WHITE PAPER

ublox

Four steps to IoT security

NAGRA
KUDELSKI GROUP

Using a robust Root of Trust to protect connected applications.

Abstract
IoT devices and the ecosystems of which they form a part are vulnerable to cyber-attacks because they rely on communications over the open Internet, are often built using low-cost hardware, and are frequently installed in untrusted locations. This means IoT devices are exposed to a wide variety of rapidly evolving threats, often intended to disrupt their communications or misuse their capabilities. It’s important, therefore, that IoT devices implement a resilient and agile security architecture. This white paper provides the background, vocabulary and key concepts necessary to develop and deploy IoT ecosystems that are resilient to evolving cyber-threats.

White paper: Four steps to IoT security
Author: Eric Heiser, Head of Services & Security, u-blox
Conor Ryan, Vice President IoT Chipset Strategy, Kudelski Group

Contents

Building a secure IoT.

The Internet of Things (IoT) depends, by definition, on creating an ecosystem of distributed devices (the 'Things' of the IoT) connected over a communications infrastructure that can be private, but which is often the open internet. Combining widely distributed, and often low-cost, devices with arbitrary network connectivity and cloud-based applications can lead to IoT ecosystems that are vulnerable to a wide variety of security threats.

One way to counter these threats is to ensure that the physical and digital assets of the ecosystem are properly protected. This means embedding robust security features in the IoT devices, so that they can form the basis of a chain of trust, control, and integrity that applies throughout the resultant IoT ecosystem, and for its lifetime.

Here are five key issues to address when thinking about how to secure such IoT assets:

- **ENFORCE UNIQUE DEVICE IDENTITIES:**
  Any device in an IoT ecosystem that produces data or executes commands must have a unique identity that cannot be cloned. These unique identities form the basis for all other security functions.

- **CONTROL ACCESS TO DEVICE RESOURCES:**
  IoT devices are often installed in uncontrolled environments, which makes them vulnerable. Hackers may access the unencrypted data the devices hold, upload malware for onward distribution, subvert the devices to carry out distributed denial-of-service attacks, or simply gain access to features for which they haven't paid. This means it is important to ensure that device resources, such as CPU, memory, and connectivity, can only be used for their designated tasks.

- **PROTECT DATA INTEGRITY:**
  The protection of data, at rest or in motion, is extremely important, to ensure privacy, confidentiality, and to meet general regulatory requirements, such as GDPR, as well as industry-specific rules such as HIPAA, the US health information privacy rules.

- **SECURE DECISION-MAKING:**
  IoT devices and ecosystems must be able to rely on the validity of the input data they use to make decisions, whether those decisions are made using traditional logic or machine-learning algorithms. Decisions should be executed in a secure environment so that they are safe from tampering and intellectual-property theft.

- **AUTHENTICATE COMMANDS:**
  It's important to be able to validate that any commands sent to an IoT device (such as 'inject insulin', 'open/close valve', 'apply brakes' etc.) come from a legitimate source.

A focus on securing IoT devices alone will not enable more secure IoT ecosystems, if it is not matched by a more agile approach to security in the organizations that develop and deploy them.

Organizations that develop IoT devices need a clear understanding of the current and emerging threats to which their devices are exposed, in order to set up and sustain the necessary security processes. These processes must be able to adapt to the rapidly evolving IoT environment and the resultant emerging threats.

Organizations that implement an IoT ecosystem will have to update their security policies and strategies rapidly, to match the rapid evolution of security threats to the IoT.

In both cases, IoT security strategies must be simple, scalable, and sustainable in order to deliver the short- and long-term objectives of IoT-enabled businesses.

Security is part of quality assurance and control.

Fortunately for IoT device developers and organizations that want to build IoT ecosystems using those devices, security issues are already part of quality assurance and control in modern software development processes. The industry has adopted total quality management strategies, and implemented them by making the principle of Plan, Do, Check, Act (PDCA) development processes central to the ISO-27001 information security management standard.

Industry and government agencies have also developed strategies for characterizing security levels as part of an overall product quality assurance and control program. These strategies include the Common Criteria for Information Technology Security Evaluation (ISO/IEC 15408), the US's Federal Information Processing Standards Publication (FIPS), and France's Baseline Security Certification (known as CSPN).

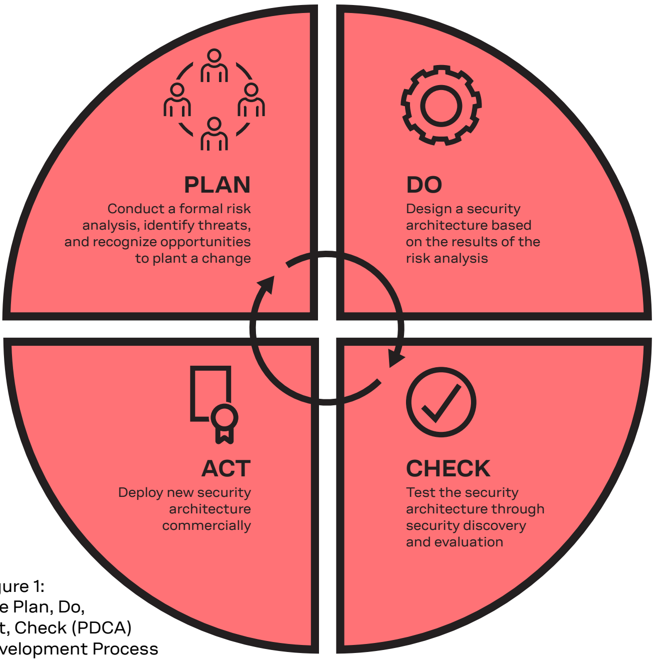

PLAN
Conduct a formal risk analysis, identify threats, and recognize opportunities to plant a change
DO
Design a security architecture based on the results of the risk analysis
ACT
Deploy new security architecture commercially
CHECK
Test the security architecture through security discovery and evaluation

Figure 1:
The Plan, Do, Act, Check (PDCA) Development Process

The European Union has also charged the European Network Information Security Agency with creating a way to issue European Cybersecurity Certificates for products, processes, and services, to be recognized throughout the Union. Its approach builds upon the success of CSPN, which is operated in France by ANSSI, the national security agency. Private organizations are also promoting their own IoT security certification schemes. Some exist solely to grow their businesses. In the best cases, the certification schemes are designed to ensure that the security features on their products are used correctly. But the only way to comply with local and international laws and regulations is to abide by standards vetted by independent public bodies.

Clearly, developing secure IoT systems that can be assessed and certified as meeting such standards is a complex and nuanced job. Our experience working with companies worldwide tells us that designing, implementing, and maintaining an IoT security architecture is too complex for most companies to undertake on their own. That's why we have partnered with Kudelski Group, a world leader in digital security.

Kudelski was an early backer of the EU approach to device security, supporting the CSPN and contributing to some of the independent bodies that oversee the Common Criteria. As a result, Kudelski has developed a comprehensive approach to security evaluation that combines industry best practices with more than 30 years of experience designing, testing, and certifying third-party components and devices.

The result of the partnership between u-blox and Kudelski is an end-to-end security process that helps users design, test, and implement a security architecture that prepares IoT devices for the diverse and constantly evolving threats they will face once deployed.

The process uses the PDCA[1] strategy pictured above. This white paper discusses each of the four steps, to provide readers with the context, concepts, and vocabulary necessary to understand how each phase contributes to the development of highly secure IoT devices and the ecosystems they enable.

[1] https://asq.org/quality-resources/pdca-cycle

1 PLAN

The route to a secure IoT starts with planning. This involves identifying business risks and high priority assets in need of protection, followed by a threat assessment and establishing security measures that mitigate risks. The assessment needs to be rigorous and combine a top-down approach, centered on what already exists and what remains to be built, with a bottom-up one, focusing on how each part of the ecosystem contributes to the security of the whole solution. The methodology adopted should be flexible enough to cover everything from an early-stage venture to an IoT system that is already in production in a large organization.

The Kudelski Group and u-blox use the STRIDE methodology (see diagram below) to carry out system- and device-wide risk assessments. STRIDE, developed by Microsoft, enables the identification and classification of threat scenarios, and the estimation of the likelihood of each type of attack and its potential business impact. The assessment provides a complete view of an organization's security policy, taking into account all security- and risk-related output already produced by the organization.

> Threat assessment is a key stepping stone to effective compliance and formal certification

The Kudelski Group's security expertise enables us to tailor an assessment that matches the complexity and business sensitivity of each situation. The assessment is primarily done through interactive workshops.

The output is a document that enables an organization to start and sustain an integrated risk-management approach encompassing both business and technology. It becomes a stepping-stone towards compliance or even formal certification, according to norms, standards, and regulations.

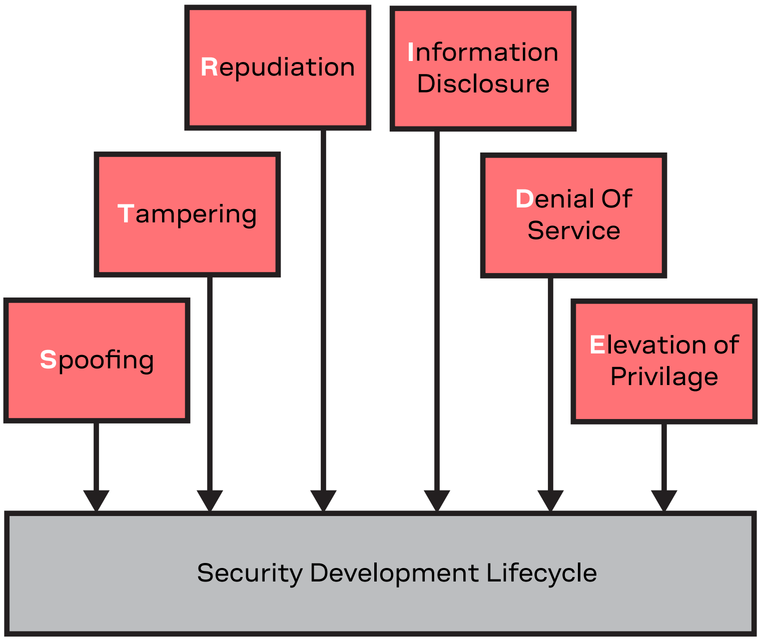


Figure 2: STRIDE Risks and Threats Assessment

[2] https://en.wikipedia.org/wiki/STRIDE_%28security%29

2 DO: Design your security architecture

Having carried out a rigorous threat assessment, the next step is to translate its findings into the design of a resilient security architecture for your IoT solution. If you choose to work with u-blox modules, you can reduce your time to market and simplify this process by using Kudelski IoT security technology, which is integrated into some u-blox cellular modules, and supports many IoT use cases (see section 5.2 for more details).

The design phase is a fundamental part of an IoT project, as it is typically done once and then reused for an entire product family. Finding, hiring, and maintaining security expertise is difficult, as expert security resources are notoriously scarce. Effective security also involves continuous, high-level training of key staff, yet this is often perceived as a cost that has no clear return on investment until something goes wrong.

Based on the findings of the threat assessment, Kudelski security experts and u-blox engineers will propose the best architecture for your IoT device design to maximize the security capabilities of the u-blox products it incorporates and avoid vulnerabilities in the field. This approach should reduce time to market and increase cost effectiveness, as Kudelski and u-blox experts are continuously trained and will quickly find a solution, reducing your need to hire and maintain in-house security experts.

The DO phase of the PDCA process addresses both hardware and software. Designing the hardware architecture is generally straightforward, because using secure u-blox cellular products inherently creates the basis for a secure design.

Designing the software involves integrating customer applications with the Kudelski IoT Security Platform. The platform includes all the functionality to connect application data to application servers at the highest level of data confidentiality and integrity. Data is secured from the device, across the communications network, and through to the application server.

2.1 The Root of Trust defines the product

The functionality that enables u-blox and Kudelski Group to be confident that they can create secure IoT devices is known as a Root of Trust (RoT). It gives a device a unique, immutable identity, along with the hardware and software cryptographic capabilities needed to enable trusted functions. Once a RoT is in place, all parties can trust the identity, authentication, communication, and data coming from a device.

The Kudelski Group has proven skills in designing, implementing, and managing this kind of functionality. u-blox is integrating Kudelski's IoT Security Platform into several of its product lines to take advantage of these skills.

It's possible to implement a RoT and the application programming interface (API) layers that interact with it in various ways, each of which provides a different level of robustness to security threats.

The most basic RoTs are implemented in software, while the most robust RoTs are implemented in hardware. The choice of RoT implementation strategy must be based upon an understanding of the appropriate security level for your application, which in turn relies on a proper threat analysis. Once the RoT has been implemented in a device, it can be used to enable any security use case.

As Kudelski and u-blox integrate their products, new options for various security requirements will be announced.

Root of Trust robustness level	Root of Trust embodiment	Application
Average	**Software only**	Preventing basic attacks. Such an implementation may have serious limitations and should be used with caution.
Good	**Inside a trusted execution environment**	A sound implementation that is adequate for IoT sensors and similar devices confronted with casual risks.
Better	**Inside eUICC (eSIM)**	An advanced implementation that enables coverage of use cases in which a device or data breach would have serious consequences for the business. Generally certified to Common Criteria.
Best	**Inside the secure element**	A best-in-class implementation that enables coverage of all common use cases. Generally certified to Common Criteria.
Best+	**Inside the integrated secure element with iUICC**	World-class security for advanced, high-risk use cases requiring a high level of security – e.g. devices that perform high-risk physical actions without human verification. Generally certified to Common Criteria.

2.2 Enabling compliance and certification

A RoT provides the functionality that underpins device security, but its robustness alone is not enough to enable specific levels of security compliance or even formal certification, because those measures apply to the device as a whole. That’s why the device must be implemented according to the security requirements of its target market and the security standards and authorities that apply in that market. Practitioners know that vulnerabilities are more often found in the implementation of security features than within the underlying cryptographic algorithms. This is why quality assurance processes are key.

The main value of a compliance or certification body is its independence. Business-backed or proprietary organizations are prone to conflicts of interest. This is one reason why a standard such as Common Criteria has stood the test of time: backed by inter-governmental bodies and strong governance, it has steered clear of conflicts of interest.

As another example, the CSPN certification defined by the ANSSI is based on a list of strictly vetted security labs. Their process bans all communication with the product manufacturer once the evaluation has started and builds in other measures to avoid conflicts of interest to ensure that the certification can be trusted.

The output of this DO phase is a secure architecture and design that is ready to face penetration testing in the next phase of the PDCA security process.

2.3 Glossary of security assurance and evaluation terms

Root of Trust
In cryptographic systems that have a hierarchical structure, a Root of Trust (RoT) is an authoritative entity for which trust is assumed and not derived. This creates a secure identity for the device that forms the foundation of all security functions and use cases supported by the system.

A hardware RoT can include features such as tamper detection and protection, secure storage, the ability to handle keys and security assets, and resistance to side-channel attacks. A RoT can also be executed in software but requires the use of advanced protection techniques, such as white-box cryptography and software obfuscation, to ensure that it can withstand attack.

Security assurance requirements
Security assurance requirements describe the measures that must be taken during the development and evaluation of a product to assure its compliance with the claimed security functionality. A security evaluation may, for example, require that all source code is kept in a change management system, or that full functional testing is performed.

Evaluation assurance level
An evaluation assurance level (EAL) is a numerical score that describes the depth and rigor of any security evaluation or quality-control process that has been applied to a product. For example, Common Criteria lists seven levels, with EAL 1 being the most basic (and lowest cost to implement and evaluate) and EAL 7 being the most stringent (and most expensive to implement and evaluate).

Higher EALs do not imply better security. They only imply that the security assurance claimed for the product has been more extensively verified.

Target of evaluation and security target
The target of evaluation (ToE) usually refers to the product or system that is the subject of a security evaluation. It can also refer to the document, known as the security target, which identifies the security properties of the ToE.

The ToE document defines the assets that are to be protected, the security functional requirements (SFRs) or security features that have been implemented to protect them, and the attacker's profile. The attacker's profile is key, as it also infers the methods and means that attackers could use to try to break the product's security. These might range from simple reverse-engineering by a student to invasive hardware attacks using capabilities only available to organized crime.

The product is evaluated against the ToE. This enables vendors to tailor their evaluation to match the intended capabilities of their product. An IoT pet tracker may, for example, not have the same functional needs as a surveillance camera, and so will be evaluated against a different list of requirements. The ToE is usually published so that potential customers can determine which SFRs have been certified by the evaluation.

3 CHECK: Defend, attack, score

3.1 Quantitative and qualitative approaches to security

When is an IoT device secure enough? Answering this question objectively requires both a formal threat assessment and taking steps to quantify and qualify the device's security robustness using accepted references and methodologies.

One widely used approach is attack scoring. This enables organizations to refine EALs by giving them a quantitative score, while limiting subjectivity through vetting by an independent third-party security laboratory. The final score is reached in agreement between a security laboratory (such as Kudelski's) and the official certification body (for instance, ANSSI). Device manufacturers can then use the score to advertise the security robustness of their product.

Baseline security certifications such as CSPN typically use the Joint Interpretation Library scoring methodology, which was born out of the Common Criteria standards. Another mechanism is the Common Vulnerability Scoring System managed by FIRST (Forum of Incident Response and Security Teams), which is mainly used to score IT vulnerabilities.

These mechanisms do not score a product's security robustness but focus instead on the seriousness of any vulnerabilities discovered.

Hands-on security evaluations can be supplemented by formal or semi-formal verification to assess the correctness of algorithms using formal mathematical methods. This may be required, for instance, to verify cryptographic protocols.

For most IoT products, a qualitative baseline security evaluation is sufficient. Any evaluation is made easier if the product relies on building blocks that have already undergone a security evaluation process, such as the u-blox modules that are already secured by Kudelski technology.

3.2 Quantitative approaches: attack identification and scoring

There are two components to identifying an attack, which is an essential part of scoring an attack. The first step is to evaluate the effort required to create an attack. The second step is to demonstrate that the attack can be applied to the ToE. This evaluation often involves assessing both the equipment and the skills an attacker would need to make an attack.

The next step is to score the exploitation of an attack. This involves carrying out the attack on another instance of the ToE using the analyses and techniques defined in the identification phase. This step measures how easily an attack can be reproduced.

Not all theoretically possible attacks are practically feasible. Some take too long. An "elapsed time" score measures how long it takes to carry out the identification or attack phases. The rating "not practical" is used when an attack cannot be exploited within a timescale that would be useful for the attacker. These timescales are defined in the threat assessment.

Other parameters include:

- Expertise, which measures the skill required by the attacker;
- Knowledge of Product, which measures whether the attacker needs confidential information to mount an attack, or if publicly available information is enough;
- Access to Product, which measures the number of samples needed to carry out an attack;
- Equipment, which measures whether the attacker needs to access specialized, standard, or custom equipment;
- Open Samples, which measures whether the attacker can load arbitrary software onto the product to simplify the attack.

The role of the security evaluation is to estimate the value of each of these factors – time, access, knowledge, etc. – to an attacker.

3.3 Qualitative approaches: the practical way to a secure IoT

An alternative way of ensuring the security of an IoT device is to get a qualitative evaluation by a trusted security laboratory. This approach emphasizes the creation of practical feedback that companies can use to achieve a security or confidence level that adequately addresses the vulnerabilities revealed by the threat analysis.

The device is tested to identify whether it has security gaps that could lead to the successful execution of high-probability, high-impact attacks. The amount of evaluation for each activity is set by the allocated testing time, the required expertise, and the complexity of the tools needed to fully simulate a realistic attack. A particular security level is said to have been reached when all testing activities fail to reveal a security gap that would enable the attack.

u-blox works with Kudelski's Device Security Discovery service to simulate the typical path of attack, taking into consideration current technologies and knowledge to highlight the strengths and vulnerabilities of the system. This approach goes beyond standard penetration testing, by covering the most probable local and remote attack vectors that could impact the device's integrity, availability, or data confidentiality.

u-blox also works with Kudelski's Device Security Evaluation service to cover hardware attacks. The security of the semiconductors embedded in the device is tested against attacks including fault injections and side-channel analysis. These techniques ensure that security countermeasures cannot be defeated when an attacker has physical access to the device, and that cryptographic algorithms and secrets such as private keys are secure. The Device Security Evaluation service requires an agreed evaluation scope or ToE, whereas the Device Security Discovery service uses a standard approach.

IoT Security Lab rating structure for Device Security services

Evaluation domains	Typical IoT security lab activities	Service coverage	
Remote attacks	Exploration phase consisting of documentation and OSINT review, security domains identification, CVE identification device penetration testing	Device Security Discovery	Device Security Evaluation
Network attacks	Communication protocol identification including proprietary interfaces and debug ports, wireless communication penetration testing, mobile app		
Local attacks	Tear-down, PCB inspection, design analysis, memory dump (targeted partial reverse-engineering), analysis of anti-tampering mechanisms, software attacks		
Elementary hardware attacks	Low-cost non-invasive hardware attacks (single electrical glitch fault injection/ simple power side-channel analysis)		
Advanced hardware attacks	Advanced non-invasive (electrical and EM glitch, differential power side-channel analysis) and semi-invasive hardware attacks (laser fault injection)		

4 ACT: Deploy, scale and, sustain secure IoT

Once IoT security has been planned, designed, and evaluated, it must be deployed, scaled, and sustained throughout a product's lifecycle to ensure the desired return on investment for IoT ecosytem operators.

4.1 Deploy

One of the biggest challenges in creating IoT ecosystems is to provide a unique identity for each IoT device before it is deployed. In situations where the threats and business value are lower, software security implementations may be used, but for high-value, high-exposure IoT applications, each device must be given a unique identity securely provisioned in a hardware RoT at a trusted location in production.

u-blox and Kudelski simplify the deployment of secure IoT devices by integrating robust IoT security into every module, ready to be integrated into devices. The unique, embedded RoT and security client protects all key IoT assets, as outlined in Chapter 2, and can be used to secure any use case you wish.

4.2 Scale

The second challenge of the ACT phase is scaling the deployment and operation of an IoT estate. If an ecosystem uses a limited number of devices, this is not an issue, but many companies are deploying millions of IoT devices. This requires features such as zero-touch provisioning, securely connecting authorized devices to the cloud, and efficient key-management schemes that minimize bandwidth usage and maximize battery life. The u-blox/Kudelski solution can ensure that an IoT ecosystem is simple and secure, even at massive scale.

4.3 Sustain

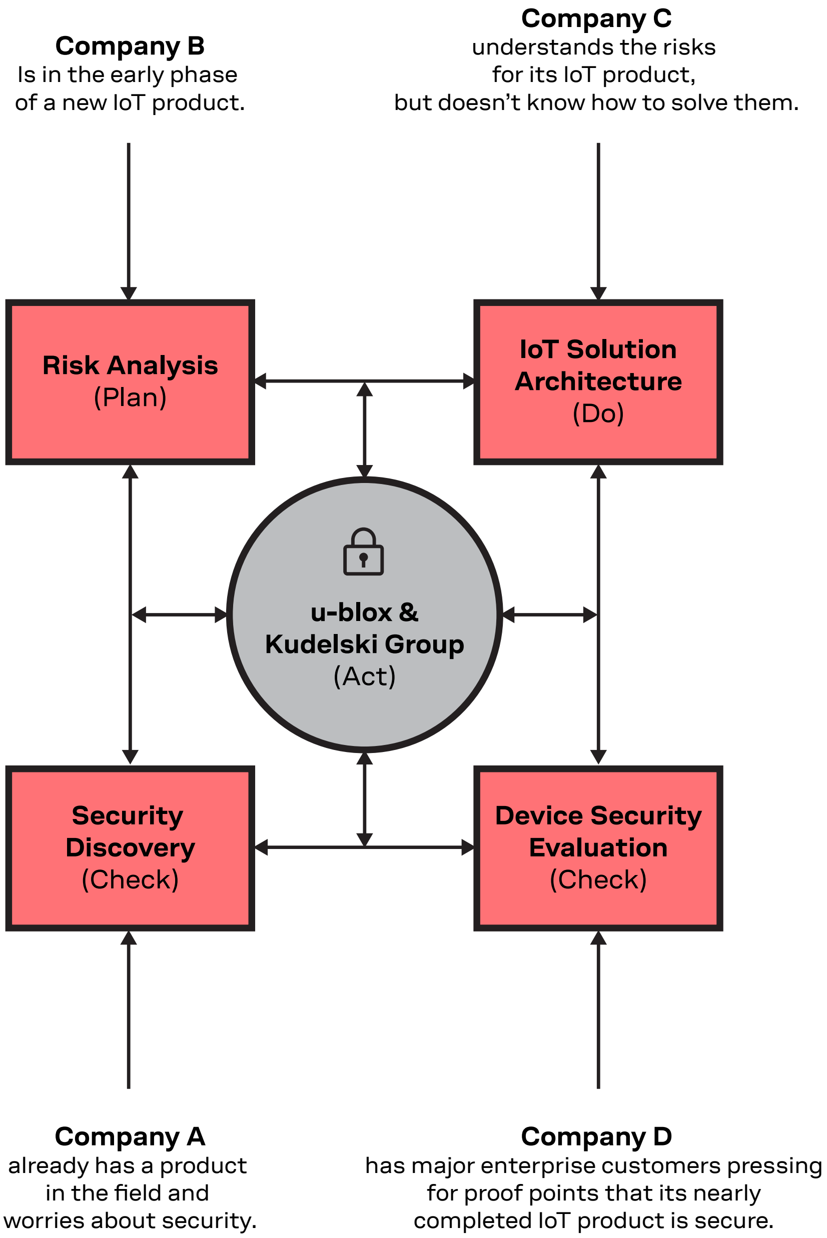
Organizations that are deploying IoT ecosystems must remain vigilant to evolving threats. This is done by using traditional cybersecurity methods as well as by receiving security telemetry from devices. Organizations can struggle to collect, index, evaluate, and process all the security intelligence data that is generated internally and gathered from external sources. But only when this is done effectively is it possible to have meaningful, actionable intelligence that reduces the time it takes to detect and remediate any threats. If this monitoring is done properly, exposure to cyber-risks is reduced and security investments are optimized.

The ongoing work of IoT threat intelligence and analysis relies on capabilities that most organizations do not possess in-house, so it is advisable to work with a trusted partner that provides managed security services to protect against evolving threats.

5 THE JOURNEY: Plan, Do, Check, Act

u-blox and Kudelski have the expert security analysis, advice, and design services needed to launch secure and safe IoT products and ecosystems. They are key to the PDCA workflow that underpins your security assurance program.

The PDCA workflow can be entered at any point, both in the planning stages for a new product as well as for products that are already in market. We can help you wherever you might find yourself in the development process.



Company B
Is in the early phase
of a new IoT product.

Company C
understands the risks
for its IoT product,
but doesn't know how to solve them.

Risk Analysis
(Plan)

IoT Solution Architecture
(Do)

u-blox & Kudelski Group
(Act)

Security Discovery
(Check)

Device Security Evaluation
(Check)

Company A
already has a product
in the field and
worries about security.

Company D
has major enterprise customers pressing
for proof points that its nearly
completed IoT product is secure.

Figure 3: The IoT Security Lab journey

5.1 IoT Security Lab

u-blox and Kudelski offers a security evaluation and consulting service, called the IoT Security Lab, which provides a tailored vulnerability and threat analysis to assess and evaluate chip-level security, PCB-level security, and software security, followed by end-to-end security architecture consulting and testing before releasing products to market. This enables customers to save time and cost, while benefiting from proven security knowledge and expertise.

Step	Coverage	Benefits	Usual duration (in staff days)
Plan: Threat assessment	**System- and device-wide risk analysis with STRIDE.** Identification of threat scenarios, the likelihood of successful attacks and their business impact.	• Identification of risks linked to processes, lifecycle, and system design that have an impact on business • Establishment of a baseline for future security evaluations	15
Do: IoT solution architecture	**Design of an IoT solution security architecture,** taking into account the outcome of the threat assessment and the capabilities of the u-blox products with the Kudelski IoT Security Platform.	• System-wide security architecture that takes the identified risks into account • All the features and capabilities of u-blox products with the Kudelski IoT Security Platform	20
Check: Device Security Discovery	**Device penetration testing** performed by security experts.	• High-level understanding of a device's security policy	15
Check: Device Security Evaluation	**Evaluation of the security implementation** based on the outcome of the threat assessment or an agreed target of evaluation.	• Identification of the most important gaps in the security of the device • Focus on the most important assets for the client's business	35
Act: Kudelski + u-blox	**Commercial production of secure IoT devices,** using u-blox products and the Kudelski IoT Security Platform. **Security lifecycle management** using Managed Security Services from Kudelski.	• Built-in Root of Trust, secure boot, secure updates, and an IoT Security Platform with key management • Monitor your IoT ecosystem and respond to security incidents	Not applicable

5.2 IoT Security Platform

The Kudelski IoT Security Platform implemented in u-blox products creates a chain of trust, integrity, and control that links devices, data, IoT platforms, and applications. It enables users to manage and control all key IoT security assets with simple APIs.

It provides pre-integrated components that bring features necessary to implement secure device designs and secure data for internet-connected applications. It enables fine-grained access management to the device data and functionality.

5.2.1 How the IoT Security Platform works

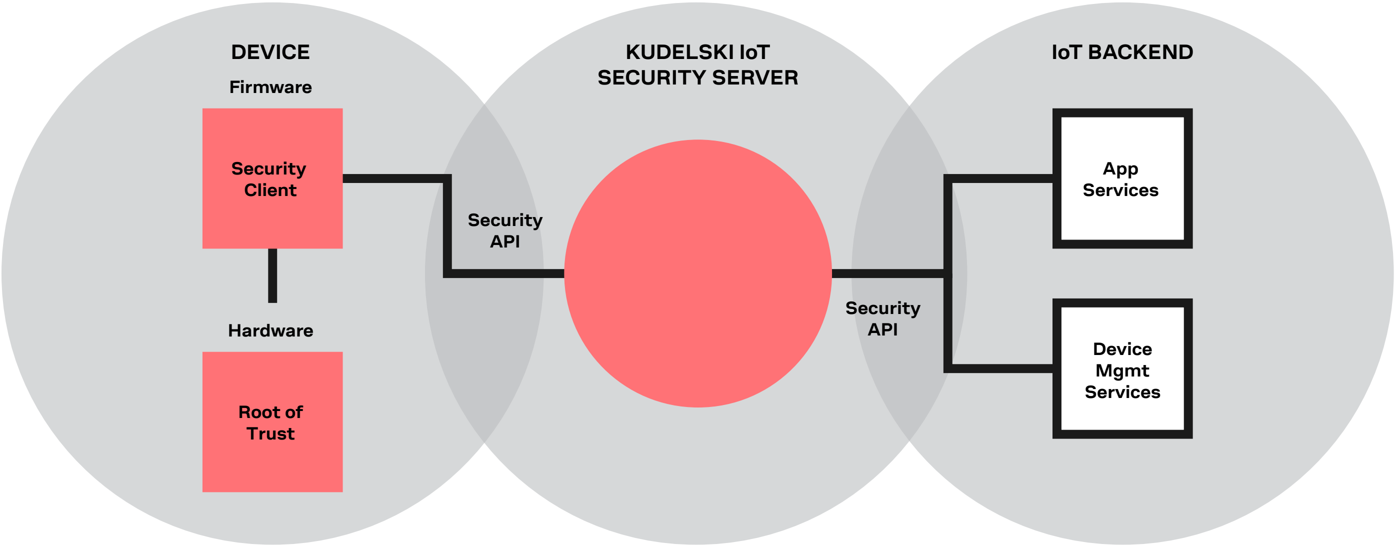


Figure 4: The IoT Security Platform

The platform consists of three main elements: a software- or hardware-based RoT, a security client in the device, and a security server in the cloud or on the customer premises. The client and server are easily integrated with devices, back-end platforms and applications using simple APIs.

Communications between an IoT device and security server are protected as follows:

- A RoT embedded in the device acts as the foundation for all security use cases. It is personalized and provisioned when the component hosting the IoT device's security functionality is manufactured.
- u-blox/Kudelski supports three types of RoT: a secure element (chip), a SIM, and a software RoT within a trusted execution environment. An integrated secure enclave, designed by Kudelski, can also be embedded into chip designs.
- A security client library is integrated with the device firmware and applications, so the customer can take advantage of all security functions.

Communications between the security server and an IoT back-end are protected as follows:

- The security server connects to the customer's back-end platform to enable secure features offered by any authorized application.
- The server provides trusted data to the customer's back-end platform. The data sent between the device and the cloud is identified, authenticated, and traceable. Device and server APIs enable encryption and authentication, and manage all IoT business logic.
- Once the platform devices can be identified and managed, data can be transferred and stored securely, and device functions can be enabled and enforced throughout the entire lifetime of the device. The platform integrates active security features to ensure that devices can be managed when new business opportunities are defined or when new security threats appear.

This enables users of the IoT Security Platform to create and operate a wide variety of digital and physical assets, both now and in the face of evolving threats.

About the authors

Eric Heiser, Head of Services/Security, u-blox

Eric Heiser joined the Product Center Cellular at u-blox AG in 2016 as Head of Strategic Partnerships for the Americas. In 2018 he transitioned to lead u-blox's Services & Security business activities. Prior to this, Eric was Division Vice President & GM, Strategic Sales & Corporate Planning at Kyocera Communications Inc for eight years.

Eric Heiser holds an MBA from Marriott School of Business, BYU and a B.S. in Electrical Engineering from University of Missouri, Rolla.

Conor Ryan, Vice President IoT Chipset Strategy, Kudelski Group

Conor Ryan joined Kudelski Group in 2003 and has held various key positions in marketing and product management, mostly in the Group's pay-TV business. In early 2017, he was instrumental in ramping up Kudelski's IoT security activities, including the opening of the IoT Security Lab.
His current responsibility is managing strategic hardware partnerships for the Kudelski Group's IoT Security Platform.

Conor Ryan was educated in Trinity College Dublin, BA, BAI, MSc in 1989. He has a wealth of experience in embedded software and silicon (Siemens, S3 Group, Parthus-Ceva) in different roles, including development and product marketing.

About u-blox

u-blox (SIX:UBXN) is a global provider of leading positioning and wireless communication technologies for the automotive, industrial and consumer markets. Its solutions let people, vehicles and machines determine their precise position and communicate wirelessly over cellular and short-range networks.

With a broad portfolio of chips and modules, and a growing ecosystem of product supporting data services, u-blox is uniquely positioned to empower its customers to develop innovative solutions for the Internet of Things, quickly and cost-effectively.

With headquarters in Thalwil, Switzerland, the company is globally present with offices in Europe, Asia and the USA.

About Kudelski

The Kudelski Group (SIX:KUD.S) is a world leader in digital security and a provider of end-to-end convergent media solutions to the digital entertainment industry, including services and applications requiring access control and rights management to secure the revenue in digital television, internet, mobile and interactive applications.
The Group also offers cybersecurity solutions and services focused on helping companies assess risks and vulnerabilities and protect their data and systems. It also supplies integrated solutions to manage access control of people and vehicles to sites and events. The Kudelski Group is headquartered in Cheseaux-sur-Lausanne, Switzerland and Phoenix (AZ), USA. For more information, please visit www.kudelski-iot.com.

u-blox or third parties may hold intellectual property rights in the products, names, logos and designs included in this document. Copying, reproduction, modification or disclosure to third parties of this document or any part thereof is only permitted with the express written permission of u-blox.

The information contained herein is provided “as is” and u-blox assumes no liability for its use. No warranty, either express or implied, is given, including but not limited to, with respect to the accuracy, correctness, reliability and fitness for a particular purpose of the information. This document may be revised by u-blox at any time without notice. For the most recent documents, visit www.u-blox.com.

u-blox AG
Zuercherstrasse 68
8800 Thalwil
Switzerland

www.u-blox.com