KUDELSKI IOT THINGS

Introduction to IoT Security

for IoT device & component manufacturers

101

DEFINITION

What is the Internet of Things?

At its very simplest, the Internet of Things (IoT) is the process of connecting physical things to the internet. These things (sensors, actuators and machines) are then connected to IoT applications on company servers or in the cloud. "Things" must also be given a digital identity that allows them to be identified, authenticated and controlled. Once connected:

- The device collects and sends data to the cloud that is then used by the applications to gain new insights and make smarter decisions (e.g. predictive maintenance of factory equipment, medical data from patients, etc.).
- The server sends commands and data back to the devices and updates devices (e.g. a power plant changes the way electricity is distributed throughout the grid, or an automobile manufacturer sends a software update to a car).
- The devices perform actions based on local or cloud-based decisions, increasingly involving Artificial Intelligence - to speed the process (e.g. a car automatically applies the breaks when its AI detects a child-shaped obstacle, or a door at a remote facility locks when the central server detects all employees have left the building).

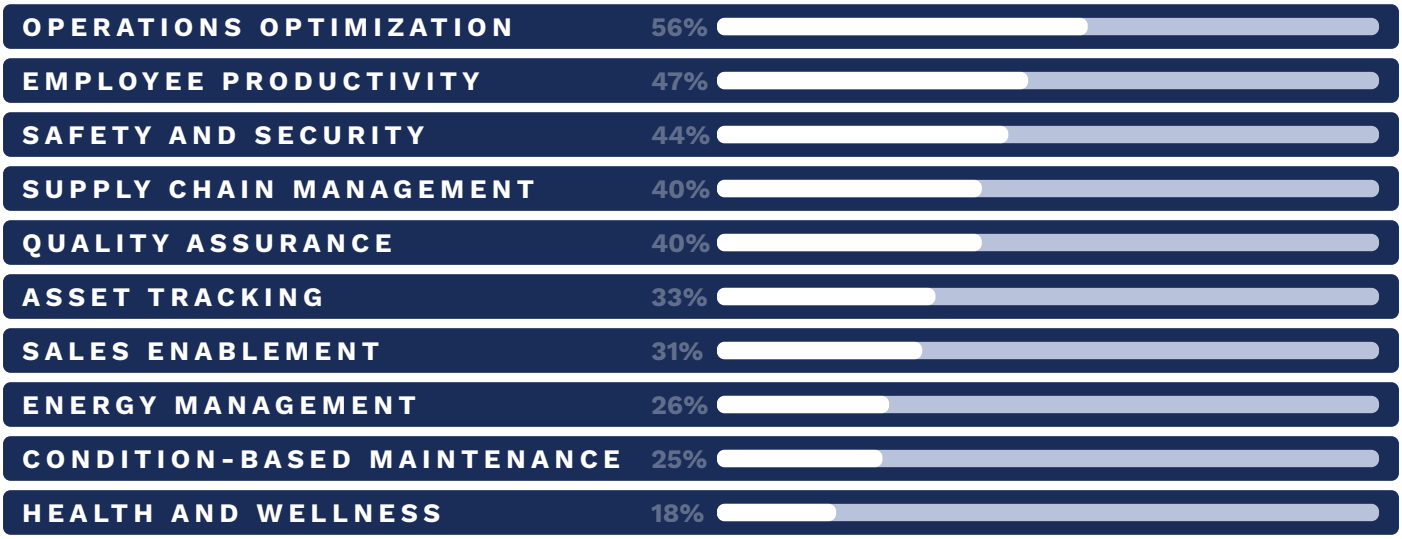
Connectivity does not always have to happen through the internet. A thing such as a wind turbine may be connected to a data center directly through a leased line, but the turbine is still a connected thing. In addition, some things aren't connected directly to the internet, but rather to a local gateway, which collects and processes data before sending it on to the cloud.

TRENDS

Why are companies investing in IoT?

Industrial equipment and medical device manufacturers, utility companies, auto makers, telco's, consumer electronics manufacturers and many others are connecting their devices to generate a sustainable and profitable return on investment.

2019 research from Microsoft based on 3000 interviews with IoT companies shows that these are the biggest reasons for IoT adoption:



*2019 Microsoft Azure: https://azure.microsoft.com/en-us/iot/signals/

APPLICATIONS

Real-world IoT use cases

There are dozens (if not hundreds) of IoT use cases that could be mentioned, but here is an example of one that generates cost savings through trusted data, and another one that transforms an entire business model by ensuring the integrity of its associated data:

USE CASE 1

Ensuring food is fresh when it arrives to the supermarket

A supermarket chain is receiving produce that appears fresh on arrival but wilts after a few days, making customers unhappy and reducing sales. Supermarkets do not know whether to blame the producer, the distributor or the trucking company. Investigation shows that the trucking company is turning off the refrigeration unit on the truck in order to save fuel costs and turning it back on again prior to delivery so the food appears cold and fresh.

The supermarket chain implements connected temperature trackers on every palate starting at the farm, and now gets complete visibility of the product's temperature and location from farm to supermarket. This improves the quality of their products, allows quick resolution of real refrigeration problems and saves hundreds of thousands of dollars on spoiled products, using data is completely trustworthy and cryptographically linked to the tag it came from, preventing disputes about the integrity of the data.

USE CASE 2

Transforming the airplane engine business by selling a service instead of a product

Rolls-Royce is no longer in the business of selling engines but of selling thrust. The engines send telemetry data to four centers, where every engine is under surveillance.

An inspection can be scheduled, or spare parts can be directed to the right destination, even before the pilots or the airline know that one of their engines has a problem.

By now, 80% of Rolls-Royce engines are sold at a loss which is recouped by an hourly fee paid under the TotalCare program.

This also makes it very hard for a third party to steal maintenance business from Rolls-Royce.

All maintenance cost is covered by the TotalCare fee which now accounts for more than half of Rolls-Royce's revenue.

The value of this data is therefore of vital business importance to Rolls-Royce, so it is critical that its integrity be guaranteed and that it is protected from theft.

KEY SUCCESS FACTOR

Many industries, many applications, one challenge

Nearly every industry has identified benefits of implementing IoT projects

Within each industry, there are many useful applications, some of which are unique (connected radiation sensors for nuclear power plants) and some of which are common across many industries (like video surveillance).

But regardless of the industry or application, security plays an important role in protecting and enabling each of those applications.

Something that is connected is - by definition - also exposed

IoT devices and their data often operate in uncontrolled environments like pubic buildings, public areas, homes, remote facilities, etc. This opens them up to threats from hackers, thieves, competition, hostile states and other enemy actors.

With connectivity, replicating an attack becomes much easier. This means that IoT solutions should never be implemented without considering the threats and the security implications, implementing the necessary measures to protect physical and digital IoT assets.

> Security isn't just about risk mitigation, it's also about opportunity creation

At the same time, IoT creates numerous opportunities

Security can support the implementation of new features and business models, so security isn't just about risk mitigation, it's also about opportunity creation. It's not just an insurance policy, it's a business enabler.

Bringing new functionalities that enable new models is just as important as the robustness of the security solution itself. Both are important and can be quantified and form an important part of the business case to justify IoT security investment to management.

OPPORTUNITIES

The benefits of Secure IoT

Organizations that invest in IoT need to have a full understanding of the risks and opportunities associated with connecting their devices. Once they understand this, they need to develop a strategy that protects their key business pillars, at design, at launch and throughout the entire lifecycle of the IoT device and ecosystem.

Customers invest in IoT security to achieve numerous benefits

- Enable new efficiencies and cost savings using device data that can be used to make important operational decisions because the devices and data that can be fully trusted.
- Enable monetization by accurately measuring product usage and materials consumption using data that all parties can trust and that can't be falsified.
- Enable new business models like rental instead of purchase (product as a service), pay-per-use, etc. using trusted data and the ability to securely control features.
- Enable/disable features so that companies can upsell them to their customers while ensuring payment and preventing fraud.
- Add security as a unique selling point for their product, enabling them to offer a valuable advantage to their customers that their competitors don't offer.
- Protect valuable intellectual property in IoT devices, ensuring that critical software, logic and AI are protected from tampering and theft using secure processing, secure storage, white box cryptography and advanced software obfuscation.

Customers also want to prevent key business risks

- Theft of potentially sensitive data, resulting in revenue loss and reputational harm
- Security exposure when formerly unconnected devices are connected for the first time
- Degradation of user experience and brand trust if the device is hacked
- Malware and Distributed Denial of Service (DDOS) attacks
- Bad data creating the wrong decisions (AI/Machine Learning)
- Bad AI decisions creating the wrong commands and actions
- Not being able to keep up with an evolving threat landscape

> In short, IoT implementers need IoT security to establish trust, integrity and control so they can achieve a sustainable return on their IoT investment.

KEY CONCEPT

Reactive monitoring

Vs.

Security by design

It is important to note that many companies have IoT devices already deployed that are not fundamentally secure by design.

This limits their ability to protect their ecosystem to methods traditionally used in the IT and cybersecurity domains.

This would include managed security services, network monitoring and firewalls that would prevent some intrusions but not fundamentally protect the device and its data.

When possible, "security by design" is a much better approach to ensure the long-term sustainability of any IoT ecosystem.

Security by design means the manufacturer designs in the fundamental components of good security (like, for instance, a root of trust) from the beginning of their product development lifecycle.

By doing this, they are well-prepared to protect everything that will need to be secured throughout the lifecycle of the device, enabling every secure IoT use case they may require.

Cybersecurity methods then become a valuable complementary approach to monitor and respond to evolving threats, but the foundations for defending the device and recovering from breaches are already in place.

SECURITY ARCHITECTURE

What needs to be secured?

With IoT, devices and cloud applications converge into one system with a dramatically increased attack surface

Organizations implementing IoT-based solutions rely on connectivity and are therefore inherently exposed. Ensuring that physical and digital assets are protected within an IoT system, starting with robust IoT security embedded in the device, will enable a strong chain of trust, integrity and control throughout the customer's entire IoT ecosystem and throughout its entire lifespan.

The following IoT assets must be properly secured:

IDENTITY

Identity of devices that produce data and execute commands must be unique and unclonable. This forms the basis for all other security functions.

DEVICES

Devices are the most exposed element of an IoT ecosystem. Often in uncontrolled environments, hackers can access unencrypted data, upload malware, conduct DDOS attacks and fraudulently access features they haven't paid for if the device isn't sufficiently protected. Device resources (CPU, memory, connectivity) must remain allocated only to their expected tasks.

DATA

Data (at rest or in motion) is privacy or confidentiality-sensitive, often subject to regulatory requirements - general (GDPR) and industry-specific (HIPAA), could be intercepted by competitors, must be trusted by AI engines, etc.

DECISIONS

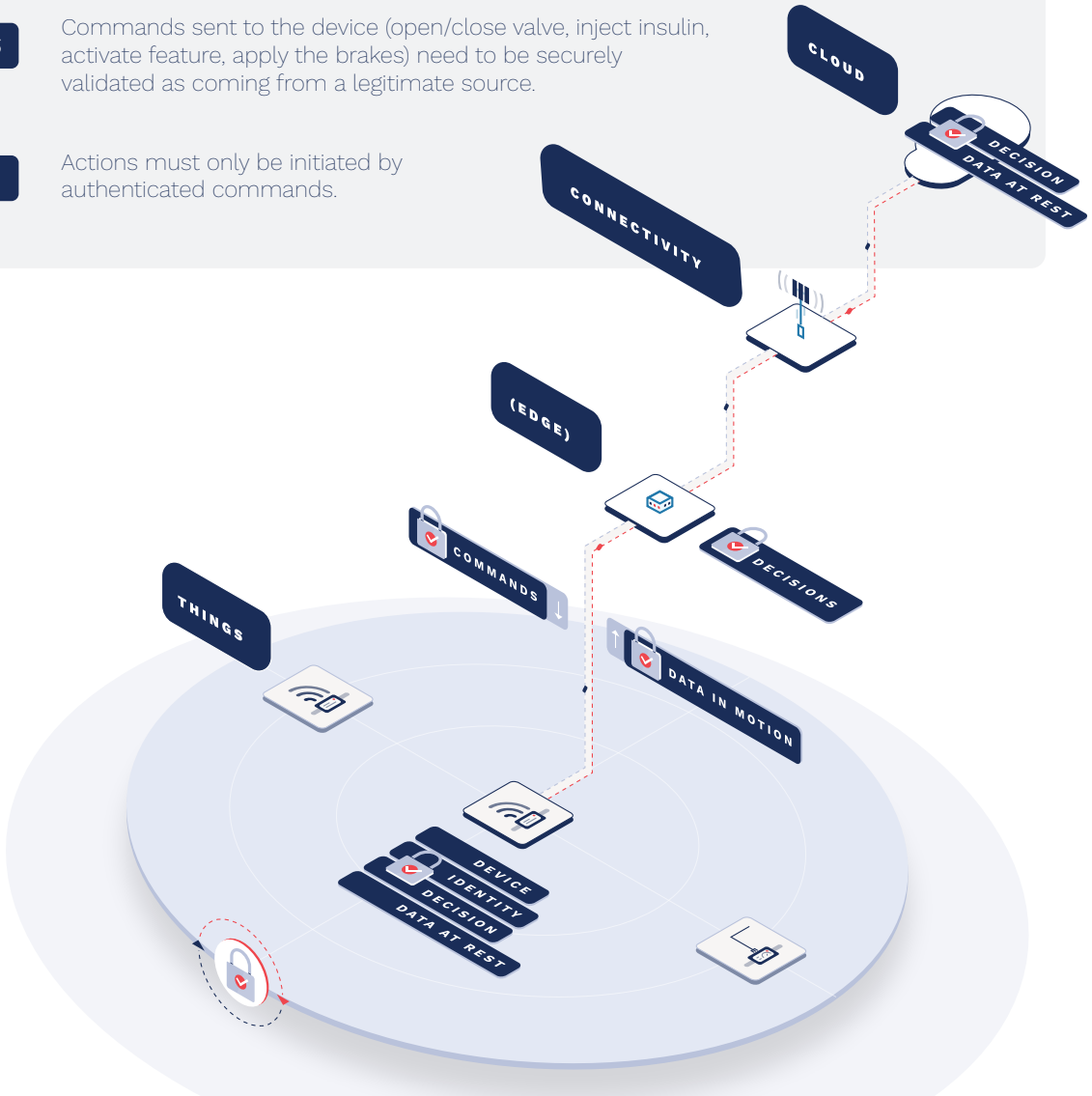
Decisions (whether simple logic or AI-based) should be executed in a secure environment so they are safe from tampering or from intellectual property theft of the AI logic, and must ensure the integrity of data input in order to ensure the validity of decisions taken (and the resulting commands and actions).

COMMANDS

Commands sent to the device (open/close valve, inject insulin, activate feature, apply the brakes) need to be securely validated as coming from a legitimate source.

ACTIONS

Actions must only be initiated by authenticated commands.



CHECKLIST

Top 5 IoT security best practices

With so much benefit to be achieved and so many risks to mitigate, where should you begin?

What are the key principles you should consider in your design process, technology choices and long-term strategies? Here are the five basic best practices to help you create secure IoT products and ecosystems:

1 Start with the end in mind

Start considering security as soon as you begin planning your IoT solution. It is far more economical and more effective to design security in from the start than adding it after a launched product has been breached (by a factor of 60 to 80 times, according to IBM).

Fully explore potential threat models while there is still time to implement controls to mitigate them.

Think carefully about the future and new functionalities or business models that might require more robust security than your initial product launch.

2 Build on secure foundations

Establish a root of trust (unique, secure identity protected inside a chip or hardened software) in the device at manufacture. That simplifies device onboarding and management and establishes the robust security tools you need to secure all current and future IoT use cases and applications.

This root of trust may be integrated into other components you're already using, like System on a Chip (SOC), MCUs (Microcontroller Units), SIM cards (including eSIM/eUICC and iSIM/iUICC) and cellular modules.

3 Protect everything

Use that root of trust and to enable protection of all your key IoT assets. Enabling things like end-to-end data encryption, command authentication, secure boot, fine-grained data access control, data integrity checks, remote feature activation/deactivation and many others.

Make sure your security solution supports all the features and functionalities you need both today as well as those you might need in the future.

4 Think long term

Consider the entire lifecycle of your IoT solution, implementing technologies that include FOTA (Firmware Over the Air) updates, countermeasures (built-in defenses), security telemetry from the device and managed security services to ensure long-term return on investment.

Hackers are constantly evolving their techniques, so work with an expert who is experienced in defending their technology and your business from sustained attacks.

5 Don't go at it alone

If you don't have security staff in house, find a proven expert who will accompany you throughout your entire IoT journey and will help you design, build, operate and sustain your IoT ecosystem long term.

Third-party, expert evaluations of your product can help you close potentially dangerous security gaps while building confidence with your buyers and giving you a strategic advantage over your competition.

OUR APPROACH

Security is our DNA

The Kudelski Group's 30 years of real-life experience in deploying and protecting connected, embedded systems is what makes it unique in the IoT industry.

The Group's security technologies and services have been widely deployed in real-life situations where billions of dollars in revenue and corporate reputation are at stake every day. We have earned the trust of our customers and have become their long-term, strategic security partners.

To achieve this level of trust, we have developed a long history of excellence in material invention, industrialization, deployment and management of robust security solutions.

We have been building and perfecting our hardware and software encryption technologies for decades, protecting devices, data, video and managing access to content and customer data.

The Group also supplies integrated solutions to manage access control of people and vehicles to sites and events.

Kudelski is also active in the cybersecurity market, offering advisory and managed security services, among others.

Over 400 million Kudelski-protected devices have been deployed.

> This combination of technologies and experience give the Group a unique perspective on IoT by combining both embedded security, smart building and cybersecurity knowledge – something very few solution providers can offer.

Long-term end-to-end partnership

By leveraging its unique heritage in both pay TV and cybersecurity, the Kudelski Group provides companies with design, implementation and long-term security lifecycle management of their connected business models across a variety of industries.

Kudelski addresses security from a system, end-to-end perspective, protecting all aspects of the connected business' ecosystem, its devices, collected data, intellectual property and associated monetization models.

The approach also incorporates Security Lifecycle Management that ensures that security is sustained throughout the lifetime of the ecosystem.

Solutions for your IoT security journey

The technology and methods required to implement IoT security are often beyond the capacities of most organizations to implement effectively on their own.

We bring a unique expertise that is directly transferrable to the IoT market by adding value to customers at every stage of IoT security journey, from design through end of life, and are a strategic security partner for the entire lifecycle of our customers' products and services.

It is that "cradle to grave" approach where we help customers through every stage of their IoT journey that truly distinguishes us from our competition.

> Two of the most important aspects to long-term IoT success are designing security into products and ecosystems from the start, as well as managing the product's long-term security lifecycle. Kudelski is a leading cybersecurity company that can do both.
>
> Michela Menting, Research Director
>
> ABIresearch®

$100B/yr	400M+	11,000	32	$716M
revenue protected	devices secured	clients	offices worldwide	revenues (2022)

Visit our website at www.kudelski-iot.com or write info@kudelski-iot.com for more info.