ERICSSON WHITE PAPER
284 23-3302 Uen | February 2017

ERICSSON

# IOT SECURITY

## PROTECTING THE NETWORKED SOCIETY

The Internet of Things (IoT) is expanding rapidly, and is expected to comprise 18 billion connected devices by 2020. But the assumptions of trust which formed the backdrop to the early development of the internet no longer apply in the early stages of IoT development. Privacy and security concerns are ever increasing, especially given the growing significance of IoT in corporate, government, and critical infrastructure contexts. Likewise, the commodification of IoT components incorporated across diverse product ranges and deployed in both managed and unmanaged use cases brings significant security challenges and creates potential for novel types of attack. The proactive cooperation of all key stakeholders will be necessary to realize the considerable economic benefits of the IoT, while protecting security, safety, and privacy.

# INTRODUCTION

The Internet of Things (IoT) is rapidly emerging as the manifestation of the Networked Society vision: where everything that benefits from a connection is connected. Yet this far-reaching transformation is only just beginning, and the number of connected IoT devices is expected to grow by 21 percent annually, rising to 18 billion between 2016 and 2022 [1]. The IoT consists of multiple ecosystems, each with different requirements and capabilities. At one end of the spectrum, there are constrained sensors made of printed electronics; at the other end, autonomous vehicles such as trucks, trains, and aircraft. In addition, usage scenarios range from temperature monitoring to mission-critical industrial control systems.

The internet began in an environment of mutual trust, where everyone could read, change, or inject information. But the IoT is taking off in a hostile environment, where the expectations of the general public and governments regarding security and privacy are very high, and information security is a top concern among enterprises adopting IoT [2]. The IoT therefore needs to be secure from the start, protecting personal information, company secrets, and critical infrastructure. Regulators need to walk a fine line between protecting privacy, safeguarding national security, stimulating economic growth, and benefiting society as a whole [3].

The IoT brings a new set of issues, such as the security, safety, and robustness of cyber-physical systems. Novel types of attack, as well as new privacy and cybersecurity regulations, may take many industries by surprise. Yet the economic benefits of the IoT as an enabler for analytics, automation, and process and resource optimization cannot be overstated. To succeed with the transformation that the IoT brings about, industries need to gather competence and understand new threats and how to mitigate them.

This white paper provides an insight into the major security and privacy challenges due to be met in the Networked Society. Specifically, it addresses security, safety, and privacy in the entire IoT value chain, which includes devices, networks, cloud, infrastructure, applications, and services. The paper also identifies the main security challenges and approaches that need to be taken in the IoT sphere to withstand attacks, and discusses how IoT security and privacy need to be addressed through technology, standardization, and regulation.

# CHALLENGES

## CYBERSECURITY FOR BILLIONS OF DEVICES

For the IT department, the IoT will create a need to manage large numbers of different types of devices, many of which may not be able to ask a user for login credentials or run traditional security software. For hackers, the sheer quantity and diversity of these devices will increase the potential attack surface. Gartner estimates that by 2020, more than 25 percent of all enterprise attackers will make use of the IoT [4]. The challenge of preventing attacks will be compounded by IoT deployments in settings where there is an absence of technical expertise, such as homes and small enterprises.

From an operational technology perspective, the Industrial IoT (IIoT) makes industrial control systems more autonomous and connected [5]. Cyber-physical systems affect the physical world and, when compromised, significant material damage may be caused, safety may be jeopardized, and the environment may be harmed. Hence a successful attack on an IIoT system has the potential to be as serious as the worst industrial accidents to date [6].

Hacking attacks are increasingly carried out by professionals with extensive resources and a high level of technical knowledge, and since the IoT affects people's daily lives and industrial operations, there will be plenty of incentives to hack IoT systems. Many current IoT devices are extremely easy to hack, and the IoT has quickly become a popular enabler for massive Distributed Denial of Service (DDoS) attacks [7]. Mitigating DDoS is problematic as neither the owners nor the sellers of the devices bear the costs of the attacks, and IoT-based DDoS has the potential to become a major problem for society. Therefore, critical infrastructure must not only be able to withstand direct hacking, it must also be resilient to attacks such as DDoS and jamming.

## PRIVACY AND INFORMATION SECURITY IN THE IOT

Privacy is understood and regulated in different ways across countries and jurisdictions. The media attention on privacy has raised public awareness, and a global customer survey [8] shows that privacy is the main IoT concern (see Figure 1). Even seemingly harmless data relating to electricity consumption or room temperature, for example, may reveal too much about a person's habits. But with billions of sensors everywhere, the IoT will drastically increase the amount of potentially sensitive information being generated concerning people's movements, activities, and health. Compounding the problem, in most cases, people will not be aware of the sensors around them, or how the combined data from various sources can be misused.

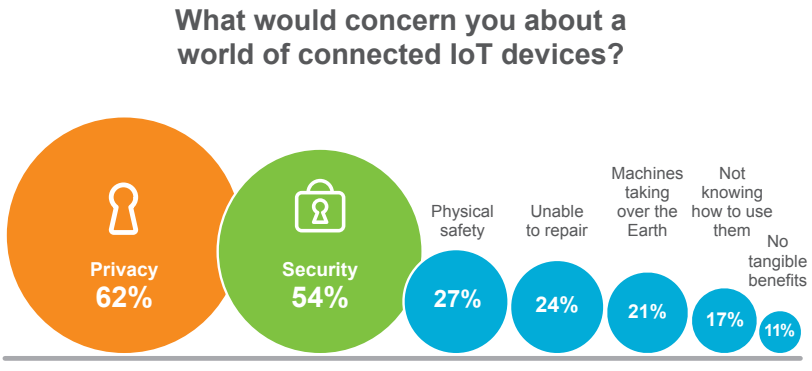



*Figure 1: Overview of an interoperable ecosystem*

The wealth of information in clouds and devices – sometimes in exposed locations – increases the risks of industrial espionage and the surveillance and tracking of people. In the IoT, individual pieces of information may not reveal much, but the magnitude of data could make it possible to determine company processes through the use of analytics. Even if traffic is encrypted, meaningful patterns may be revealed through the analysis of that traffic.

## DEVICE SECURITY AND SOFTWARE UPDATE

Today's users expect security and privacy even of the smallest devices. However, a high level of tamper resistance may conflict with a desire to keep device costs down. Limited processors, small amounts of memory, and low throughput radio make some existing security protocols less than optimal for many devices. Any device running on batteries has yet another limitation as every micro ampere-hour needs to be rationed to prolong the device's lifetime.

Many IoT devices will have a long lifetime and, as manual configuration is expensive, over-the-air firmware and software updates become crucial. However, ensuring robust and non-fatal updates when there is not enough memory to save both the old and new firmware is still a challenge. Another challenge is how to enforce remote firmware updates when the operating system and applications are infected by viruses attempting to block these updates.

## TRUST IN INTERMEDIARIES – A NECESSARY THREAT?

IoT systems rely on intermediaries to reduce response time, bandwidth, and energy consumption. Since radio reception and transmission draw relatively high levels of power, many IoT devices sleep almost all of the time and, therefore, need to rely on proxies to cache requests and responses. Gateways are needed to bridge different radio technologies or offload processing. Furthermore, in mesh networks, every node is an intermediary.

While proxies and gateways are necessary in many IoT deployments, they open pathways for attacks. Even when security protocols like IPsec and TLS are used, there is commonly a breach in security when an intermediary is able to read, change, or inject information without being detected. A trust model involving a multitude of trusted intermediaries breaks down as soon as the security of one of these intermediaries is compromised. Application layer security is needed to address such challenges. Another challenge related to this situation is working out how to maintain trust in data that is processed on its way from sensor to consumer.

## THE IMPLICATIONS OF REGULATION

As the IoT affects a range of diverse sectors such as agriculture, transportation, utilities, and healthcare, many IoT systems are governed by various regulatory frameworks in each country. And in some cases, such as autonomous vehicles, completely new regulations are required. The regulatory focus on security and privacy has intensified in recent years. The US Government, for example, has enforced secure management of radio parameters and fined companies for using default passwords, and the EU has reformed its regulations on the protection of personal data [9]. Several countries have published directives on cybersecurity and protection of critical infrastructure [10]; some have even pushed for substitution of foreign technology suppliers with domestic ones. So far, regulators have taken a heavy-handed approach to privacy, but a light-handed approach to the IoT and cyber-security. But since society will depend more on the trustworthy functioning of the IoT, regulators will most likely increase its regulation.

## DEFENDING CYBER-PHYSICAL SYSTEMS

In autonomous cyber-physical systems, integrity and availability become more important than confidentiality. Losing control of locks, vehicles, or medical equipment is far worse than having someone eavesdrop on them. Therefore, properties like message freshness, proximity, and channel binding also become essential, sometimes in unexpected ways. As a current example, consider the proximity-based security systems used in smart car keys, access cards, and contactless payment systems. While those systems all verify freshness, they do not verify proximity, so two attackers can relatively easily relay the signal from a device in a victim's pocket, gaining access to office buildings, opening and starting cars, or transferring money (see Figure 2). Unless the security, safety, and privacy properties of IoT systems are carefully evaluated, suppliers may get some embarrassing and costly surprises.

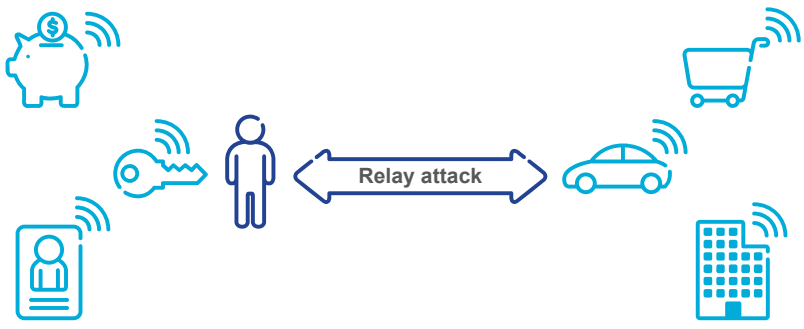



*Figure 2: Relay attacks on proximity-based security*

# APPROACHES TO SECURING IOT

While most activity today takes place in the devices and connectivity phases, most future revenue is expected to come from platforms, applications, and services. In the following sections we discuss the various approaches to security during the different phases in the IoT value chain (Figure 3).

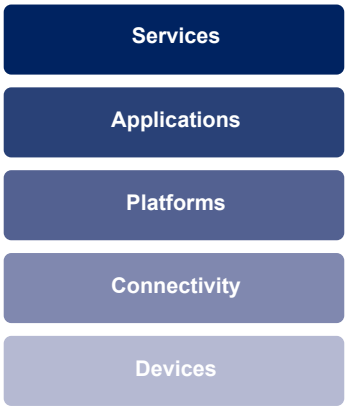



*Figure 3: The IoT value chain*

## DEVICES – HARDWARE ROOTS OF TRUST

As many IoT devices are placed in exposed environments, these devices should have the means to automatically protect their functioning and the data they contain. In particular, sensitive data in non-secure storage needs to be encrypted and integrity protected to obtain a secure storage function. Devices must cryptographically verify firmware and software packages at boot or update, and should maintain the ability to receive remote firmware updates even in case of malware infection. Devices should have enough storage to carry out automatic rollback in the event of an update failure, but malicious rollback to older versions of the firmware or software with critical vulnerabilities must be prevented.

These security features must be kept isolated from the applications on the devices. Hardware-based isolation can be used for these security features and is needed to protect applications from other applications and potentially compromised operating systems (see Figure 4). This type of functionality constitutes a root of trust – traditionally provided by dedicated hardware, but now achievable with trusted execution environments (TEEs) isolated from the rich execution environment (REE) in common processors, including low-cost embedded processors. For deployments where cost is important, the use of TEE is preferred. Strong device security is necessary to protect sensitive data and prevent IoT devices from being used as stepping stones for attacks.

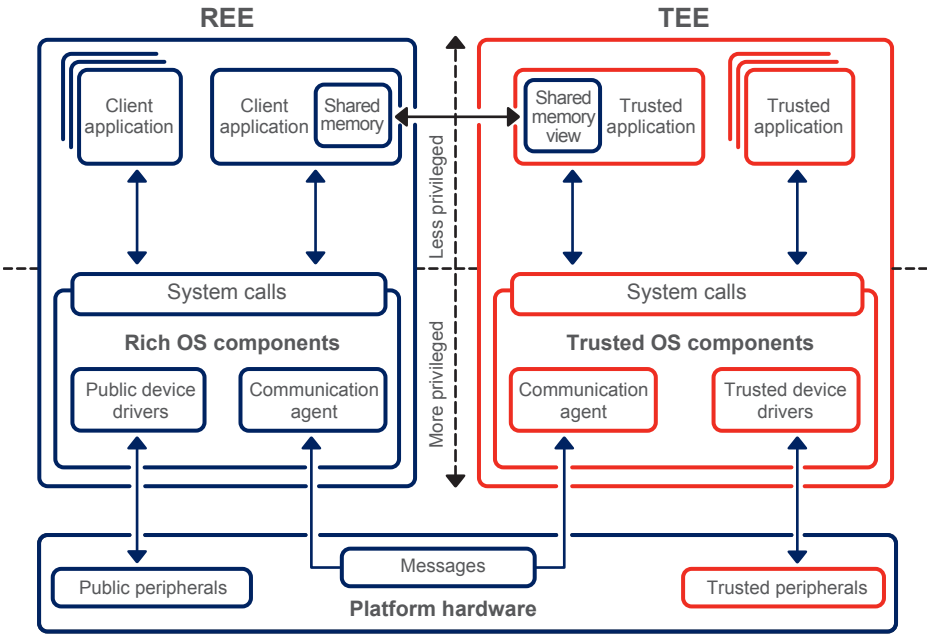



*Figure 4: Hardware isolation using TEE*

Modern cryptographic algorithms are significantly faster than legacy algorithms; even asymmetric cryptography runs well on everything except processors in the most constrained ultra-low cost segment. Furthermore, the energy cost of symmetric cryptography is negligible compared with that of wireless communication. Lightweight cryptography is needed for some environments, but not for the IoT in general. A future challenge is that the current asymmetric algorithms need to be replaced with post quantum resistant variants, where keys and signatures are expected to be much larger. For IoT devices in exposed environments, protection against side-channel attacks is essential to prevent leakage of keying material through timing information, power consumption, electromagnetic waves, or sound.

## CONNECTING BILLIONS OF DEVICES – WHO'S WHO?

The purpose of connectivity is to facilitate the secure interaction of applications on the device and in the serving network nodes. This requires two crucial functions: identification based on credentials and secure data transport. IoT connectivity must be able to cost-efficiently handle billions of devices (see Figure 5), and will be realized through heterogeneous access technologies. Many devices will be deployed in capillary networks and connected to cellular networks via gateways. Enablers in the cellular network can then provide device management, secure bootstrapping, or assertions such as verifying device location or trustworthiness of platforms. Mobile operators should leverage their unique position as both connectivity and platform providers. Evolved 3GPP technologies such as LTE-M, NB-IoT and EC-GSM-IoT are superior solutions designed to meet IoT requirements [11]. They provide global connectivity and offer unrivaled robustness compared with unlicensed spectrum. The use of encryption on the radio interface makes traffic analysis significantly harder.

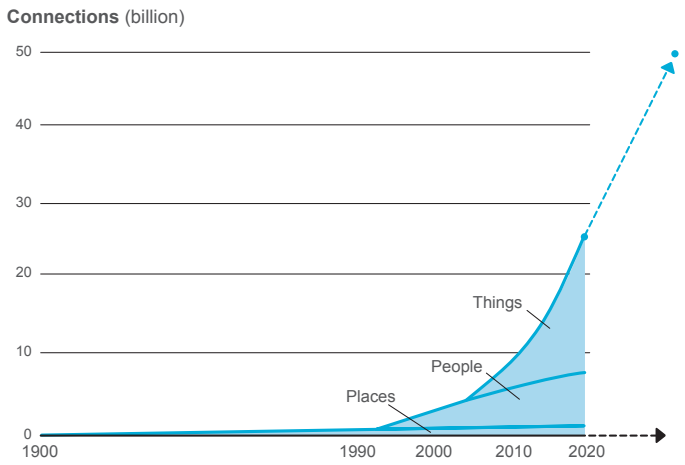



*Figure 5: Connecting places, people, and things*

Based on pre-provisioned device credentials, access technologies need to provide automatic and secure remote provisioning of connectivity credentials. 3GPP credentials have traditionally been provisioned on physical UICC cards, requiring dedicated readers and local manual provisioning. An embedded UICC (eUICC) enables remote provisioning and management of credentials. By generating credentials on the device, the risk of breaches is reduced [12]. The next logical and necessary step is to use the trusted execution environment that is already integrated in the baseband or application processor. This evolution offers reduced hardware cost and power consumption, improved speed, and flexibility to use new types of credentials.

The IoT, including interworking with existing identities and credentials in various industries, is one of the main 5G focus areas [13]. Industry customers want a single service layer agreement with a single connectivity aggregator providing reasonable and predictable fees. For some use cases, it might be a security benefit only to allow connection from a single base station or access point, while other use cases such as transportation require global roaming. As the IoT consists of so many different ecosystems, flexibility is a must. There must be a possibility to bootstrap connectivity credentials from device credentials, or application credentials from connectivity credentials.

## PROTECTING THE PLATFORM – A CASTLE IN THE CLOUDS

IoT platforms need to ensure the security of data and control commands, and provide strong isolation between different devices and users, as well as between third-party applications and platform services. According to Gartner, security and privacy concerns continue to be the main inhibitors to cloud adoption. IoT platforms need to provide flexible key management, allowing customers to decide on the tradeoff between information security and ease of use, from managing their own keys to letting the platform provider generate and store the keys. Additionally, one of the main goals of an IoT platform is to minimize manual handling. Management functions should, for example, be able to restore devices with malware infections without the physical presence of a service technician.

IoT platforms should supervise devices' lifecycles from manufacture to decommission:

- During manufacturing, each device should have credentials (keys and identifiers) stored in a secure hardware module, application processor, or baseband processor.
- In the installation phase, the device uses the pre-configured credentials to automatically bootstrap itself to services. The IoT platform should perform initial configuration, including update of firmware, configuration of applications, and provisioning of credentials for application layer services.
- During operation, the platform should monitor the device, provide software updates, and enforce security policies such as authorization and access control. To save bandwidth and storage, firmware and software updates should be delta encoded.
- Before the device is taken out of service, the IoT platform should remotely erase all the sensitive data on it. Remote decommissioning is almost as important as remote provisioning, and should be a requirement for IoT devices.

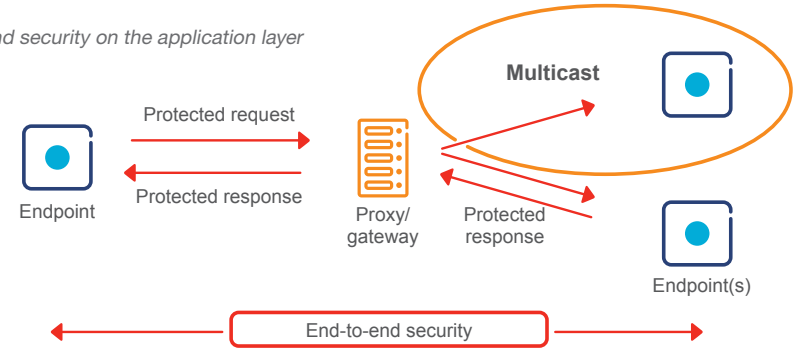
## APPLICATIONS AND END-TO-END SECURITY

Applications can be seen as a combination of micro services that are used to create a service. These applications can be statically located or dynamically migrated to the environment that is optimal for their realization. The security of the applications will be the result of the application code itself and the platform it is using. In cases where applications can migrate, it is important that migration between platforms happens securely [14]. In cloud systems, applications can be securely placed on trustworthy platforms by using attested information that comes from roots of trust in the cloud infrastructure.

After devices or applications have used identities to establish contact, the exchange of data is secured by different kinds of security protocols. The Internet Engineering Task Force (IETF) has driven the standardization of several new lightweight profiles of existing security protocols. One example is an authorization framework based on OAuth suitable for resource access in constrained environments [15]. By reusing existing solutions where possible, innovation is accelerated and integration with existing systems is made easier.

To protect information in the presence of intermediaries, traditional security protocols such as IPsec and TLS are not sufficient, as they support only trust models with fully trusted endpoints. As a rule of thumb, authorization to access information should be given on a need-to-know and need-to-change basis. To accomplish this goal, end-to-end security is needed at the application layer (see Figure 6). Object security (the use of information containers providing confidentiality, integrity, and origin authentication) is the preferred solution to protect message exchanges, since it enables end-to-end security independently of intermediaries and lower layers in the protocol stack.

*Figure 6: End-to-end security on the application layer*



## SERVICES – SECURING NEW BUSINESS OPPORTUNITIES

The IoT will transform most existing industries and enable a multitude of new business opportunities. Some of the most interesting potential IoT applications are in the transport industry, where the transformation to connected vehicles occurs at the same time as the transformation towards electrical and autonomous vehicles. In the future, connected vehicles may work like schools of fish or flocks of birds, using artificial intelligence to take over safely when the connection to the network and other vehicles is lost – either owing to malfunction or as a result of attacks, such as jamming.

A look at the internal workings of a modern connected vehicle reveals a complex system with thousands of sensors and actuators, and a large code base across a set of embedded processors. Hardware and logical isolation are essential, so that, for example, a breach in the infotainment system cannot be escalated into a breach in the steering system. Firmware updates must be carried out so that compatibility between different subsystems (such as the brake pedal and the brakes) is sustained. The simplest solution is to update all subsystems at once, and roll back if some of the updates fail. Transportation is currently one of the riskiest activities in everyday life, and vehicle-to-vehicle communication has the potential to prevent almost all automobile accidents. Hence, while accidents caused by malfunctioning machines seem inevitable, fear should not be allowed to curb development.

The IoT will also increase public safety in other areas of society. By integrating sensors and cameras into traffic lights, vehicles will be aware of people crossing roads and tracks far in advance. The IoT enables huge possibilities to increase the safety of emergency response agencies and the society they are sworn to protect. Emergency vehicles will automatically get free lanes, missing children will be easier to find, and both citizens and blue light personnel will be possible to track during emergencies such as fires. The critical nature of these functions means that strict authorization and transparency are needed to hinder misuse or suspicion of such misuse. While some aspects of surveillance may be a necessary component of public safety, the right to be forgotten should also be considered.

## SECURITY, SAFETY, AND PRIVACY BY DESIGN

A legitimate expectation of society is that IoT technologies and services will be designed with security and privacy in mind. To meet this expectation, a common effort is required, including industry, regulators, and standardization organizations. Privacy controls should allow flexible management of identities and private data across IoT devices, networks, and services. To provide security and privacy at a low cost, the IoT needs standardization in several steps: first, common enablers, such as IETF and 3GPP, that work in a multitude of different verticals, and second, specific standardization for each vertical, such as the Industrial Internet Consortium.

The IoT must be allowed to flourish without being hampered by restrictive or inflexible regulations. Premature regulation may miss the target and move investments to other regions of the world. Regulators should adopt a market-driven approach that encourages growth. Policy makers should focus their efforts on developing appropriate policy tools to identify, respond, and ultimately prevent cyber-threats to IoT systems related to utilities and critical infrastructure, including autonomous systems such as transportation and manufacturing. This includes actions so that IoT devices have enough security not to be enablers for massive DDoS attacks.

Due to the complexity of IoT systems, new types of threats, and increasing regulation, there is a growing need for professional security services, including end system and application security verification and more commonly an industry-driven methodology to have a solid approach to assuring security for IoT-based services and platforms.

# CONCLUSION

The widespread use of IoT creates new challenges, and its unprecedented interaction with the physical world impacts the safety and privacy of individuals. The right to privacy needs to be protected on the device, during communications, and in the cloud. As a rule of thumb, information should be transferred and accessed on a need-to-know and need-to-change basis, and events such as data creation, data access, and control commands should be logged in a verifiable way.

The deployment of IoT systems is a challenge considering that the devices often have no user interface and are deployed in large quantities, and the associated business models do not afford manual per-device configuration. To enable secure and automated bootstrapping, each device should have device credentials pre-provisioned during manufacturing. The use of trusted execution environments has substantial cost benefits and facilitates the use of 3GPP technologies in various industries. Authorization and protection of data in transfer are best carried out using over-the-top security on the application layer.

To enable rapid deployment of the IoT and realize its vast potential, the costs need to be low and, therefore, the technical differences between various geographical regions and industries must be small.

In general, IoT security and privacy are high on the agenda for the general public, media, enterprises, governments, and ICT companies. Security is a major concern among enterprises adopting IoT and cloud solutions, with Gartner expecting IoT security spending to grow by almost 60 percent in the next two years, reaching around USD 547 million. The opportunity cost of not doing enough about IoT security, safety, and privacy is very significant, due to the potential harm caused to people and property, public distrust, administrative sanctions, and even threats to national interest. For societies and economies to realize the positive benefits of the IoT, all key stakeholders need to proactively consider security, safety, and privacy throughout the entire IoT supply chain. To succeed, a mix of vendor responsibility, regulation, and certification is needed.

# GLOSSARY

| | |
|---|---|
| **3GPP** | 3rd Generation Partnership Project |
| **5G** | 5th generation mobile wireless standards |
| **DDoS** | Distributed Denial of Service |
| **EC-GSM-IoT** | extended coverage GSM IoT |
| **eUICC** | embedded Universal Integrated Circuit Card |
| **IETF** | Internet Engineering Task Force |
| **IIC** | Industrial Internet Consortium |
| **IIoT** | Industrial Internet of Things |
| **IoT** | Internet of Things |
| **IPsec** | Internet Protocol Security |
| **LTE-M** | simplified term for LTE-MTC LPWA (Long Term Evolution Machine Type Communication Low Power Wide Area) |
| **NB-IoT** | Narrowband IoT |
| **TEE** | trusted execution environment |
| **TLS** | Transport Layer Security |
| **UICC** | Universal Integrated Circuit Card |

# REFERENCES


[1] Ericsson, Ericsson Mobility Report, November 2016, available at:
https://www.ericsson.com/mobility-report

[2] Gartner, Forecast: IoT Security, Worldwide, 2016, available at:
https://www.gartner.com/doc/3277832/forecast-iot-security-worldwide-

[3] Edelman, Technology and Trust, available at:
http://www.edelman.com/p/6-a-m/technology-and-trust

[4] Gartner, Securing the Internet of Things, available at:
https://www.gartner.com/doc/3316617/securing-internet-things

[5] Fireeye iSIGHT Intelligence, Overload: Critical lessons from 15 years of ICS vulnerabilities, available at:
http://www2.fireeye.com/rs/848-DID-242/images/ics-vulnerability-trend-report-final.pdf

[6] Industrial Internet Consortium, Industrial Internet of Things, Volume G4: Security Framework, September 2016, available at: https://www.iiconsortium.org/pdf/IIC_PUB_G4_V1.00_PB.pdf

[7] The New York Times, Hackers Used New Weapons to Disrupt Major Websites Across U.S., available at: http://www.nytimes.com/2016/10/22/business/internet-problems-attack.html

[8] Mobile Ecosystem Forum, The Impact of Trust on IoT, available at:
http://mobileecosystemforum.com/initiatives/analytics/iot-report-2016

[9] European Commission, Protection of personal data, available at:
http://ec.europa.eu/justice/data-protection/

[10] European Commission, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, available at:
https://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf

[11] Ericsson, Cellular Networks for Massive IoT, January 2016, available at:
https://www.ericsson.com/res/docs/whitepapers/wp_iot.pdf

[12] GSMA, IoT Security Guidelines, available at:
http://www.gsma.com/connectedliving/future-iot-networks/iot-security-guidelines/

[13] Ericsson, 5G Security – Scenarios and Solutions, June 2015, available at:
https://www.ericsson.com/res/docs/whitepapers/wp-5g-security.pdf

[14] Persson et. al., Calvin – Merging Cloud and IoT, available at:
http://www.sciencedirect.com/science/article/pii/S1877050915008595

[15] IETF, Authentication and Authorization for Constrained Environments (ACE), available at
https://tools.ietf.org/html/draft-ietf-ace-oauth-authz