WHITE PAPER

SECURITY BEST PRACTICE CHECK-LIST FOR IOT APPLICATION DESIGN

Having a secure platform and environment for IoT devices to operate is important, in order to ensure safety of users and prevent unwanted consequences that might occur as a result of a security loophole. In this sense, organizations delivering and using IoT systems must be diligent in their defense of device data and security aspects must be considered and implemented in their early design phase, not as an afterthought.

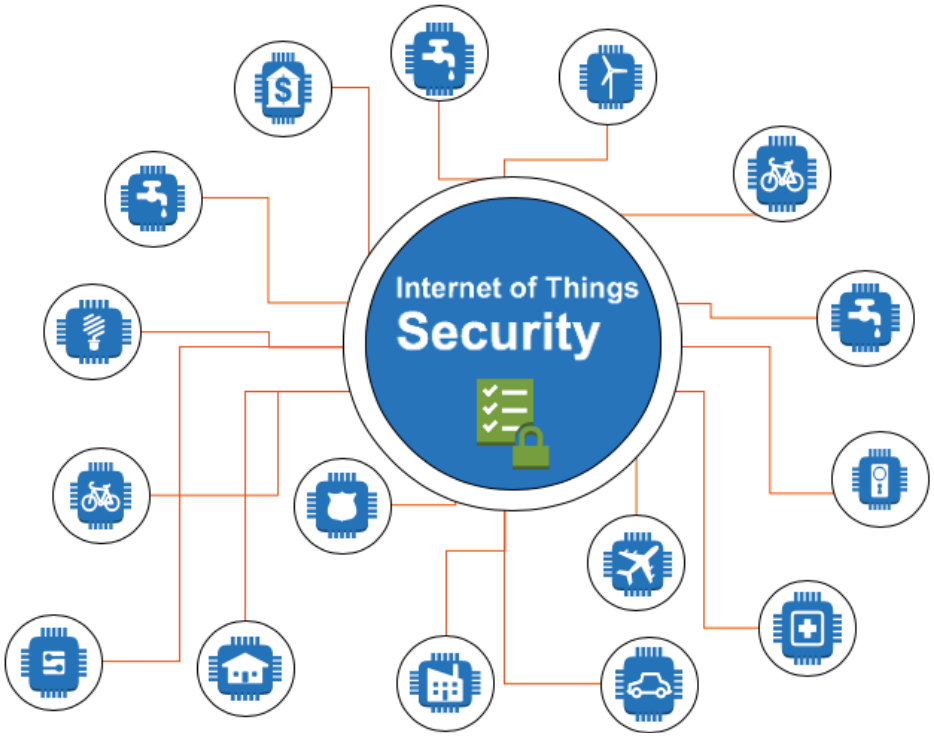
Sirris has built up extensive experience and knowhow in IoT security and will publish a series of white papers in which all the issues will be discussed in detail.

Our first white paper contains a security best practice check-list for IoT application design.

To ensure confidentiality, integrity and availability in IoT systems, the following security aspects need to be considered, in order to achieve security and privacy by design.

Security best practice check-list for IoT application design	
1. Authentication & Authorization	✓ Password authentication ✓ Strong device identity ✓ Multi-factor authentication ✓ Fine-grained access control
2. Communication Security	✓ Security against attacks ✓ Cryptographic protocols (e.g. TLS) ✓ Secure network communication (e.g. VPN)
3. Storage & data integrity protection	✓ Encrypted storage (security at rest) ✓ Data integrity assurance
4. Devices management	✓ Secure provisioning ✓ Secure activation/deactivation ✓ Secure monitoring
5. Privacy protection	✓ Privacy-aware application ✓ Private data access control ✓ Private data usage control
6. Secure IoT infrastructure	✓ Secure computing, processing and communication environment
7. Device setting security	✓ Devices must be configured to operate (no default configuration) ✓ Re-configuration control/ prevention

sirris
driving industry by technology



1. AUTHENTICATION/AUTHORIZATION

Ensuring that devices connected to system, as well as the associated application users are genuine is important in order to prevent malicious devices from tampering with the system. Authentication ensures that only allowed devices can connect to the system and interact with other devices, governed by access control policies (authorization), which ensures protection of devices and their data. If a password is used (local or remote) for authentication, strong passwords and multi-factor authentication (if possible) should be used. Hard-coded passwords on devices should be avoided. The identity of device (generally built in the hardware), which is used also as an authentication factor, should be well protected against exposure to the outside world.

2. COMMUNICATION SECURITY (END-TO-END SECURITY)

Devices in IoT environment need to communicate and exchange data (e.g. between sensors, controller and actuators) in a secure way in order to ensure integrity and availability. The attacks, such as eavesdropping and DoS, must be carefully addressed. If a security protocol such as TLS, relying on public key infrastructure (PKI), is used to secure the communication between different devices and system components (end-to-end security), the certificates must be well managed. The same applies to any secret keys used for symmetric ciphers (e.g. AES) and message authentication codes (e.g. HMAC). Certificate or secret-key renewal should happen automatically with minimum intervention from a physical person, in order to minimize the risks. Cryptographic secrets should never be transmitted “in the clear”; instead, other secure means (e.g. a separate VPN) should be used to limit their exposure.

3. STORAGE AND DATA INTEGRITY PROTECTION

In some cases, IoT devices need to store and process data locally («edge computing»), in order to improve performance and reduce the load at the back-end. However, processing data locally requires protection to ensure data integrity and to prevent data stealing. In case IoT data is processed at the back-end, such as a cloud platform, the data integrity and confidentiality need also to be ensured.

4. DEVICE MANAGEMENT

One of the most difficult tasks in an IoT system is the device management. How to securely provision, organize, activate, monitor, and remotely manage IoT devices at scale are the main challenges, which need to be addressed carefully when designing an IoT system. Closely following the lifecycle of the devices, keeping firmware and software updated are also parts of the devices management plan to make system secure.

5. PRIVACY PROTECTION

A large number of IoT use cases include the need to address the privacy issues. A thorough design and a careful review of privacy policies of the controlling applications, back-end services and data exchanged between them is necessary. In case private data is exchanged between different IoT systems (controlled by different organisations), ensuring data is used in compliance with privacy protection regulation is important and required by law.

6. SECURE IOT INFRASTRUCTURE (THIRD-PARTY PLATFORM)

In some cases, an IoT system is designed to be deployed on third-party infrastructure such as cloud platform. In such cases, it is necessary to research and carefully review the security model of the cloud provider and the system components used for IoT. This should be followed by examination of the IoT platform reference architecture and the communication protocols used by the provider to ensure the protection of data exchanged between different system components.

7. DEVICE SETTING SECURITY

In general, users (e.g. IT-illiterate users) like using default setting for devices. This is the security loophole and must be avoided. Non-default setting should be considered and a device with default setting should not be allowed to be provisioned in the system. Once devices are configured and provisioned in the system, re-configuration of devices without permission must be prevented. Automatic tools built to detect device reset and reconfiguration should be in place.

SUMMARY

In the next instalment in this series, we will discuss in detail each security features and its associated solution. We will also highlight some of lessons learned from IoT security failure of both IoT products and services.

AUTHOR

Annanda Rath

Senior Expert Software Engineering & Security

CONTACT : +32 493 31 06 45 - annanda.rath@sirris.be

Over the last 8 years, Annanda has been active in software and data security (in particular the access and usage control). At Sirris, he is a senior software security expert and actively working on different aspects of software security, from data to system security and privacy. He is particularly interested in data integrity and confidentiality in distributed environment: distributed ledger technology (e.g. blockchain and directed acyclic graph). Cloud, IoT and smart mobility are also his area of interest.

Annanda has a Phd in Computer Science from the University of Namur, a Master's degree in Computer Science from the Indian Institute of Technology, Bombay, India (IITB) and an Engineering degree in Computer Science from Cambodia Institute of Technology (ITC), Cambodia.