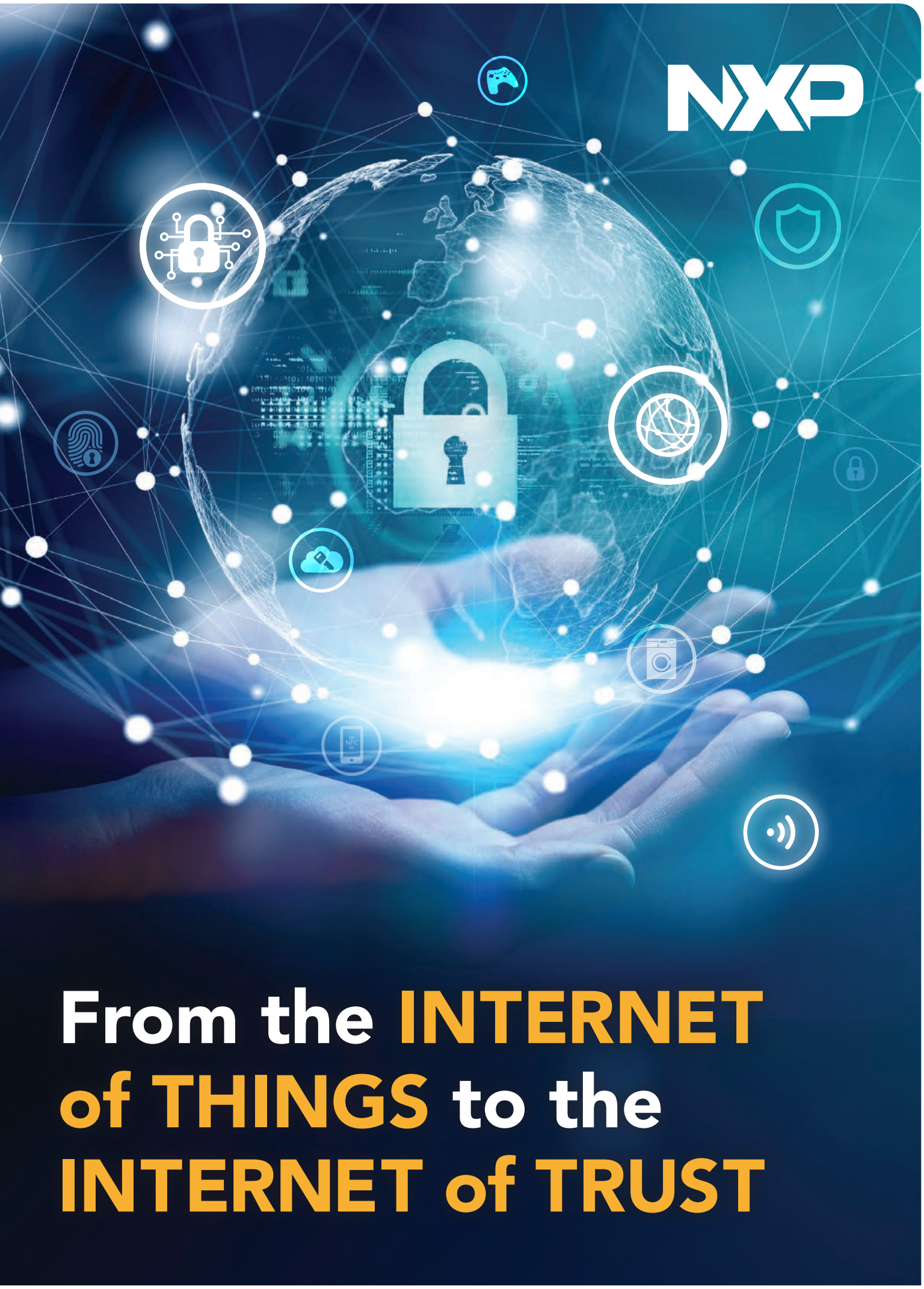

NXP
From the INTERNET of THINGS to the INTERNET of TRUST

CONTENTS

IT and – more recently – **IoT, the Internet of Things**, have invaded almost every part of our daily life. Our society is increasingly reliant on smart devices and services, from home automation to manufacturing, medicine, finance and transport. These billions of inter-connected devices with sensors and actuators, reachable almost instantaneously through the ubiquitous internet from any location and any other device in the world, are collectively called the Internet of Things (IoT). All too often, "reachable" means reachable by unauthorized entities as well as intended users. Consequently, as a society and global economy, we have become very exposed to a plethora of new **IoT security-related threats** that never existed before, some of which have the potential to impact profoundly on our way of life.

Vulnerabilities to IoT devices are announced at a rapid rate, such as the Meltdown and Spectre[1] vulnerabilities of CPUs, the ROCA[2] attack, or Heartbleed[3] for OpenSSL. The revelation of those threats have deeply impacted the industry. Some companies have lost stock market value and struggled for months, to deliver a solution to their customers and try to recover the damage caused to their brand image. Many of these incidents highlight that we are increasingly reliant on a few, dominant system building blocks, which have not been thoroughly security vetted.

At the same time, there are growing concerns that some countries or organized groups may use their advanced expertise of IT technology to influence elections and important decision making in other countries. Our reliance on IoT could be a most serious target for terrorists and foreign powers alike to gain even more influence and seriously hurt our society.

What needs to happen to counter the threat? First of all, IoT needs to be based on reliable, robust technology that cannot be tampered with easily. Not when it is being designed, nor during its operational lifetime, nor when it is decommissioned after use.

It is unrealistic to expect that tampering will be made impossible since it is always a question of the amount of money and effort that somebody is willing to spend. However, the risk and impact can be minimized by tailoring the security level of products and services according to the risks and threats identified for them. To do this, security technology must be vetted. Independent certification can deliver an independent judgement of how fit a product or service is from a security point of view, whether it lives up to all of its claims, and for how long it will continue to meet the required standards.

Therefore, products, systems and services need to be designed with security testing in mind. They need to be upgradeable so that patches can be applied after a security breach, which will inevitably happen at some point. Systems need to be designed in a resilient way to prevent the collapse of an entire system due to an attack. Furthermore, because security requirements vary considerably for different markets and applications, it is important to create scalable security in the architecture of products and services.

1. *https://meltdownattack.com/*
2. *https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-15361*
3. *https://cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2014-0160*

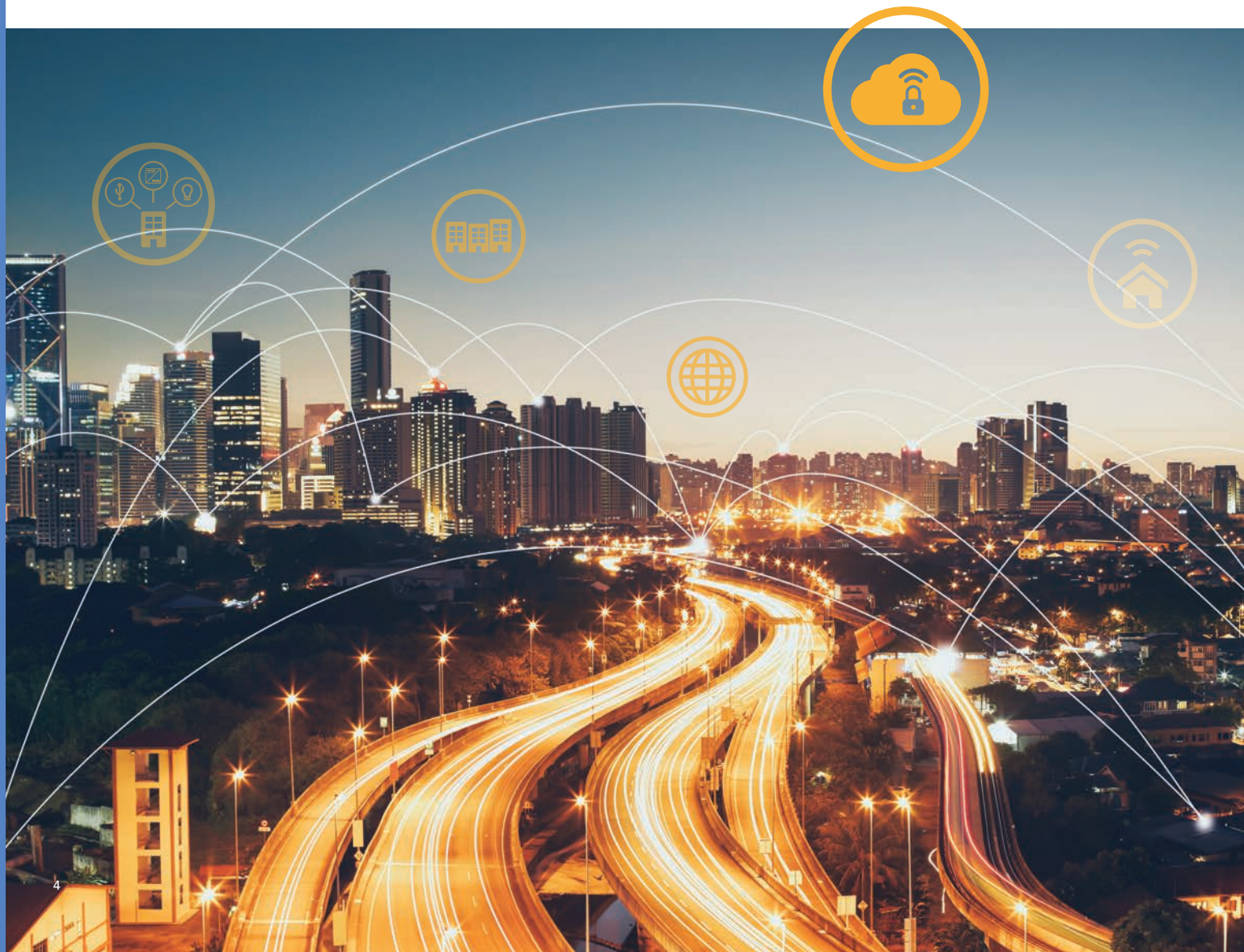
More effort in protecting end-users' privacy is needed, and in the long run, privacy will become a key consideration in the design of any product or service. Also, the legal landscape is changing and new privacy-preserving regulations that are aimed at the new technologies are developing.

NXP, a market leader in embedded security, has a successful track record of providing solutions to secure ecosystems such as secure microcontrollers, NFC, payment, access control and high-speed network switches, among others. This success stems from NXP's system approach, where NXP not only delivers secure products but also ensures that design for security and design for privacy solutions are provided to NXP's customers. NXP's security by design approach also encompasses design for secure manufacturing, secure trust provisioning and secure delivery. NXP has extended this expertise to products and solutions within the IoT ecosystem.

NXP is fostering security for IoT by actively contributing to new certification standards and offering a system and solution approach to its customers. Additionally, NXP is actively exploring new avenues to meet the various IoT security challenges, such as runtime protection, analytics, and recovery and damage control, while enriching the IoT security toolbox with innovative technologies, including whitebox cryptography, machine learning, homomorphic encryption and blockchain.

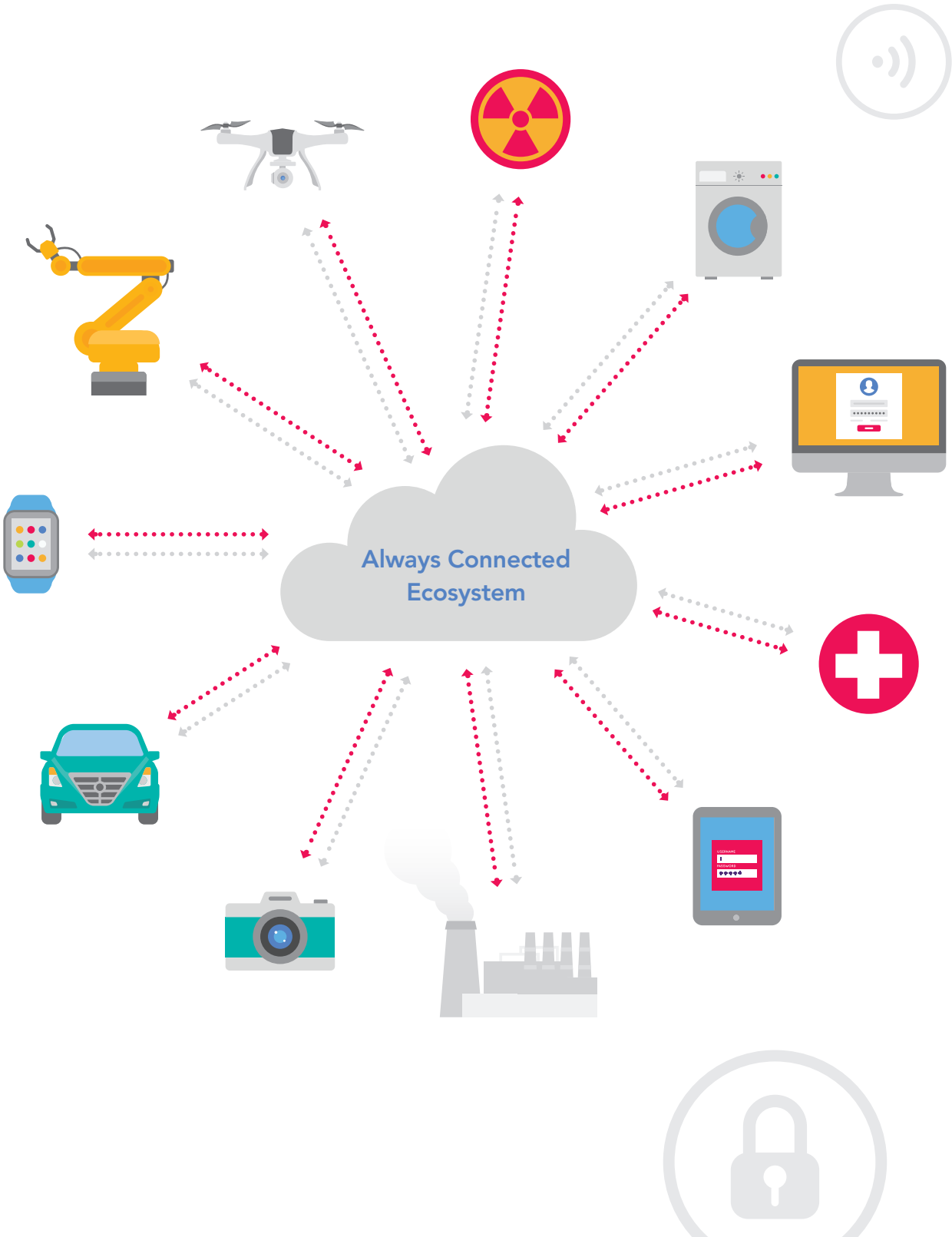
What is the challenge? What is the solution? What is the NXP engagement?

This Whitepaper will tell you more.



THE CHALLENGE

Billions of **connected IoT devices** are an attractive target for attackers. Before exploring some of the main IoT challenges and their potential security impact, the types of attacks that can be mounted against a system of interconnected devices are described.



TYPICAL ATTACKS

Attacks can be classified according to two major characteristics: **local vs. remote** and **logical vs. physical.**

IoT Security Threats and General Protection Principles

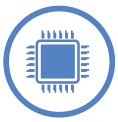
Threat Spectrum

	Physical	Logical
Local	Power Analysis, Light Attacks, Glitching	Exploiting JTAG, serial, USB
Remote	Rowhammer, Cache Timing	Buffer overflow, Heartbleed, Flooding/DoS

Solutions Rationale Against Threats

Physical	Logical
If an attacker can get local access to the device, make a cost/benefit trade off and protect against relevant local physical attacks over the lifetime of the device.	If an attacker can get local access to the device, aim to protect against local logical attacks. Reason: can be automated and executed by non-experts.
Aim to protect against remote attacks. Reason: scalable attacks can be automated and executed by non-experts from anywhere in the world.	

Level of importance to ensure security against threats High Higher Highest



Local attacks are performed by gaining physical access to a device, while **remote attacks** are performed by sending commands remotely over network connections. Knowledge gained from performing a local attack may lead to mounting future remote attacks. Although developing a remote attack may require significant expertise, it may be possible to automate the attack and have it executed by unsophisticated adversaries on a large scale. This implies that remote attacks are scalable. Remote attacks have the potential to be initiated from one device and impact millions of target devices in a very short time.

Logical attacks on devices, internet services or organizations occur by exploiting weaknesses in the implementation, which are mainly in software. They are performed by accessing standard interfaces, both wired and wireless. They can be automated and, once known, they do not require much competency to be mounted on a large scale.

Physical attacks hack devices by exploiting known, or learned, physical characteristics during device operation and breaking a critical piece of security, for example a cryptographic key. Remote physical attacks, implemented in software, such as Rowhammer[4,5], Meltdown/Spectre[6], cache attacks and power domain controller remote attacks have emerged in the past few years.

IoT will be confronted with all combinations of attack types[7,8]. Absolute security may be an illusion, but it is critical to ensure that a successful attack against a network node (IoT device or service) cannot be scaled and cannot impact an entire ecosystem.

4. *https://en.wikipedia.org/wiki/Row_hammer*
5. *https://googleprojectzero.blogspot.com/2015/03/exploiting-dram-rowhammer-bug-to-gain.html*
6. *https://meltdownattack.com/*
7. *https://securelist.com/iot-hack-how-to-break-a-smart-home-again/84092/.*
8. *https://www.pentestpartners.com/internet-of-things/ again/84092/.*

Let us say Bob had a **pacemaker installed 5 years ago**. This pacemaker has an actuator that, whenever certain fibrillation conditions are sensed, triggers an 800V impulse to defibrillate[9]. Note that it can be deadly to give such an impulse when a patient's heart is working normally. The pacemaker is **connected wirelessly** to Bob's smart watch and the smart watch is connected to his smartphone. Periodically, the pacemaker sends the measured data and its actions, via the smart watch and smart phone, to a hospital for remote patient monitoring. The pacemaker has a real-time clock used to accurately time-stamp the information sent back to the hospital. Its **firmware is upgradable** and new firmware is authenticated and integrity protected using a non-diversified shared secret – the password "abracadabra" – that is stored in the pacemaker. What can possibly go wrong?

A potential attacker, Jack, whose ultimate goal is to trigger the 800V impulse for as many victims as possible in a short period of time, has to first get the shared secret. Jack is not in a hurry, he can wait months preparing without being noticed before he launches the final, massive attack. The shared secret is in all pacemakers. He acquires a few samples of the pacemaker, analyzes the printed circuit board inside and performs local physical attacks. He identifies the components, locating the memories, power supply and JTAG connection. Jack puts a monitor on his acquired pacemaker to capture all the wireless messages sent to it. The objective of this monitoring phase is to wait until a firmware upgrade is performed to determine the format of the upgrade messages. Once this is known, he sends either the recorded upgrade messages or a fake random number of bytes, encapsulated in what looks like a firmware upgrade, to his samples and using a $300 digital oscilloscope, he recovers by simple power analysis the shared secrets used by the pacemaker to authenticate and decrypt the firmware upgrade. Now that he has the key to decrypt the firmware update, he can reverse engineer it and generate new firmware that will be accepted by any pacemaker because he now has the key used to encrypt and authenticate the malicious firmware.

The next step is mounting a massive remote logical attack. Jack prepares special firmware that on Friday the 13th at 00:00 will trigger an 800V impulse. For this purpose, he acquires the pacemaker management application used on a patient's smartphone. He reverse engineers it to find out how to detect that this application is installed on a phone and to detect how the firmware upgrade is sent to the smartwatch. He prepares a game for smartphones that contains a special function to detect whether the smartphone on which it is installed also has the pacemaker management application. The game also contains the new special firmware he has prepared which will be sent to the pacemaker by the game, if the pacemaker management application is also installed on the phone. The last step is to publish the game and to wait. If the game is popular, it will reach many patients and on the next Friday the 13th, the pacemaker catastrophe will happen.

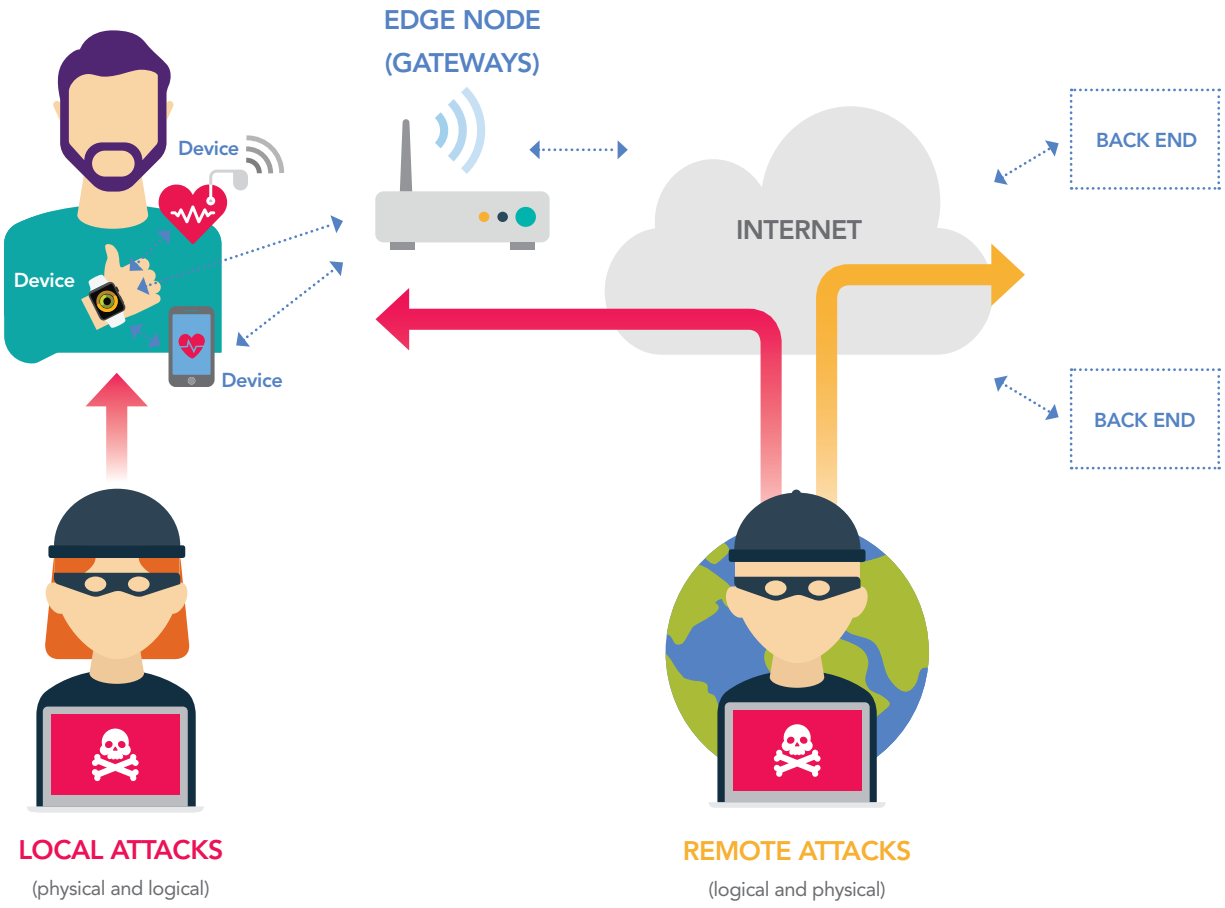
Now let us say that the designer of the pacemaker solution has raised the bar by applying good security practices like secret credential diversification, one may think this makes it safe against Jack – and it may for an average Jack. But if Jack is more sophisticated and has much more resources and competencies, or is simply more incentivized, he will use other tricks. Acquiring the secret in one pacemaker does not help Jack any longer, since he cannot reuse the secret learned from reverse engineering one pacemaker to attack all the others. He will invest more in another, more challenging attack where he will reverse engineer the interface software for the firmware

updates until he finds a bug. There is almost always an exploitable bug in software. Jack creates an unencrypted fake firmware update that exploits the bug found in the interface to prevent the decryption being performed, i.e. the specially developed firmware update from Jack is used in unencrypted form by the pacemaker because it has been told that it should not decrypt it. If Jack does not find a bug in the pacemaker's firmware update mechanism, he can try all other potential remote interfaces of the pacemaker until he finds one where a bug is present and can be exploited to remotely inject new firmware into the pacemaker to perform the same attack on Friday the 13th.

It may be that Jack is not interested in performing the attack against the pacemakers themselves but rather in exploiting the health monitoring application on the smartphone to install a botnet. In this case, Jack is an accomplished dark-side business man who can make a living by selling the services like DDoS or spam mails of his installed botnet.

This story may seem like a science fiction nightmare but the new challenges of IoT listed in the next section confirm that if security is not taken seriously, reality may soon catch up with science fiction. As shown in next chapter, NXP solutions with security by design are deployed in IoT devices and systems to make those scenarios unlikely, using countermeasures to raise the bar for an attacker to a level that makes it unattractive to mount the attacks in the first place.

Kinds of attacks

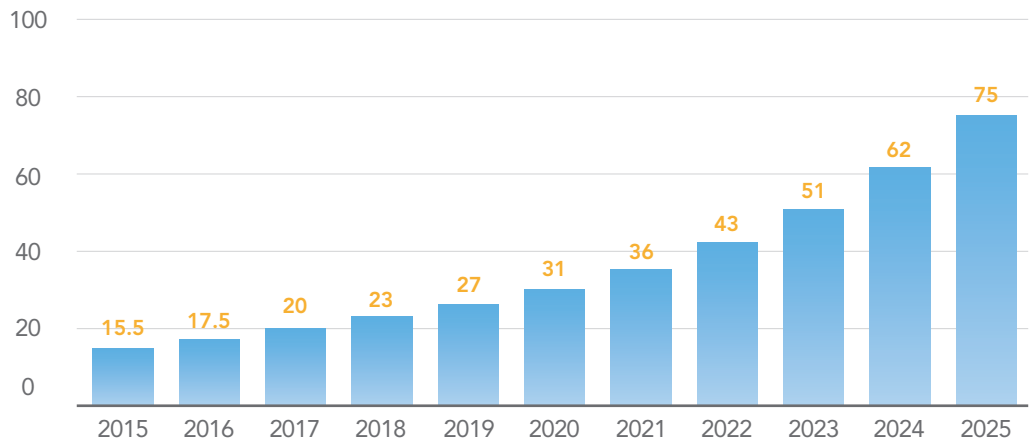


9. http://fortune.com/2017/08/31/pacemaker-recall-fda/

NEW CHALLENGES OF IoT

IoT brings a lot of new challenges and most of them bring their fair share of additional security burdens.

Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025 (in billions)



Source of data: https://www.statista.com

Large number of devices of the same kind

There can be millions of instances of each IoT device. If security-by-design is not considered, breaking one instance allows all similar devices to be broken as well. If an attack succeeds, it could lead to a large economic impact and in some cases to loss of human life.

Large number of devices accessible from one network access point

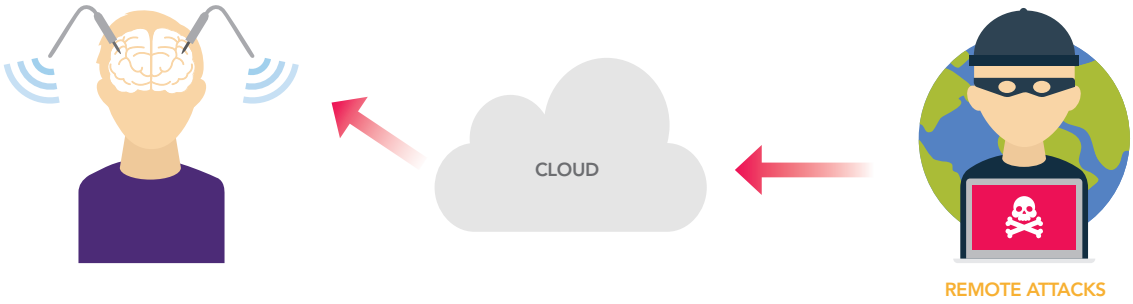
Often one access to the internet is sufficient to reach any other device on the network. This remote accessibility creates a huge attack surface for both remote logical attacks and remote physical attacks[10]. Most remote attacks start with the discovery of vulnerabilities while carrying out local attacks (logical and physical) against a few instances of the targeted class of devices. As an illustration, the Jeep Cherokee hacks all started with local logical attacks based[11] on local physical reverse engineering of a car, but were then extended and demonstrated to become massive remote attacks[12,13]. The potential reach of this remote attack was 471,000 vehicles. These massive remote attacks are facilitated by the fact that legacy IoT devices have no or very limited access controls. Most of the time access to the functionality of the device is controlled by a login and a password, which in many cases are the same for all devices of the same type[14], or a shared secret/key instead of diversified keys. To make the matters worse, there are sites on the internet that provide near automated attacks against classes of devices. These sites combine the possibility to select devices in a given class using search engines such as Shodan[15], Censys[16] and Zoomeye[17], and the application of an exploitation to those devices such as autosploit[18]. While massive attacks can be targeted at an ecosystem to harmfully alter the functions of the devices and their ecosystem, they can also be used to insert malware that does not alter the normal behavior of the devices but instead hosts a botnet application. In the latter case, the

10. *https://ics-cert.kaspersky.com/media/KL_ICS_CERT_Predictions2018_ICS_IoT_EN_30112017.pdf*
11. *https://www.computerworld.com/article/2484616/data-center/researchers-reveal-methods-behind-car-hack-at-defcon.html*
12. *https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/*
13. *https://www.wired.com/2016/08/jeep-hackers-return-high-speed-steering-acceleration-hacks/*
14. *https://www.theinquirer.net/inquirer/news/3012365/15-per-cent-of-iot-devices-owners-dont-change-the-default-password*
15. *https://www.shodan.io/*
16. *https://censys.io/*
17. *https://www.zoomeye.org/*
18. *https://www.scmagazine.com/autosploit-marries-shodan-metasploit-puts-iot-devices-at-risk/article/740912/*

infected devices are used to trigger a distributed denial of service (DDoS) attack against other targets. In yet another scenario, the attacker acquires any stored secrets – keys, PINs, passwords, confidential information – in the remote IoT devices and collects them, with the legitimate owner of the IoT device oblivious to the fact that his credentials have been stolen to be misused later.

Many IoT devices have actuators and are autonomous

IoT devices may not have only sensors but also actuators like wireless neurostimulators in people's brains[19]. Unlike smartphones, tablets or personal computers, devices such as autonomous cars, fitness monitors, surveillance webcams and household devices operate the actuators on their own and generate data during operation and communicate them without their owner's awareness. This autonomous operation exposes IoT systems to additional attack vectors, which have a huge impact on system security and safety: it has the potential to be life-threatening if the wrong decisions are taken or if the decision process is hijacked by attackers.



Many types of IoT devices for many use cases

There are ever expanding types of IoT devices as new use cases appear every day. As of now, there is no common standard and no interoperable security framework defined for IoT devices. This is different from other ecosystems such as payment, automated fare collection and electronic identity management, which are centralized. IoT security will require a consolidated standardization effort since all these devices are eventually connected to the same network. IoT will have to converge on globalized regulations the same way that the radio frequency regulations allow coexistence of RF devices. But these globalized regulations must encompass the mix in complexity and use cases of IoT devices. There is no one-size fits-all solution but the solutions must have an interoperable security.

IoT devices have unmanaged lifetimes

The lifetime of an IoT device spans an undefined number of years. It is not centrally managed. While a bank card is typically valid for 2 to 5 years and a passport for 10 years, an IoT device may be used for the number of years that the end customer chooses. This implies that the device content and device security have to be updated in the field to address new attacks or vulnerabilities discovered over its lifetime. This is applicable only if the device has been developed to be updatable. Even if designed for this purpose, a device may run out of processing power or have insufficient memory to support future updates. A manufacturer

19. *https://www.theregister.co.uk/2018/04/18/boffins_break_into_brain_implant/*

of devices may go out of business before the devices it produced have reached their end-of-life. Devices with different ages and with different security levels will coexist in the same network, and in the same systems. Legacy devices will likely be the weakest links and may have to be protected by additional security devices put around them or replaced. However, replacing old devices may be a challenge as well since the expensive systems they control have to be designed for such replacements. These are reasons why interoperable and standardized security features are needed.

Many IoT devices have limited resources

Many IoT devices will have limited processing power, storage capability and communication bandwidth, making implementation of standard security techniques challenging. The objective then is to distribute the security burden among the various IoT devices such as end-nodes, gateways, edge computing nodes and cloud services, so that overall system security is achieved. See Chapter 2 for more challenging thoughts on this topic.

IoT devices for critical and non-critical applications are mixed in one network

For example, critical energy distribution facilities are essentially interconnected with non-critical sport monitoring wearables as they share the same network. This provides enormous advantage for attackers who can hack non-critical and potentially low security, devices by reprogramming them remotely and making them members of a botnet to attack highly critical functions such as a smart factory, smart grid, the infrastructure for autonomous vehicles, hospital IT systems or emergency alarm systems[20,21].

IoT devices generate huge amounts of personal data

For reasons such as analytics and machine learning, IoT devices collect enormous amounts of detailed data and send the information to their service providers. Many of the IoT devices can be associated with a single individual. This implies that the collected data could be used to violate the privacy of the person, even if each individual device has been designed to be privacy preserving. This is because the potential for a privacy breach from unexpected data correlation can come from the system design. The challenge here is to balance the desire of IoT device manufacturers and IoT service providers to collect as much information as possible to improve their businesses, with the privacy preservation of individual users.

IoT devices could be the ammunition for future cyberwars

The highly damaging potential of remote attacks offers governments and large entities the opportunity to mount cyberwarfare. This goes beyond cybercrime. Cyberterrorism and cyberwarfare will have to be addressed seriously as they are present. In October 2016, approximately 100,000 IoT devices were hijacked by the Mirai botnet in a DDoS attack[22]. In 2017, a more sophisticated IoT botnet called Reaper was discovered, with code based partly on Mirai[23]. The resources available to attackers are unprecedented, meaning that security technology must match the level of risk. However, for IoT devices it is not reasonable to design them individually to the highest security level. The world must consider new co-operations.

20. *https://www.sirenjack.com/.*
21. *https://www.theregister.co.uk/2018/04/11/awooga_sirenjack_lets_hackers_channel_their_inner_hawaii_ema/*
22. *https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet*
23. *https://www.wired.com/story/reaper-iot-botnet-infected-million-networks/*

THE SOLUTION

SECURITY TIMELINE

IoT security must rely on two basic principles: security by design and privacy by design. Not applying those principles has the potential to be life-threatening or induce unbearable economic losses. The solution appears easy at first sight – simply apply those principles to the design of IoT devices and their associated systems such that their security level is sufficient to prevent those losses in life and money. The difficulty is that the ones making the decisions on the appropriate security levels and features, and the ones implementing them are not the ones that will bear the losses. However, ultimately manufacturing companies will be held accountable for their choices and implementations.

Given these boundary conditions, it is even more mission critical that the security choices must be commensurate with the economic value of the assets to be protected. Paying a reasonable price for security today will eliminate the need to pay an exorbitant amount later to fix the situation after a catastrophic event.

This implies that security features must be introduced to anticipate the sophistication of attackers and the scalability of attacks due to the explosion in number of devices and to the improved connectivity. The assumption must be made that attackers will go for the highest potential return on investment while the device is operational.

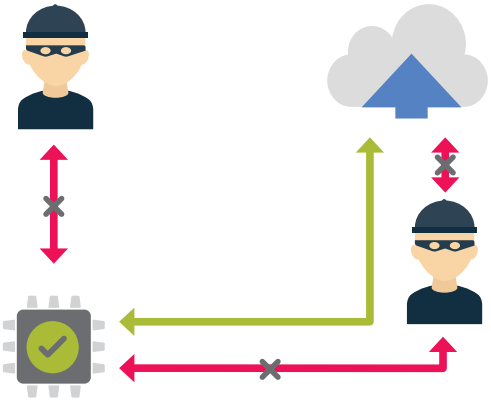
More and more devices will become directly connected and those devices have to defend themselves, but in some cases they can rely on other devices to protect them. These gateways have to also to protect themselves but they have more resources available than end nodes. The purpose is to keep the security expectations on low-end IoT devices within reasonable economic and usability margins.

As shown later in this document, a spectrum of architectures and related security features are available and can be used to make the transition to a fully trusted IoT future. NXP is developing products and solutions with future security needs in mind.

All the stakeholders building and maintaining IoT ecosystems should cooperate for interoperable and assessable security. The stakeholders span component and device makers, service providers, governments, standardization bodies, and educational institutions. This is how the path to the Internet of Trust can be paved.

SECURITY BY DESIGN

Security by design relies on well-known system properties: integrity, confidentiality, authenticity, availability. They must be combined in systems to offer end-to-end security, to comply with future, still to be created, IoT security standards, to counter the potential attacks and to act as cost-effective and safety-effective security protection mechanisms.

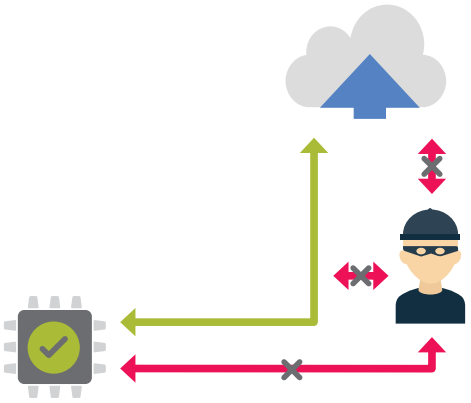


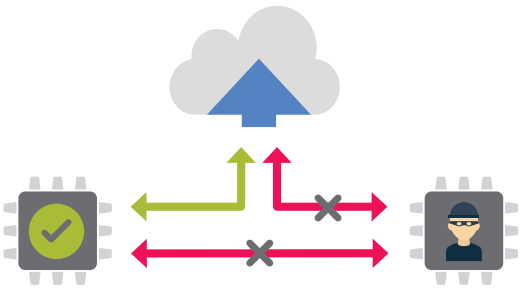
Integrity

Ensuring unmodified data transport & unmodified SW execution

Confidentiality

Keeping secrets secret (business value of data, privacy) – encryption is the technology of choice



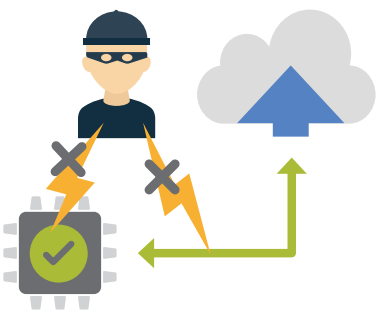


Authenticity

Verifying identities for source of data/SW, access control (trusted operations)

Availability

Ensuring that the services remain available



Devices and solutions must be resilient and should be designed as if they cannot depend on the integrity of the infrastructure; this is due among others to the large number of non-coordinated stakeholders operating this heterogeneous infrastructure. This means that attention must be given to runtime protection, recovery and damage control.

Runtime protection

Many assume that if one has secure boot and secure update mechanisms then the system is secure. For this to be true, both mechanisms and the firmware would need to be secure and without bugs. This is not the case as bug-free software should be considered an impossibility. An attacker can exploit the software and hardware bugs to mount runtime attacks after the system has securely booted and been securely updated while the system is up and running.

Analytics, recovery and damage control

The assumption is that devices will be attacked and sometimes the attacks will succeed. The security design of IoT devices can proactively limit potential damage using techniques like key diversification or white-listing IP addresses. But this is not enough, if an attack succeeds, analytics can be used to detect this situation and additional recovery and damage control can be applied with or without external service support.

In addition to blocking attacks and recovering when they do happen, security by design aims to reduce the attractiveness of attacking devices by ensuring that a successful attack against one device cannot be scaled to a myriad of similar devices. Among other measures, this implies that diversification of secret credentials (e.g. keys) is applied to all devices and all services.

Certification

If security protection techniques are combined to achieve proper system security, it is still essential to convince stakeholders that they can trust the system. One way to achieve this goal is to turn to certification schemes where the security claims of ICs, components, devices, services and systems are checked by trusted independent third parties according to well-defined and agreed procedures. Existing certification schemes developed for other ecosystems, such as Common Criteria or FIPS 140-2 for e.g. payment systems, are likely not adequate as-is to face the challenges of IoT. They are too rigid and tailored to their respective segments. NXP is actively participating in the definition of a European Certification Framework for IoT[24].
This is a mandatory step to go from the Internet of Things to the Internet of Trust.

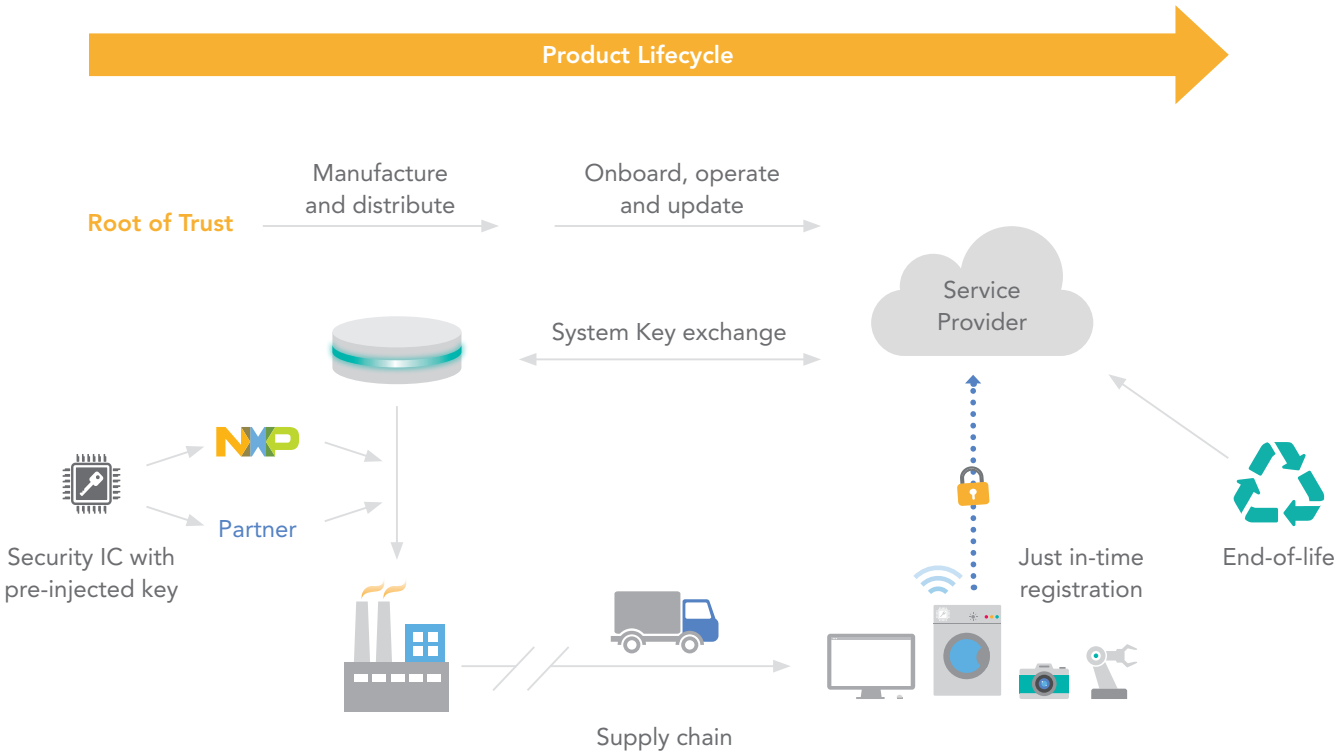
Security relies on secrets such as cryptographic keys and unforgeable identities. These are created and stored in the ICs, devices and systems. They are optionally updated during the operational lifetime and are retired with the decommissioning of the ICs, devices or systems. This is the purpose of trust provisioning and life-cycle management.

24. https://ec.europa.eu/info/law/better-regulation/feedback/8000/attachment/090166e5b6fa35cc_en

Trust provisioning

The way the secrets (keys and credentials like passwords, PINs, PUks, etc.), key digital certificates, identities and specific configurations are created, derived, diversified, and injected in the ICs, devices and systems is the purpose of trust provisioning. It is designed to make each and every instance of a device unique, identifiable and distinguishable from cloned or counterfeit devices. It also provides the necessary credentials for onboarding to the network and services. If the trust provisioning process is not designed with system security in mind, the overall system security of deployed devices and services will potentially collapse. The challenge is that, contrary to ecosystems like payment and identity where the trust provisioning process is in the hands of one or more clearly identified, cooperating stakeholders for the entire ecosystem, with IoT there are many independent actors and the split of liability and trust among those actors is not clear-cut. Therefore, the definition and implementation of trust provisioning must result from a partnership between the various potential stakeholders. NXP has proposed IoT relevant trust provisioning umbrella schemes to remove most of the burden from the shoulders of the stakeholders in the value chain.

NXP Security Solutions Deliver Protection at the Ecosystem Level



Security lifecycle

Some industries, like the payment industry, have a long tradition of standardizing the security lifecycle, while the IoT industry has yet to discover what it means. The IoT industry must introduce mature security management through the entire lifecycle of the product.

During the design, manufacture or distribution of products (ICs, components, devices…), they have to be protected against local attacks, but the manufacturing machines themselves have to be protected against local and remote attacks.

During the onboarding phase, the device comes in contact with the network for the first time and protection against remote attacks must be active. This is the moment where the security features must be such that attacks against specific operational devices are not scalable against the others.

During the operational phase, the device is protected by its intended security and privacy features. These features must provide protection against the scenario of the device being left unattended or stolen. While in operation, the device must also accept functional or security enhancements. This update mechanism needs to be protected against attackers as well.

When the device reaches its end-of-life, either because it is broken, it is stolen, it is lost, or it is deliberately decommissioned and not used any more (i.e. it is put in the trash bin), or when the device has been forgotten or sold secondhand, mechanisms should be in place such that getting a hold of such a device, where some keys could still be extracted, does not make a scalable attack possible.

Software security and hardware trust anchor

Some advocate that for IoT, hardware security can be replaced by SW-only security. There is no black and white validation of this position, but NXP advocates that the security of devices should be grounded in a hardware trust anchor. This HW trust anchor should, as a minimum, resist local logical and basic physical attacks, which are performed to scale to massive remote attacks. The HW trust anchor should also resist remote physical attacks. Countermeasures required to resist those new attacks are conceptually similar but not always the same as the ones to resist local physical attacks on the chips. The two families of attacks, remote physical and local physical, are not aiming at the same physical characteristics. Last but not least, the HW trust anchor should help augment the resilience of the devices by supporting runtime integrity, analytics, recovery and damage control.

PRIVACY BY DESIGN

Privacy must be taken into account when starting with the architecture of a new system and cannot be treated as afterthought. NXP uses strong security measures to facilitate the privacy preservation properties of its product portfolio. NXP products are designed to protect users' privacy.

Privacy preservation adoption will happen globally, driven by new legislation and regulations like the General Data Protection Regulation (GDPR) in Europe. These new regulations will restrict the data collection that is allowed to be performed by devices and services.

This is another strong reason why a hardware trust anchor is required in IoT architectures – it offers secure storage of the keys and secure management of user identities while respecting their privacy settings, individual device identities in a privacy preserving way, and enables the deployment of confidential communication.

Homomorphic encryption – computations are performed on encrypted data without decrypting them – and attribute-base cryptography – an encryption scheme where the decryption is conditioned by specific values of attributes of the user to support, among others, anonymous operations – are part of the toolbox available to enhance the privacy of the users while using IoT products.

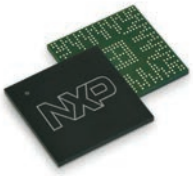
NXP SOLUTIONS

NXP contributes significantly to the expansion of secure IoT ecosystems. In support of this goal, NXP offers a comprehensive product portfolio including application processors, micro-controllers, NFC devices, smart labels, secure controllers and authentication devices. These categorized solutions cover solutions from basic hardware and software with limited platform security to richer solutions that provide HW isolation, as well as protection against side channel and fault injection attacks. At the top end of the scale, NXP solutions provide highly secure, hardened HW secure elements as discrete components as well as embedded secure sub-systems.

As an example, the NXP i.MX based MPUs, designed for demanding IoT devices such as gateways, are equipped with extensive platform security features (secure boot, secure update, tamper detection) with internal hardware isolation, enabled by several cores, and a sub-system with secure storage and crypto-acceleration to independently enhance the security of the entire SoC (System On Chip).

For smaller nodes, NXP offers the Kinetis micro-controller family with wireless connectivity. They come with standard platform security features (secure boot, secure update), and some Kinetis variants include a secure sub-system.

As another example, NXP automotive high-end gateway processors (S32G) are available for integration into secure designs for Car2X communications and in-vehicle networks.

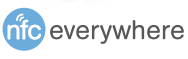


In addition to those processors, NXP offers companion ICs that can contribute to security architectures. For example, the A71CH is an authentication IC that provides tamper-resistant key storage and key usage, and offers a trust provisioning service to the host platform.

NXP product definition and implementation are designed to adhere to the security by design and privacy by design principles wherever required.

NXP's vision is that there will be a large palette of security architectures for IoT appropriate for different use cases. The security by design approach will consist of selecting the right architecture, and subsequently matching the various components of the chosen architecture, with the right products and the required software architecture on top. NXP provides many of the IoT components with different security levels. Let us illustrate this concept on a few example architectures. These architectures will also evolve with time with the addition of additional HW protection mechanisms to match the evolution of attacks and the growing security expectations of the IoT ecosystems.

The minimum architecture is a standard SoC with SW and basic HW hardening together with a secure boot mechanism, lifecycle protection and secure debug. All functions are performed by the SoC, with any sensors and actuators connected to it **(see Figure 1)**.



The next step is to apply one or two of the following improvements. Replace the SW-based hardening with further HW-based hardening, such as Arm TrustZone, to improve the partitioning between the non-sensitive and the sensitive processing. Add a secure element to the architecture, to where any sensors and actuators are directly connected **(see Figure 2 (without TZ) and Figure 3 (with TZ))**.

A step-up architecture is to embed a secure sub-system in the SoC itself. This is designed to enable protection on the complete SoC platform, secure boot, secure access control, secure processing units and key stores. The "Security Controller" on latest i.MX MPUs is such a sub-system **(see Figure 4)**. In this case, sensors and actuators are connected to the SoC and it is the integration of the secure sub-system, the optional TZ support and the HW and SW architecture that enhances the integrity of the sensor and actuator data and behavior.

Figure 1

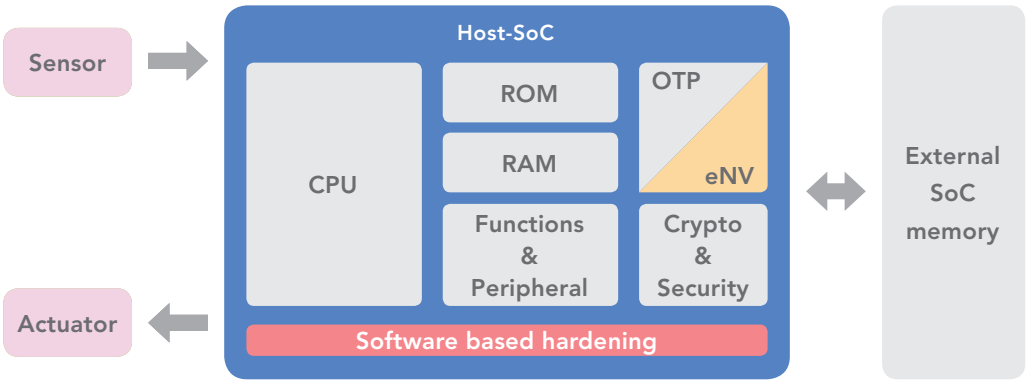


Figure 2

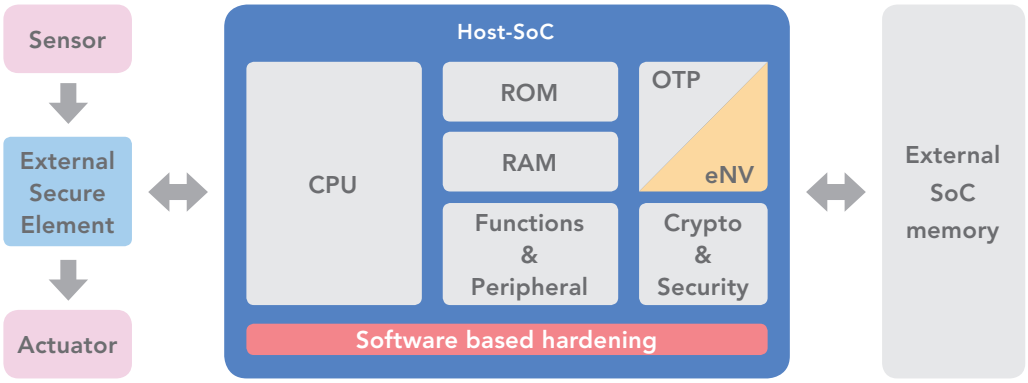


Figure 3

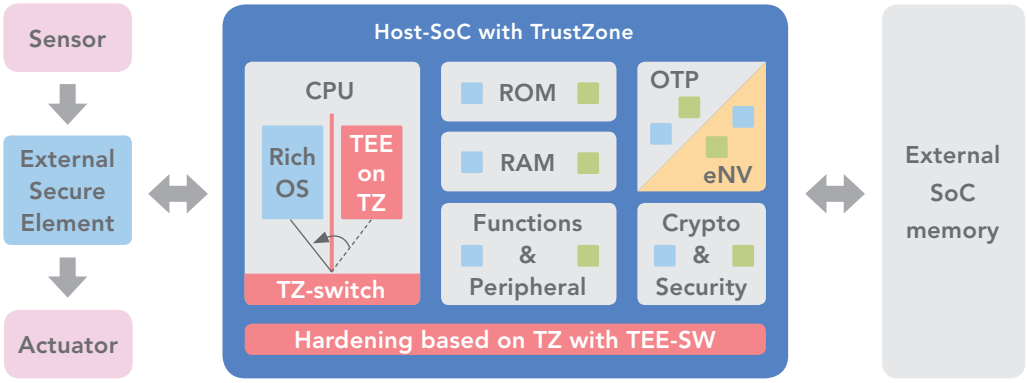
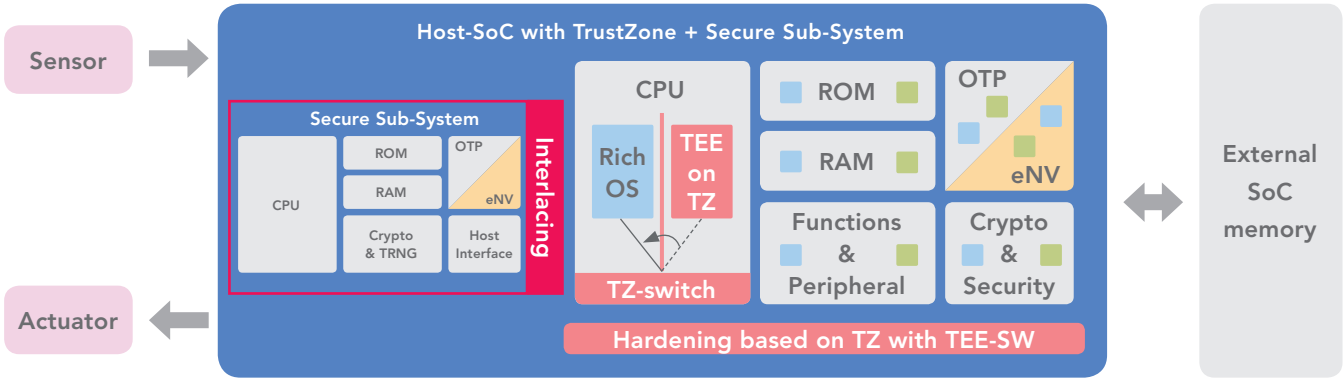


Figure 4



NXP ENGAGEMENT

NXP is committed to the future of IoT and driving its evolution from the Internet of Things to the Internet of Trust. With this goal, NXP has signed the Charter of Trust[25] with other key industry players and stakeholders of IoT ecosystems.

Security ownership

Matching the expectations of the Charter, NXP is committed to actively owning its share of responsibility for the security of IoT. NXP has been connected to national and international governmental institutions around the world for many years. With them, NXP helps coordinate the security expectations, security certifications, security requirements and security legislation. For example, NXP is a member of the European Cyber Security Organisation (ECSO)[26] and has connections with the European Union Agency for Network and Information Security (ENISA)[27]. NXP also actively participates in standardization bodies such as ISO, FIDO, GlobalPlatform, and NFC Forum, to promote future security interoperability. NXP also participates in the definition and promotion of new certification schemes to give adequate and affordable guarantees that IoT solutions match their security claims.

Responsibility throughout the digital supply chain

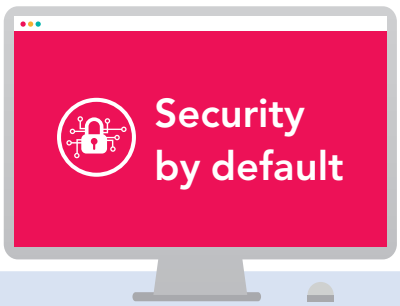
NXP provides security building blocks to provide secure identities (either as a discrete component used in conjunction with MCUs and MPUs or as an IP integrated in MCUs and MPUs), but the device identities and trust can only be established by partnering with the device manufacturers: system security is paramount. Encryption and other security functions are available in relevant NXP offerings. A dedicated group in NXP, Customer Application Support, helps NXP key accounts to make secure design-ins to help them achieve the expected system security. NXP is also engaged in partnerships with key stakeholders such as cloud and service providers.

Charter of Trust

25. *http://media.nxp.com/phoenix.zhtml?c=254228&p=RssLanding&cat=news&id=2332965*
26. *https://www.ecs-org.eu/*
27. *https://www.enisa.europa.eu/about-enisa/structure-organization/psg*

Innovation and co-creation

NXP invests in innovation as exemplified by its broad patent portfolio, its having been honored in 2016 and 2017 as a **"Top 100 Global Innovator"**[28,29], its participation in multinational innovation projects and its cooperation with many universities. NXP also invests in exploring new areas, like machine learning, to improve security and resilience against attacks.



NXP has a long tradition of applying the concepts of security by design and privacy by design throughout its product portfolio and NXP is continuing on this trajectory, as shown by NXP announcements[30].

28. *http://top100innovators.clarivate.com/*
29. *https://globenewswire.com/news-release/2018/02/01/1330436/0/en/NXP-Honored-as-2017-Top-100-Global-Innovator.html*
30. *http://media.nxp.com/phoenix.zhtml?c=254228&p=irol-media-center*

CONCLUSION

The clock for the **Internet of Things** is ticking. Industry, governments, standardization bodies and service providers need to work together to transform the Internet of Things to the **Internet of Trust**.

The challenges are unprecedented with huge numbers of devices, highly complex systems, almost instantaneous interconnectivity and many different use cases with different security level requirements all mixed up in the same network. Safety-critical devices are already accessible from non-safety critical devices, there is a mix of legacy unsecure devices and new moderately secure devices, end-nodes have limited resources and there are large amounts of sensitive data in the end-nodes and gateways. To add to these challenges, new attacks are uncovered at an increasingly rapid rate. Remote physical attacks have emerged and new powerful attackers have entered the scene. The word "cyberwar" is now part of IoT vocabulary.

The path to the Internet of Trust is to introduce the appropriate security and privacy-preserving features at the right time, while maintaining the balance between functionality, performance, usability, innovation and cost. If features are introduced too early, or too costly or overly complex, they may not be accepted. If too late or not meeting the security expectations, the financial losses (or worse, human losses) may be high.

The trust will come from interoperable security and new certification schemes. All stakeholders must be able to trust that the security and privacy claims of products and services are matched by their implementation.

NXP is playing a key role in the creation of the Internet of Trust. The engineering teams and businesses live according to the Charter of Trust. NXP defines IoT security certification schemes. It continuously improves its product offering to strengthen the security of end-nodes and gateways while supporting its customers in building end-to-end secure and privacy-preserving systems. NXP is introducing new technologies and contributes to advanced security toolboxes like machine learning and secure sub-systems for SoCs, to cite only two.

With this Whitepaper we bring our expertise as a market leader in secure connectivity to the table. NXP technology helps developers build IoT equipment that is designed to be reliable, secure and trusted. From MCUs, to processors, to secure elements, to software and services — NXP provides solutions for ecosystems that require built-in protection. As shown in this paper, adding optional security to IoT systems as a defense against attacks is not sufficient. Instead, NXP commits to a security by design approach, taking privacy and data protection into account in the design and set-up of products and services. We at NXP see the industry's responsibility in protecting device security and privacy with respect to the storage, transfer, use and processing of data. Let's make this thinking integral part of the future IoT!

GLOSSARY

5G	5th generation wireless systems
Car2X	Vehicle to Vehicle & Vehicle to Infrastructure Communication
CPU	Central Processing Unit
DoS	Denial of Service
DDoS	Distributed Denial of Service
ENISA	European Union Agency for Network and Information Security
eNV	Embedded non-volatile memory
EU	European Union
FIDO	Fast Identity Online
FIPS	Federal Information Processing Standard
GDPR	General Data Protection Regulation
HW	Hardware
IC	Integrated Circuit
IoT	Internet of Things
IP	Intellectual Property, Internet Protocol (depending on context)
ISO	International Organization for Standardization
IT	Information Technology
JTAG	Joint Test Action Group
MCU	Microcontroller Unit
MIFARE	NXP Semiconductors owned trademark of a series of IC used in contactless solutions
MPU	Microprocessor Unit
NFC	Near Field Communication
OTP	One time programmable
PIN	Personal Identification Number
PUK	PIN unlock key
RAM	Random access memory
ROCA	Return of the Coppersmith Attack
ROM	Read only memory
SoC	System on Chip
SSS	Secure sub-system
SW	Software
TEE	Trusted Execution Environment
TRNG	True random number generator
TZ	TrustZone
USB, USB-C	Universal Serial Bus connector system, USB Type C