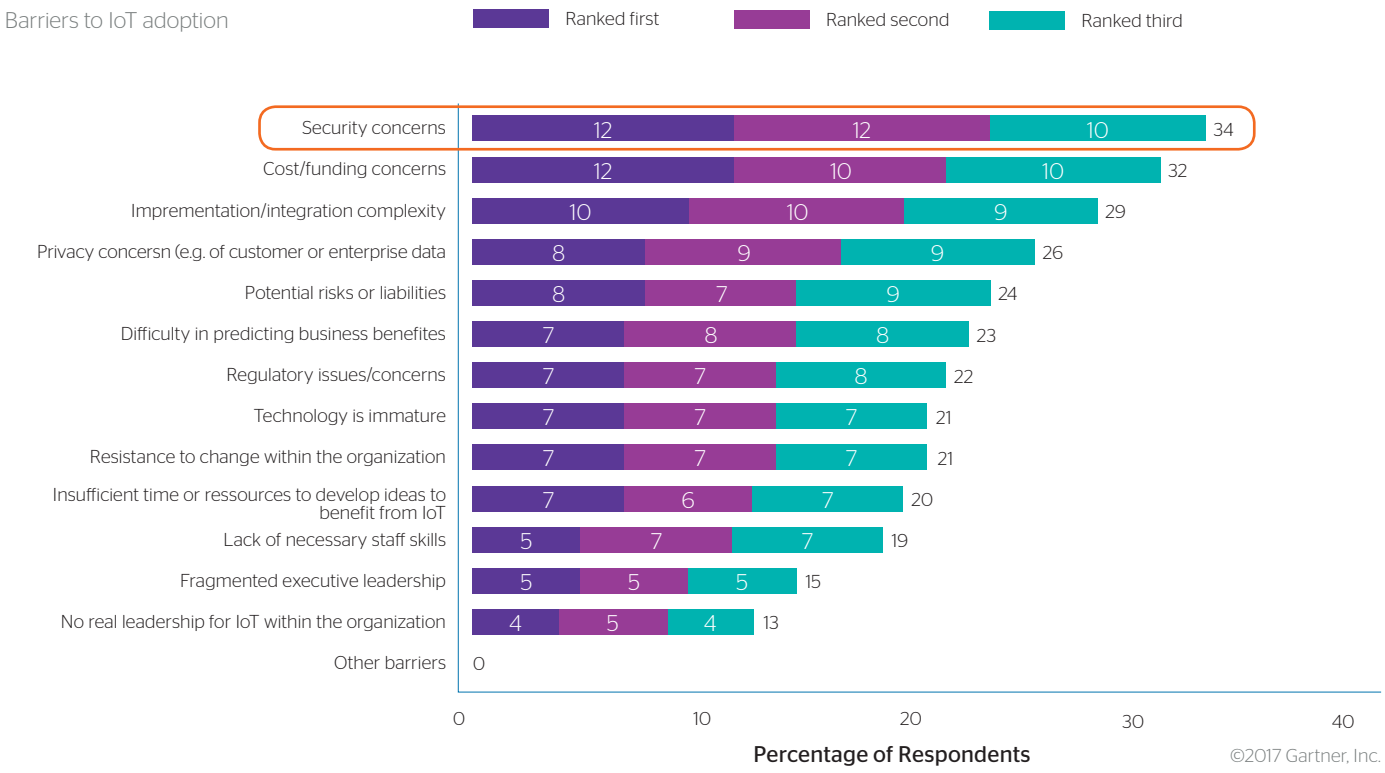
There are still plenty of security challenges to be addressed while the market is continuing to massively adopt IoT technologies. **IoT Security remains the major concern when deploying IoT solutions.** Gartner[4] predicts that by 2022 half of all security budgets for IoT will go to fault remediation, recalls and safety failures, rather than on protection.

Innovation around IoT security is key to enabling safe and effective IoT adoption. Moreover, the increase of compute capabilities outside of the cloud will bring increased complexity to the "edge": this complexity is by its nature less controlled and more exposed to security threats.

There are plenty of entities providing IoT Security services and solutions but there are none covering the overall landscape, especially considering it is such a massive ecosystem with new threats emerging on a daily basis.

Standardization, centralized orchestration and end-to-end management are core drivers, together with an IoT Security framework that converges security controls from Things, or Edge, up to the backend platforms and all communications in between.

Therefore, it is important to obtain a proper understanding of the various categories of IoT Security pain points' in existence today, and what security controls we can put in place to mitigate them.



[1] IDC, Worldwide Datacenter 2016 Predictions
[2] Gartner, Top Strategic Predictions for 2018
[3] Forrester, The Top 10 Technology Trends To Watch 2018 To 2020
[4] Gartner, Top 10 Strategic Technology Trends for 2018

"Things" security

To discuss the security of "things" we first need to define what a "thing" is in terms of IoT.

Gartner defines the Internet of Things as "the network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment[5]. So this gives us a very broad definition of what could be considered a "thing" ranging from temperature sensors to smart plugs to cameras to medical devices up to industrial robots and automobiles (or even discrete parts of these things). The following classification of things is a useful construct in helping to visualise the categories of IoT devices that we can be dealing with:

Class A

Tag

- no processing capability
- no signal transmitting capability
- may depend on external readers that uses radio frequencies to automatically identify and track them as tags that are attached to objetcs

Examples: RFID, barcodes, magnetic stripe

Class B

Single Purpose

- may have some processing capability
- operating system
- ability to communicate with other objects using agreed protocols

Examples: Heat sensors, smart watches, personal health devices

Class C

Integrated

- may have some processing integrated with devices that have other core functionalities
- customized operating system
- processing capability

Examples: Robots in plants, industrial automation devices, connected vehicles, medical equipment

Class D

High End

- similar to Class C devices, and with additional requirement:
- rugged
- highly secure
- highly reliable

Examples: Military and high-end medical devices

[5] Gartner IT Glossary https://www.gartner.com/it-glossary/internet-of-things

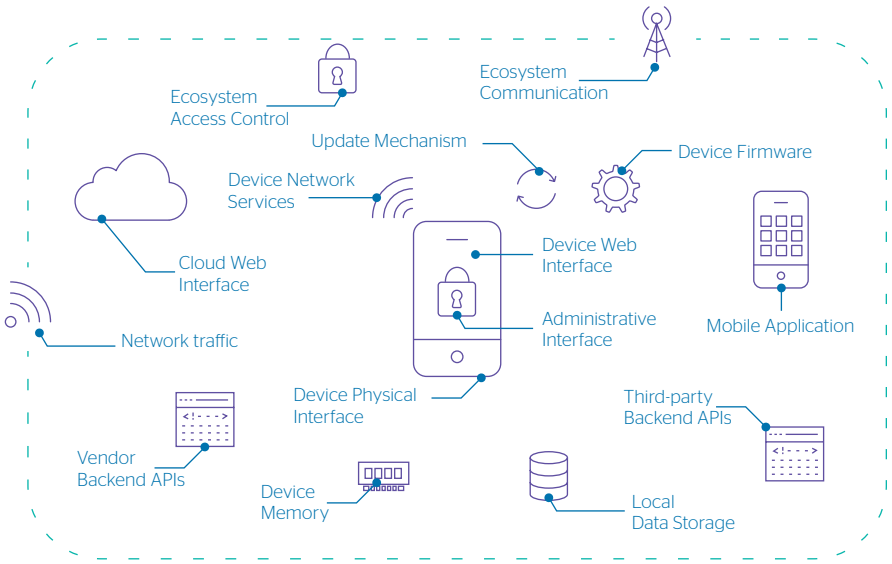
Given the wide variety of these things which have potential to access, store and transmit data, it is not possible to have a single security protocol or technology capable of securing everything to the appropriate level. Indeed, they are ranging from having no security or privacy implications through to sensitive and potentially having national security implications.

We need to look at IoT Security from both an architectural point of view, as well as from a risk based perspective, in order to concentrate our efforts on those things that are at a higher risk of compromising sensitive data. It is the case with audio/video devices located within meeting rooms or data centres for example and less for those which may be highly vulnerable but would only be capable of leaking the temperature of a part of a building or informing that your toast has burned.

Once we have determined the subset of IoT devices that require a higher level of security through risk assessment we then have a range of techniques available to protect the devices themselves. One of the key areas to look at stopping data being leaked from things in general is to look at securing from policy, configuration, patching, network/ edge protection, vulnerability management and asset management. These levels will be discussed in the upcoming sections and concentrate on device level security.

We need to note that some IoT devices, especially those designed for home usage were not designed to be easily upgraded once installed and of course these are not normally part of any monitoring systems and thus are more likely to have vulnerabilities and not be patched. The impact of exploiting these vulnerabilities have been evidenced in recent DDoS attacks where devices such as web cameras, printers etc. have been compromised and added to botnets to be used on demand in worldwide denial of service attacks. The Mirai botnet was a pretty good example creating a 1Tbps attack with 500,000 webcams.

There are fifteen key IoT Attack Surface Areas according to OWASP[6].



As can be seen the scope for vulnerabilities within IoT devices is very broad and each of the areas can be protected only through the overall security approach at each level. Indeed, **defence in depth is the key to security.**

Looking at securing the actual device the key measures that need to be taken are around hardening of the devices and continuous vulnerability management including:

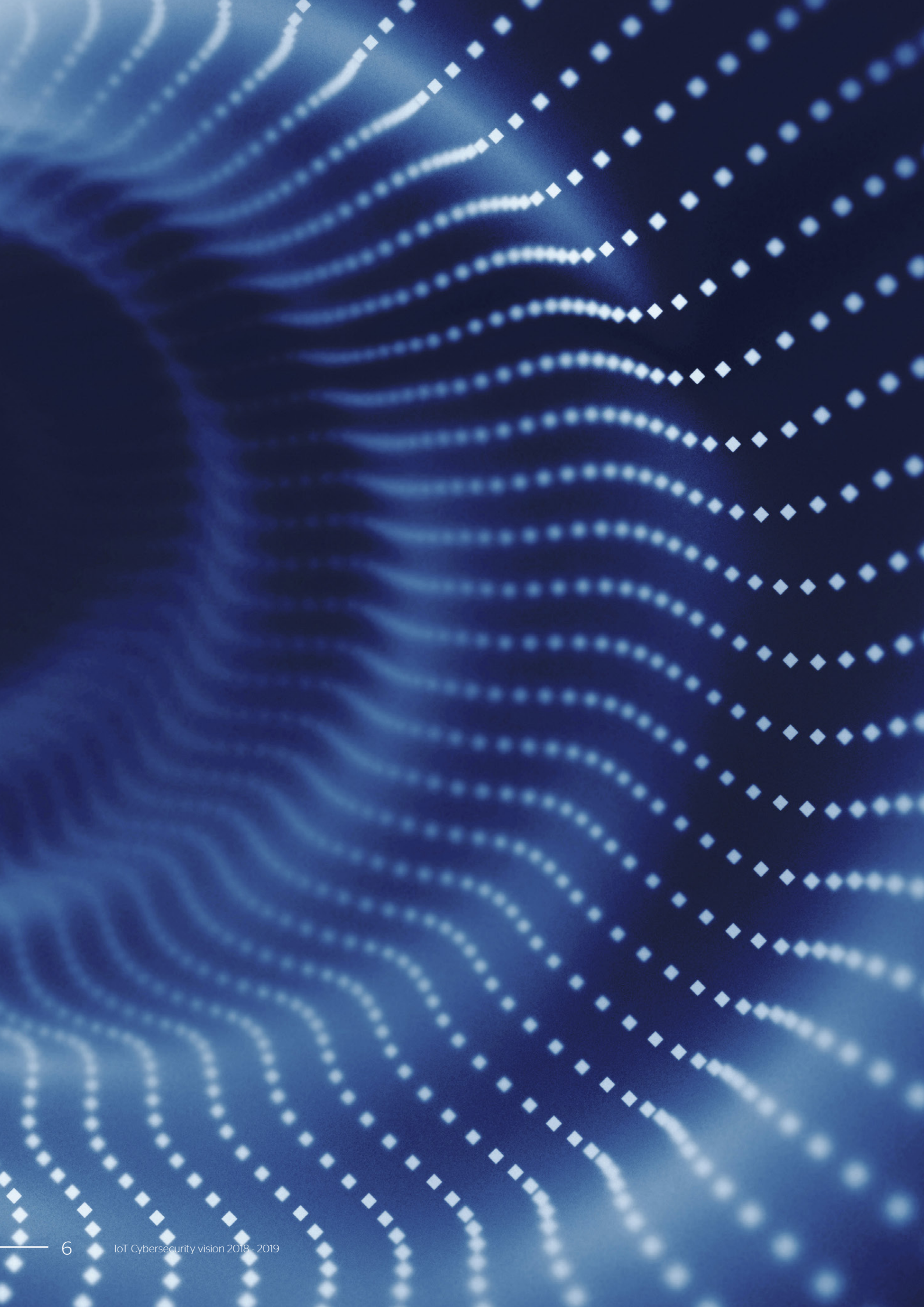
- Change default settings/passwords
- Disable unneeded ports/interfaces/ functionality
- Enable all available security features
- Use of hardware based trust anchors "roots of trust" for trusted boot process
- Use of Cryptographic Embedded Controllers to ensure firmware integrity
- Enable encryption options and force it where possible
- Apply security updates regularly
- Regular monitoring and scanning for vulnerabilities

From an architectural point of view:

- Only permit connectivity to external sources where absolutely necessary/ required
- Encrypt data at rest and in transit
- Ensure physical access is restricted (where relevant and practical)
- Segregate IoT devices on network away from critical/sensitive systems
- Ensure monitoring and asset management in place
- Harden by default

It may have struck you how similar the management of security vulnerabilities is in IoT (especially for Class C & D devices) to how we manage the same on Servers within our environments. So to a very great degree we should look to apply the same defence in depth and hardening principles that we do on our Server estates to our IoT estates. It may seem fairly simple but if you think about it, these devices are in most cases carrying embedded servers. We will keep this principle in mind as we go through the various defence layers which follow.

[6] https://www.owasp.org/index.php/IoT_Attack_Surface_Areas



Edge communications security

In a world where we have IoT networks everywhere, as in the trucks which transport our merchandise, the machines in a factory which are monitored and controlled and even the household appliances and lights which are IoT enabled, we realize that all of this communication with the IoT has to be controlled somehow. This is where IoT Gateways come into place and concept of Edge Security becomes a major consideration.

IoT Gateways will play a major role in the IoT landscape going forward. The reason for their importance is due to the way in which IoT Gateways are converging the world of IoT with the traditional infrastructure space, whether this be on premise or in the cloud. Since the large amount of data which are expected to be produced by the IoT sensors, the IoT Gateway will also play the role of a data controller, and in this case it should offer the following services:

- Data collection
- Data aggregation
- Data filtering
- Data processing
- Data real-time analytics
- Data real-time decisions and actions

IoT Gateways will evolve as well and all the services above might be distributed among different entities in the IoT network, sometimes embedded in Things hence enabling full Machine to Machine communications.

Security for the IoT Gateways services- wherever those are- requires security by design and in depth, since much of the data which will be processed could be classed as confidential or could contain sensitive personal information. Encryption techniques are the most suitable to address such requirement.

Since gateways exist in a variety of environments, and they need to be upgraded and protected against all the latest vulnerabilities, the future leads towards virtualization. Containers which run on different hardware depending on the application, from automotive, to industrial, to power grid measurement systems and residential home control, these gateways need to be upgradable and maintainable with the least possible interaction. Therefore, specifying well defined data providers, listeners, actors and interfaces is essential for allowing automated cloud updates and controls. Of course, the software which is loaded onto each device must be hashed, signed and verified ensuring that changes will not be possible via an unauthorized source.

To ensure the security of the IoT edge communications, we must make sure that the various attack vectors are properly considered. Security areas to focus on:

- **Platform**: it should implement PKI[7], IDS/IPS, Anti IoT DOS or use a Trusted Platform Module (TPM) or Secure Element (SE)[8] as trust anchor, adding vulnerability and patch management as minimum security features.
- **Communication**: for the Edge to be secured we need to consider the security of the internal and external communication. For the internal or local communication where the various endpoints are connected to the gateways we need to have encryption and digital certificates like X509. For the external we need to have again digital certificates and other like 5G, Lora, Sigfox.

As virtualization is in the cockpit, the IoT Gateways will soon become the gateways for IoT Micro Clouds, and will offer all the needed services for Data Collection and filtering. The IoT Micro Cloud will have all the sensors communicating with NCF, Zigbee, Z-Wave, LiFi, Bluetooth etc, and the gateway will communicate to the clouds in a secure manner with 5G, Lora, Sigfox and other.

We can find today relevant developments in the area of edge security:

- An innovative technology is IOTA[9] which brings new capabilities to IoT with automated Machine to Machine transactions and leverages the ledger technology.
- Another interesting and promising technology is the NetFoundry[10] IoT platform and the EdgeX[11] Foundry from the Linux Foundation which tries to build a common open framework for IoT edge computing.
- Atos Horus IoT Security Server fills the gap enabling secure by design IoT Gateways, providing on top a scalable solution and flexible deployment allowing to be tailored to any business needs.[12]

IoT Gateways will take a major part in the future infrastructure, and applying security in all the layers is essential.

[7] https://atos.net/en/products/cyber-security/digital-identities/pki-for-iot
[8] https://atos.net/en/products/cyber-security/digital-identities/smart-card-solution-cardos-for-iot
[9] https://iota.org/
[10] https://netfoundry.io
[11] https://www.edgexfoundry.org/
[12] https://atos.net/en/products/cyber-security/digital-identities/security-server

End-to-End Security Management for IoT

Security Management is crucial for secure and reliable operation of any IP (Internet Protocol) based device. For IT, Security Management has already been standard for many years but today it is often neglected within the IoT world. As a result, billions of IoT components are at a potentially higher risk of becoming compromised by attackers.

To mitigate such risks, IoT Security Management should cover, as a minimum, the following aspects:

- **Asset and Configuration Management** to have clarity about existing IoT devices and their security classification.
- **Patch and upgrade management** for keeping IoT software updated and secure.
- **Security Monitoring** to get visibility on things happen on the IoT devices and their communications.
- **Storage Security Management** to be sure the data at rest will be safe.
- **Platform Security Management**, to prevent unauthorized access and avoid misuse and data alteration or loss. TPM shall play a key role in such platforms.
- **Connectivity Security Management** to make sure data in transit are secure. Digital certificates and encrypted communications should be used.

We will focus on the first 3 topics as we already dealt about Platform and communications through this paper.

IoT Asset management

Asset management has been a challenge for everyone, even when we are moving towards greater degrees of virtualization. Frequently, every management tool deployed in an environment presents a different number of assets under it, be it an antivirus solution or Vulnerability scanners.

The approach for IoT asset management would ideally be based on the individual device reporting itself to the Asset management tool and every other solution should be integrated with that tool. Several existing well-known message exchange protocols like Message Queuing Telemetry Transport (MQTT), Advanced Message Queuing Protocol (AMQP), and Constrained Application Protocol (CoAP) can be used for asset management of IoT devices.

An Exchange protocol should be chosen bearing in mind that they use less data as the potential traffic generated will be enormous.

Another approach is the use of **Distributed Ledger Technology** or **Blockchain** in order to identify a device as it reports itself into a management tool. This approach creates new opportunities in managing identities as a homogeneous group, and opens a range of possibilities in the of asset management for IoT.

Devices such as sensors, and individual smart devices, may be feeding their data to a central server, or a monitoring device which may be keeping track of those sensors and individual smart devices.

In such cases we can get the data on those devices from that central server or monitoring device.

To address the issue of the additional complexities, and potentially huge data volumes, inherent in IoT devices some new approaches will most likely be required. To this end, we can find interesting solutions as the one provided by Forescout, which has developed an extended module for ServiceNow which links their real time and IoT specific information with ServiceNow's CMDB functionality[13].

13 https://forescout-wpengine.netdna-ssl.com/wp-content/uploads/2017/07/ServiceNow-PressRelease_ForeScout_FINAL.pdf

Patch management

Patching IoT devices poses a number of unique challenges compared to what is now taken for granted in IT; these challenges are linked to the characteristics of the devices themselves (what they can do on their own), their operating environment (where they're deployed), their numbers (how many devices are deployed) and their life cycle (for how long they'll be around).

For many users, having to patch their watch or their car as frequently as they have to patch their PC can be a major hindrance to keeping them secure; there must be a better way.

Patching constrained devices

Many devices lack the processing power, memory, storage or overall on-board system capabilities necessary for:

- checking for updates
- validating updates
- testing updates
- installing/reverting updates

Checking for necessary updates and following a consistent update policy across distributed and heterogeneous environments heavily relies on asset management being in place for the IoT system. In any case, relying on the devices to automatically "update themselves" is generally not advisable when consistency is vital.

Albeit cryptographically validated updates (using digital signatures or block-chain techniques such as DLT) are generally advisable, devices' limitations in terms of CPU or power consumption may force that validation outside of the devices themselves. Such a validation would then occur on a trusted local distribution point (updates server), that would check the updates' integrity and origin on behalf of the managed population.

Not all devices support online updates (updates without downtime) and some of them might need to be temporarily pulled offline from production or even physically accessed as part of the update process. Reverting updates might also prove a challenge, forcing a factory reset or replacement of failed devices.

Patching in a distributed and heterogeneous environment

Because of their very nature, IoT devices are routinely deployed in very remote or difficult-to-reach network locations without local IT staff or expertise. Such locations do not fit well with a traditional hierarchical IT segmentation and management approach.

Setting up a local distribution point for updates allows alleviating network bandwidth issues. By checking for updates, checking updates and storing update packages on behalf of IoT devices, the local management gateway allows a more efficient use of resources and a better control over the environment (enforcing a consistent update policy becomes a matter of defining groups of devices for distribution).

Another network bandwidth-saving approach for updates distribution is to use peer-to-peer distribution of updates; this approach has a number of drawbacks, though:

- it requires quite "smart" IoT devices (i.e. capable of propagating updates to their neighbours)
- updates must be validated on-device (i.e. signed)
- isolated devices still need special treatment

Life cycle

The exact life cycle of IoT devices is often unclear (products support matrix, updates roadmap, etc.) and a sheer number of older, obsolete devices can be expected to be around after their end-of-support date (and sometimes even their manufacturer's disappearance).

Patching obsolete or critical devices may be impossible (temporarily or permanently), which means that other work-around methods have to be employed, such as network isolation or filtering.

When patching is not advisable or not possible, partially or completely disabling devices features becomes the only option (a "smart toaster" can probably still be used as a plain toaster).

In conclusion, a successful patching strategy for IoT devices will be a combination of tactics:

Tactics	Preference	Situation
Network "patching" / filtering	As a last resort	Deployment of updates impossible
Signed updates	Always, unless devices are unable to verify	Integrity of updates should be ensured
Local distribution of updates	Consider	Network/devices constraints
Peer-to-peer distribution of updates	Consider	Big population of devices / network constraints
(Partial) de-activation	As a last resort	Updates or vendor no longer available

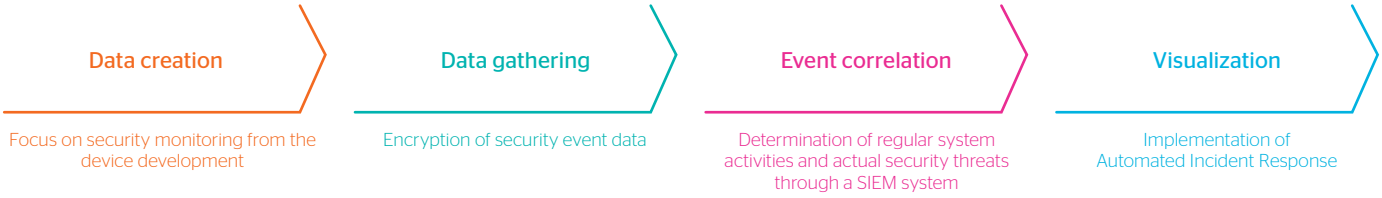
Successful patching strategy for IoT devices

IoT Security Monitoring

One of today's biggest challenges in security organizations is to stay permanently in line with the newest type of security threats. Security Operation Centers (SOC) with their security experts are fighting day by day against malware, abuse of data, fraud and other kinds of cyber-attacks. At the base level of defence a SOC needs to get clarity about the normal and abnormal processes and their entire communications which happen in the infrastructures they are responsible for. Some new technologies such as Behavior Analytics or Pattern Detection definitely contribute to paving the way, but IoT environments are so heterogeneous that the end-to-end monitoring requires further Security Analytics techniques and proper integration among all the monitoring tools.

Only permanent and consequent end-to-end Security Monitoring of the entire IoT infrastructure can provide a clear view about the infrastructure's security health. The IoT devices themselves, the central IoT infrastructure as well as the gateways in between must be in the focus of the monitoring. This fundamental IoT security monitoring method, a so called descriptive monitoring is just reactive. It doesn't prevent from being attacked.

In general, a typical monitoring process looks as follows:



This is similar to other processes in IT Security Monitoring. But on IoT devices there are some specific problems which need to be solved first:

1. Data creation:

In IoT there is a large variety of device types. Operating systems are seldom based on OS standards such as Linux or MS Windows but are very often vendor proprietary. Depending of a device's purpose the technical platform is typically restricted. Beside lower system performance mostly local storage availability is limited. The main questions are: Is the IoT device generally able to generate security log data and if yes, how? And can they be stored locally?

Sometimes the environments around (for instance on network level) could be monitored to fill the gap but this still lacks the device itself. Only the device manufacturers and system programmers can solve these problems. Security monitoring must be in their focus already during the device development.

2. Data gathering

Security event data should be pushed encrypted to the central monitoring systems as soon as they will be generated.

But active pushing, like for instance a syslog daemon does, binds additional system resources and requires on top of this sufficient network bandwidth. Security event data can be pulled alternatively by centralized data collectors which relieve the device from active data pushing. But the polling interval of the collectors, which is typically in the range of minutes, defines the blind phases in the monitoring process. Btw. the data collectors must also be able to handle the various types of event data formats.

3. Event correlation

The large number of gathered security events must be brought into the right context. Security information from external institutes and companies, mostly provided via Threat Intelligence (TI) data bases, should additionally be used to enrich these data sets. A Security Information and Event Management (SIEM) system can correlate all these events and information on basis of correlation rules to determine regular system activities and actual security threats. The SOC operators' expertise about the monitored IoT systems and their applications is the key to define reasonable correlation rules for normal and abnormal system and application behavior.

4. Visualization

Visualization can be done combined with IT and OT security monitoring. But the extremely large number of IoT devices and the resulting security alarms might overflow the graphical views. Therefore, implementation of Automated Incident Response becomes of increasing importance. It will be the only way out of the dilemma to enable effective security monitoring of the massively growing IoT under control.

Security Analytics and Threat Handling

During the last years, business analytic methodologies are coming more and more also into focus of security technologies. Extreme large amount of information collected in Data Lakes from log files as well as data streams can be fed now into decisions about normal and abnormal behavior of users, systems and environments. Simple pattern matching with known normal behavior as well as complex self-learning mathematical algorithms can be used to constantly improve the level of threat detection. These allow more precise automated security incident response and support SOC teams during their daily forensic tasks.

Compliance

Although there is no globally adopted IoT security framework, we see several initiatives from specific providers or consortiums to establish a Common Criteria for secure IoT implementations.

Good examples are the Platform Security Architecture (PSA[14]) from Arm, the IoT Security Foundation (IoTSF[15]) best practice guides, NIST publications[16], among others... There is no unique approach to compliance either, but there are a series of legislative requirements and standards that provide guidance both to regulators and users. Below we expose some IoT Security frameworks and compliance standards worth to review closely.

Requirements by International standards providing certification

ISO/IEC (ISO = International Organization for Standardization / IEC = International Electrotechnical Commission)

1. ISO/IEC 27001:2013 (Information technology. Security techniques. Information security management systems. Requirements)

This International Standard has been prepared by ISO/IEC JTC 1/SC 27 to provide requirements to establish, implement, maintain and continually improve an info-security management system.

This International Standard can be used by internal and external parties to assess the organization's ability to meet the organization's own information security requirements.

ISO/IEC 27001:2013 is structured in 7 domains and in Appendix A provides 114 security controls in 14 groups and 35 control objectives.

2. ISAE 3402

ISAE 3402 (International Standard for Assurance Engagements) is an assurance standard managed by the Governance Institute in Utrecht, Netherland. Its title is "Assurance Reports on Controls at a Service Organization." Apart from ISO27001, **ISAE 3402 is an audit standard to report on outsourced activities.**

This standard allows far more freedom on its application, as it only provides guidelines and a general testing framework. ISO 27001 has more specific requirements. Still, achieving compliance to ISAE 3402 can be more expensive than to ISO 27001.

3. NIST 8200

NIST 8200 (National Institute of Standards and Technology) Draft Interagency Report on Status of International Cybersecurity Standardization for the Internet of Things (IoT) was recently released by The Interagency International Cybersecurity Standardization Working Group (IICS WG).

This report defines overall IoT functions and applications, and then provides an end-to-end cybersecurity overview for it (cybersecurity objectives, risks, threats and available standards), mapping existing solutions and standards to cybersecurity core areas. It provides guidance for secure development and use of cybersecurity standards in IoT components, systems or services, both for government and commercial bodies.

4. GDPR.

The EU General Data Protection Regulation 2016/679 (GDPR) took effect on 25 May 2018. While it does not refer directly to IoT technologies, it definitely has a role to play in it. Deterrent effect of drastically high fines implies vivid compliance activity (and business) at the 2017/2018. Situation is complicated by the fact, that EC has not provided a clear explanation of GDPR 99 articles and 173 recitals.

In the terms of GDPR, Data Protection Impact Assessment (DPIA) can be required for "high risk" personal data processing, under which most probably fall all the personal data controllers resp. processors providing the services on the base of IoT. However, there are still not clearly defined neither exact conditions for mentioned "high risk," nor the form of DPIA.

[14] Platform Security Architecture (PSA) from Arm - https://www.arm.com/news/2017/10/a-common-industry-framework
[15] IoT Security Foundation (IoTSF) - https://www.iotsecurityfoundation.org/
[16] National Institute of Standards and Technology (NIST) - https://www.nist.gov/topics/internet-things-iot

Frameworks by open licence publications respectively "open source"

1. AIOTI

The Alliance for Internet of Things Innovation (AIOTI) was initiated by the European Commission in 2015, with the aim to strengthen the dialogue and interaction among IoT players in Europe, and to contribute to the creation of a dynamic European IoT ecosystem to speed up the take up of IoT. Its "Policy Issues" working group (WG04) Report deals with privacy, security and liability.

2. IoT Security Compliance Framework

IoT Security Foundation (IoTSF) is a methodical publication licenced under "Creative Commons Licence v.4". It can be briefly introduced as follows:

"... IoTSF advocates the core security values of: security first / fitness of purpose / resilience. The Framework is therefore intended to help all companies make high-quality, informed security choices by guiding users through a comprehensive checklist and evidence gathering process. ...

More broadly, organisations that follow this process are demonstrating a duty of care towards their customers and other stakeholders in the IoT ecosystem. ..."

Vision regarding IoT Cybersecurity Compliance

In order to effectively manage IoT cybersecurity compliance, the processes of compliance shall focus on the following domains[17]:

1. **Business processes**
2. **Devices and aggregation points** such as related gateways/hubs that provide generic part of the connectivity for IoT devices
3. **Networking** including wired (whether LAN or power supply), and radio connections using short-range, LPWAN and cellular
4. **Cloud and server** elements as specific to IoT

Regarding IoT cybersecurity compliance, these basic principles can be considered[18]:

- Everything is connected to everything
- Basic cybersecurity controls still hold as true
- Users are (and always shall be) the biggest security risk
- Utilise existing frameworks/guidelines
- Be aware of credential theft techniques

For the certified systems adherent to ISAE 3402, there should be a portfolio of emerging recommendations for IoT forthcoming.

For open frameworks, there should be observation of the situation relating to the activities and publications of non-profit organisation on global resp. EU level (e.g. IoT Security Foundation or AIOTI). Regarding to the implementation resp. management of IoT Cybersecurity Compliance processes for ISO/IEC certified Information systems with IoT components, can be continued existing methods based on standards 27001 resp. 9001, 20000. "Portfolio" of ISO/IEC standards within Subcommittee JTC 1/SC 41 "Internet of Things and related technologies" shall gradually evolve to more usable stage, therefore we shall expect imminent developments to be published in the ISO website[19].

[17] IoT Security Compliance Framework, IoTSF, 2017
[18] Dr.Benetits,V, Cullen, M., Hollis, R., ISACA, 2016: Suggested tips auditors need to know about cyber security
[19] Namely published, as "ISO/IEC TR 22417:2017 ... Internet of things (IoT) use cases" and under development like awaited "ISO/IEC CD 20924 ... Internet of Things (IoT) -- Definition and vocabulary"

Conclusions

As we have discussed, IoT has rapidly transitioned from futuristic concept to an integral part of modern society, with billions of units connected today, and tens of billions predicted in a not too distant future.

As with any new technology, IoT comes with its' own unique set of security challenges. And given the growing volume of interconnected IoT devices, and the amount and type of data they generate, those challenges are significant. We are all aware of the lack of skilled cybersecurity resources within the IT industry, this is felt more keenly within the IIoT industry and could jeopardize the transition of IoT into a security by design mode of operation.

As companies continue to adopt IoT solutions, security is foremost on their mind. To this end, there are several steps that can be taken to ensure your IoT infrastructure is secure.

1. Secure the device

While many IoT devices may lack the processing power to run standard security tools, steps should still be taken to ensure the endpoint device is hardened whenever possible.

2. Manage your IoT devices

Just because they are not traditional computing endpoints does not mean your IoT devices shouldn't be treated as part of your standard management strategies. Patch management, antivirus, asset management, vulnerability management and other standard IT management strategies for IT devices are also a requirement for your IoT devices.

3. Secure the gateway

IoT infrastructure frequently relies on gateway devices to interconnect with other networks. Ensuring the security of these gateways is key to a successful implementation.

4. Secure the data

IoT devices generate enormous amounts of data. It's critical that this data is secured appropriately, especially if it contains private data.

5. Be compliant

When rolling out IoT devices, ensure you are in compliance with existing regulatory requirements. Regulations such as GDPR in Europe place stringent requirements on compliance, including your IoT devices.

6. Leverage frameworks

There are a number of existing security frameworks that can be leveraged when designing an IoT security framework. It is important to select the most appropriate framework to the purpose of the IoT project.

7. Take advantage of encryption

Whenever possible, encrypt your IoT data while at rest and in transit.

8. Ensure the integrity and availability

Ensure the integrity and availability of data created by (and sometimes stored within) IoT devices.

9. Select the right partner

When identifying an IT partner, be sure to select a partner with the vision, strategy and expertise to ensure your IoT deployment is a success.

Atos provides a variety of IoT solutions with a data-centric focus to ensure the successful deployment and security of your IoT infrastructure: from a comprehensive Atos Horus IoT Security Suite to our end to end IoT Security and Service Management under the Atos Codex IoT label. You can benefit from an expertise built on the vision and early adoption of IoT solutions in support of demanding global organizations.

Atos is your trusted partner for the full breadth of IoT solutions and services.

About the authors

The authors would like to thank the Atos Experts Community and the following experts for their reviews and valuable comments to early versions of this white paper: Jordi Cuartero, Celestino Guemes, David Leporini, Koen Maris, Purshottam Purswani and Zeina Zakhour.

This paper has been prepared by the Atos Experts Community Cybersecurity Domain with contributions from:

Dave Bixler
Risk Management
and IT Control Framework

Konstantinos Brokalakis
Product Security Officer

Peter Bukovinsky
Auditor

Parag Ghosalkar
Cloud Operational Security Officer

Ruediger Hoischen
Global Cybersecurity
Product Manager

Marc Llanes Badia
Global Cybersecurity Architect
Member of the Atos Scientific Community
@atosllanes

Lyonel Vincent
Global Cybersecurity Architect

Colin Young
Global Cybersecurity Architect,
Certified Ethical Hacker

About Atos

Atos SE (Societas Europaea) is a leader in digital transformation with circa 100,000 employees in 73 countries and pro forma annual revenue of circa € 12 billion. Serving a global client base, the Group is the European leader in Big Data, Cybersecurity, Digital Workplace and provides Cloud services, Infrastructure & Data Management, Business & Platform solutions, as well as transactional services through Worldline, the European leader in the payment industry. With its cutting edge technologies, digital expertise and industry knowledge, the Group supports the digital transformation of its clients across different business sectors: Defense, Financial Services, Health, Manufacturing, Media, Utilities, Public sector, Retail, Telecommunications, and Transportation. The Group is the Worldwide Information Technology Partner for the Olympic & Paralympic Games and is listed on the Euronext Paris market. Atos operates under the brands Atos, Atos Consulting, Atos Worldgrid, Bull, Canopy, Unify and Worldline.

Find out more about us
atos.net

Let's start a discussion together

For more information:**atos.net/contact-us**

CT_181010_LPM_Wp_IoTCybersecurity_vision_2018-2019_en1