neXus

Guide

How to build a secure IoT infrastructure

- 5 pillars for state-of-the-art security for the internet of things

How to build a secure IoT infrastructure

Executive summary

The internet of things (IoT) is booming, with more than 20 billion connected devices expected worldwide by 2020. Whether the purpose is to remotely control smart home devices, to manage communication between cars, or to monitor the street lights of a city, security cannot be overlooked.

This guide explains why security is vital to consider for any IoT application, and suggests these five pillars for a well-founded security design:

Pillar 1: Define your needs
Do you need to protect confidential data? For how long? Do you need to verify the source of the information? Have you thought of all parts of your IoT architecture, to make sure you don't leave any loopholes?

Pillar 2: Team up
Since IoT security is a truly complex area, you need to find a trusted and experienced partner early in the process to help you select the right implementation.

Pillar 3: Take advantage of available technologies
Don't reinvent the wheel. As much as you can, build on tried and tested industry standards and open-source technologies.

Pillar 4: Ensure scalability and flexibility
Scalability is an inherent need in IoT since applications typically involve large numbers of things, and businesses grow quickly. Make sure that the security system can grow with your business.

Pillar 5: Take account of industry demands
While the IoT area as a whole is still unregulated and lacks common standards, there are very specific technical and policy requirements within certain areas, such as connected cars and eHealth. You must take these and applicable legal regulations into account.

Why security is crucial in IoT solutions

The IoT landscape brings unique and complex challenges in the areas of safety, security and privacy. If your service goes down or your IoT device stops functioning due to a cyberattack, or if user data is stolen, it can cause financial damage or evoke ill will or lost confidence from customers. If your IoT devices start functioning in an unexpected way due to hacked software, material damage can occur and human safety may be in danger.

So, let's look at the specific security considerations to bear in mind with IoT applications:

IoT devices are easily accessible
The complex ecosystem of IoT includes a multitude of devices, networks, interfaces, cloud services, and people.
"Many IoT devices are easily accessible, either physically or over networks. A potential attacker has the opportunity to examine a device and find out which vulnerabilities it has. And, due to the connected nature of IoT devices, if you break into one device, you have a good chance to access many devices and a lot of information," says Tina Lindgren, information security consultant at Combitech and PhD in information theory.

Business secrets and privacy is at risk
The gold of the internet age is data. An IoT device may expose business-relevant and private data by simply transferring it to a cloud service or to other devices. Such data may be eavesdropped on the internet or collected by other businesses, intelligence agencies, or criminal parties. Big data from many devices over time can be analyzed to derive business secrets and behavioral patterns or preferences of users, which can be commercialized or used in other ways.

Material and human safety is at risk
Since IoT involves not only information systems, but also actuators that act in the physical world, security threats can also become safety threats.

"Earlier, the worst thing that could happen was that someone would steal data, but now safety is also concerned. If someone hacks my computer, they can't physically harm me, only steal my data. But if someone hacks my car, my personal safety could be in danger," says Shahid Raza, director and cybersecurity researcher of the Security Lab at RISE SICS.

In 2015, the security experts Charlie Miller and Chris Valasek at the Pentagon's Defense Advanced Research Projects Agency (DARPA) showed how they could remotely stop a car and disable its brakes [1]. This and similar examples show how hackers could cause real danger to material and lives.

IoT devices have limited resources and often lack security
Sensors and similar small IoT devices often have limited capabilities for processing, memory, and power. For such small products that are sold in large numbers and for a low price, security has often been overlooked. These constrained devices offer an easy target for hackers.

This was shown in the Mirai cyberattacks in 2016, where small devices such as web cameras were used as part of a botnet used in distributed denial of service (DDoS) attacks [2].

Resource-efficient lightweight cryptographic methods, security protocols, and techniques are available to mitigate the risk of cyberattacks.

It's costly and difficult to add security later
Consider the security aspects from the start. 'Security by design' is the principle here, rather than trying to add security later to a large number of insecure devices that might be installed in various locations.

"It's often considerably more costly to amend an existing product than it is to implement security features during the design process," says Tina Lindgren in the IoT guide [3].

Now that you know how important security is for IoT, how can you go on to implement it? If you build your security around the following pillars, you will have a much clearer picture of how to proceed towards an appropriate, yet affordable, IoT security architecture.

Pillar 1: Define your needs

Since IoT includes all use cases that involve things connected to the internet, the associated risks vary a lot. You must find out what your biggest threats are, and where you have possible loopholes that hackers can take advantage of.

Be aware of the risks
Do a risk assessment to find out where your biggest risks are. Use any relevant common standards, such as ISO 27001, to assess and counteract on cyberthreats. Do regular revisions as new threats may arise.

Since internet connectivity is part of the definition of IoT, there is an inherent interface with the outside world. You must assess what type of information is captured, processed and transferred by your IoT devices and your IoT cloud applications, and what the consequences are of eavesdropping, data manipulation or loss. What happens if an unauthorized person accesses your device or if manipulated software is executed by it? What happens if hacked devices or malicious software deliver manipulated or forged data to your cloud services?

The risks and their consequences must be balanced against the added value of collecting data, as well as any specific requirements on how accessible your service needs to be and how simple it must be to use.

"To create a successful solution, you must start with how the customer will benefit. You can connect all kinds of things all over the world and make them communicate, but what is the added value?" says Ulrika H. Westergren, associate professor of Informatics at Umeå University, and author of the IoT guide [3].

Limiting the functionality to the really valuable parts, reduces risks and makes security easier to put in place.

What do you need to protect and for how long?
Depending on what you need to protect – storing or transferring data, activating a physical function of a device, or accessing a function of a cloud service – different security mechanisms are needed. If the purpose is to keep data secret, it can be encrypted, whereas digital signatures can be used to prove the origin of data and guarantee its integrity. Access to functions is typically protected by means of authentication from the accessing party.

Depending on the lifecycle of your product or data, different measures may be suitable.

"If you only need to protect something for a couple of days, for example a message on who will win the Oscars, the scenario is different than if you want to protect something for many years, such as intellectual property. The encryption algorithm and the length of the keys should be chosen considering the specific scenario," says Tina Lindgren.

Make sure to secure all parts of the IoT solution
The European Union Agency for Network and Information Security (ENISA) has defined these four layers of an IoT infrastructure [6]:

- Devices – such as sensors and actuators.
- Communications – such as PAN, LAN, gateways.
- Cloud platform, backend, and services – such as databases, process automation, and decision systems.
- Use cases – such as transport, healthcare, and smart homes.

For best possible end-to-end security, all these layers need to be protected.

"Some sensor vendors say that they offer security, but actually they only protect the IoT gateway, and not the devices themselves. That way, if someone hacks into one device they can get to all the devices," says Shahid Raza.

Consider all the included parts of your solution, to make sure you don't leave any security holes.

Pillar 2: Team up

IoT security is a complex area. It needs expertise and experience to overview risks and consequences, and to define how to mitigate them. The environment is constantly changing, as new types of operating systems, communication protocols, and cyberattacks are developed. For these reasons, it is crucial to find an established partner to advise you.

Find an experienced advisor

A security expert with a solid background is likely to have come upon issues that are relevant to your use cases, for example they may have experience providing security for large IT deployments or to organizations in the same industry. Many issues can be addressed the same way, even across industries.

”Every business thinks that they are unique. But when you look at it, you find that organizations usually have to solve the same issues. What is the customer benefit? What shall we measure and when? Who has access to the data? Who owns the data? How shall we store the data?” says Ulrika H. Westergren.

Trusting the vendor is key

If you don’t have the competence inhouse on how to secure your IoT application, then it may also seem hard to evaluate and choose a partner. Lack of standards in the IoT area makes it even harder. So, how can you go about choosing a vendor for IoT security?

”Companies need to get help from experts, who are already established, clear on what they can offer, and trustworthy. Use your connections to find if someone has helped others with similar issues,” says Ulrika H. Westergren.

Focus on your core business

Taking advantage of the competence and experience of your security advisors lets you focus on your core business and develop innovative and highly usable services to your customers.

Look for a security vendor that offers a solution that is easy to use, deploy, and operate. Preferably, you get a choice between operating a solution on-premises or consuming it as a cloud service, whichever fits you best.

Pillar 3: Take advantage of available technologies

There are many available technologies for security that can be applicable to you, so there is no need to reinvent the wheel.

Trusted identities with PKI
All connected IoT devices and services must have trusted digital identities to be able to distinguish them from each other and from unauthorized or malicious parties trying to intrude on or disrupt your devices and services. This is sometimes referred to as the identity of things (IDoT). Digital identities are the basis for security services; they enable encrypted communication, verification of the origin of data, and guaranteed integrity of data and software being stored, transferred, or executed.

Public-key infrastructure (PKI) certificates provide cryptographically secure, unforgeable, theft-safe identities, which enable devices and services to be empowered with:

- Authentication: Strong authentication ensures that only approved users and devices can connect to the network.

- Encryption: Certificates enable encrypted communication between devices and services.

- Integrity protection: Digital signatures prove the origin and integrity of data and software.

PKI is a mature and well-standardized technology, so you can choose from a large pool of software vendors, open-source implementations, service providers, and system integrators [4]. All these can provide you the same core technology, so that you are safe from being locked into a solution.

Strong authentication
Since IoT means that services and devices are connected with the internet, it is especially important to prevent unauthorized persons from accessing the systems, devices, and cloud services.

Passwords are proven to be insecure. For example, according to the 2017 Data Breach Investigations Report by Verizon, 81% of hacking-related breaches leveraged stolen or weak passwords. With strong, cryptography-based authentication, you make it much harder for the attackers. For persons that need to access devices or services, apply two-factor authentication (2FA). In addition to the strength of the method, consider how the keys are created, distributed, and stored. Unsecure management spoils the security of even the strongest cryptographic method.

Also, look for simplicity in your authentication solutions. For example, a mobile app using biometric factors is both user-friendly and secure. If the security solutions are hard to use, then people find ways around them.

Use industry standards and open source
Apart from the aforementioned methods, here are some other examples of available technologies that fit well into IoT applications:

- Constrained Application Protocol (CoAP): Web transfer protocol for use with constrained devices in and narrow-band connection to the internet.

- Message Queuing Telemetry Transport (MQTT): Messaging protocol that provides resource-constrained network clients with a simple way to distribute telemetry information.

- Transport Layer Security (TLS): Cryptographic protocol for secure communication security over reliable communication channels. It is the most common means for securing client-server data transfer on the internet, such as communication between a browser and a web application.

- Datagram Transport Layer Security (DTLS): Cryptographic protocol for secure communication over unreliable communication channels.

- Enrollment over Secure Transport (EST): Certificate enrollment protocol for issuing certificates to resource-constrained things.

Pillar 4: Ensure scalability and flexibility

IoT has only just begun, and the number of connected devices is constantly increasing. Devices must be possible to manage in an efficient way, no matter if they are 100 or 1,000,000. Scalability is a prerequisite for IoT. So, you need to make sure that your security solution also scales.

IoT devices are often limited in resources, such as processing power and communication bandwidth. For end-to-end security, these devices must also be secured, using suitable lightweight cryptographic functions and security protocols.

PKI is scalable

Symmetric cryptography is typically used to secure point-to-point communication. For this, the same secret key is used by both communicating parties for example to encrypt and decrypt information. This works fine for low-scale IoT applications. Keys must be preshared for every single connection between devices or services. Key management in this form is clearly not scalable to millions of devices.

Asymmetric cryptography, which is employed in PKI, uses a private and a public key. Only the public key needs to be known by the relying other party. Key distribution is easier, because the public key can be transferred via a non-encrypted, public channel. This works better for large systems.

PKI adds a twist to asymmetric cryptography: it works with digital certificates, containing the public key, the identity of the key owner – a device, service, or user – and the digital signature of the issuing certificate authority (CA) to verify the integrity of the certificate content. Using a hierarchy of CAs, PKI allows a relying party to trust certificates of all other parties.

"When the system scales, let's say to more than 100 devices, you need asymmetric encryption to be able to handle key management. Then certificates are issued as you go. This system scales easily when new devices are added," says Shahid Raza.

For scalability, the processes of issuing and distributing certificates must be automated. A CA solution must provide such automated processes and corresponding interfaces.

High performance needs?

As your IoT application grows, consider what requirements there will be on the performance of the PKI, that is, how many certificates you will need to issue.

In many applications, PKI performance is not an issue. Devices may receive life-long certificates and there may be no reason to revoke them. In other applications, revocation may be useful to block unauthorized use of lost devices. Further security measures may limit the validity of certificates and require them to be renewed frequently, or even require ephemeral certificates that are only valid for one transaction.

An interesting application of certificates is in vehicle-to-vehicle (V2V) or vehicle-to -everything (V2X, Car2X) communication. To guarantee the privacy of the driver, each vehicle gets 50–100 pseudonym certificates for every week, which are randomly used throughout the week. After a week, a new set of certificates is delivered by the CA. This process requires an extremely high-performing PKI platform, especially when delivering to millions of cars.

Secure over-the-air updates

When vulnerabilities are found in software, it must be possible to upgrade the software or firmware on the devices. Secure, remote, so called over-the-air (OTA) updates are needed at scale.

"Make sure that devices can be updated, so that you don't get stuck with an unpatched or old operating systems. Remote updates should be considered, since it would be costly to collect all devices to update them. For a remote update, it is important to be sure of the source of the update," says Tina Lindgren.

harmful code, the update files should be signed by a trusted authority. To protect against eavesdropping and reverse engineering, the software updates should be encrypted during transfer to the device. Decryption and validation keys must be installed in the device during production or commissioning, as part of the security solution.

Connecting a variety of devices in a secure way
All devices in your IoT network must be secure, to achieve good end-to-end security.

Many IoT devices are battery-powered and have limited processing and communication capabilities. Therefore, choose a security solution that is flexible and supports also these constrained devices, for example by using lightweight cryptography and specially tailored protocols, such as CoAP and DTLS for communication, and EST for certificate enrolment.

Pillar 5: Take account of industry demands

The IoT area in general is still unregulated and without common standards and common security, safety, and privacy polices. There are, however, very specific requirements and regulations within certain areas, such as connected cars and eHealth. More standardizations and regulation will certainly follow in many other areas [5, 6].

Example: Security in connected cars

The Car2X use case raises many specific requirements. As shown, a high-performing PKI platform is one of them. Other requirements are more efficient ways to generate keys using butterfly elliptic curve cryptography, a redundant setup of two certificate authorities (CAs) to guarantee drivers' privacy, and high availability to reliably function at all times.

There are technical standards to describe these requirements, such as IEEE1609.2 in the US [7], and ETSI TS 102 941 and TS 103 097 in the EU [8].

Consider data privacy

For privacy of data, consider all international and national regulations that might apply. Since the Global Data Protection Regulation (GDPR) went into effect in May 2018, it is still not clear how it will apply to IoT.

"IoT devices often contain some personal data. But, there is no interface by which to give your consent, for example, when you use your lawn mower," says Shahid Raza.

Besides personal data, unsecure IoT devices may expose behavioral patterns such as the movement profile or home absence of the owners, or deliver audio and video streams from the private environment.

Stay aware of legal issues

There are many legal issues that are still uncertain. For example, regarding who owns the data collected by an IoT device.

"Who owns the data is a giant question. Today, we see the whole spectrum out there, from companies who claim absolute ownership of data, to those who gives anyone access to it. There is no generic advice to give, only to stay aware of this issue," says Ulrika H. Westergren.

Another question is who is responsible and liable, when something goes wrong.

"What if someone turns off my IoT-enabled thermostat in the middle of the night and it is -30 degrees outside? This cybersecurity hack can become a serious safety issue. Who can be held responsible?" says Shahid Raza.

Since there are no easy answers to these questions today, the best you can do is to try to stay aware.

Conclusion

IoT comes with apparent safety, privacy and business risks. Therefore, security considerations and a suitable implementation are crucial for IoT applications.

Stay aware of the risks, and define what you need to protect and for how long. Design your IoT infrastructure for security and privacy from the start. Rely on trusted and experienced IT security professionals to help you. Use available technologies such as PKI and strong authentication to ensure security, as well as efficiency, scalability, standardization, and usability. Make sure to follow any specific requirements on performance, protocols and policies for your industry, while being aware of general privacy and legal demands.

As complex as it may appear, if you build on the pillars in this guide, you get a good start to defining your specific needs and your way of securing your IoT application.

Further reading

[1] Hack of connected car raises alarm over driver safety, in USA Today: https://eu.usatoday.com/story/tech/2015/07/21/hack-connected-car-raises-alarm-over-driver-safety/30462317/

[2] Mirai (malware) article on wikipedia: https://en.wikipedia.org/wiki/Mirai_(malware)

[3] IoT Guide http://www.iotguiden.se/#english-version by Ulrika H., Westergren, Ted Saarikko, and Tomas Blomquist at Umeå University, in cooperation with IoT Sweden, https://iotsweden.se/

[4] PKI Is Gearing Up for the Internet of Things, Gartner: https://www.gartner.com/doc/3426421/pki-gearing-internet-things

[5] Cybersecurity IoT program, National Institute of Standards and Technology (NIST): https://www.nist.gov/programs-projects/nist-cybersecurity-iot-program

[6] IoT and smart infrastructures, European Union Agency for Network and Information Security (ENISA): https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures

[7] Standard for Wireless Access in Vehicular Environments (WAVE), Institute of Electrical and Electronics Engineers (IEEE): https://standards.ieee.org/findstds/standard/1609.2-2016.html

[8] Intelligent transport system security, European Telecommunications Standards Institute (ETSI): https://portal.etsi.org/services/centrefortestinginteroperability/activities/intelligenttransportsystem/security.aspx

About Nexus Group

Swedish-owned Nexus Group is an innovative and rapidly growing identity and security company. It secures society by enabling trusted identities for people and things in the physical and digital world. Most of its technology is integrated into the Nexus Smart ID solution, which provides standardized and easy-to-use modules that enable organizations to issue and manage physical and digital IDs, manage physical and digital access, enable electronic signatures, and issue and manage public key infrastructure (PKI) certificates. The Smart ID solution is most commonly used for corporate IDs, citizen IDs, and IoT (internet of things) security. Nexus has 300 employees across 17 offices in Europe, India and the US, as well as a global partner network.

neXus | Enabling trusted identities

Contact us:
E-mail: contact@nexusgroup.com
Web: www.nexusgroup.com