Contact us

Cybersecurity for IoT

IOT CYBERSECURITY AT ALL LEVELS

An IoT system is made up of various connected devices – which in turn comprise a number of integrated components – as well as a management, control and processing infrastructure.

Applus+ Laboratories has a team of engineers who are experienced in the security evaluation of hardware, software and communications protocols and able to evaluate the cybersecurity of IoT components, IoT devices and, indeed, entire IoT systems.

- IoT component cybersecurity evaluations
- IoT device cybersecurity evaluations
- IoT system cybersecurity evaluations

CYBERSECURITY EVALUATIONS OF IOT COMPONENTS

Every IoT device is made up of a number of components, which are themselves responsible for the device's key security functionality. Hence why the use of certified components or ones whose security has been evaluated is so important.

Security evaluations under recognised certification schemes:
Applus+ is a security laboratory that is accredited to evaluate hardware and software components embedded in IoT devices in accordance with a range of internationally recognised certification schemes:

- Common Criteria (Accredited Lab for the US, Canada and Spanish schemes)
- Sesip (Licensed Lab)
- PSA Certified (Accredited Lab)
- Fido (Authentication solutions)
- GlobalPlatform (TEE - Trusted Execution Environments)

Customised, independent evaluations:
In cases where certification is not mandatory but a manufacturer needs to evaluate the security of a particular product, Applus+ can provide independent, customised evaluations suited to all component types and applications. These evaluations can be fully adapted to meet the needs of the client: white/grey/black box, source code review, vulnerability analysis, design review, etc.

CYBERSECURITY EVALUATIONS OF IOT DEVICES

Security evaluations under recognised certification schemes:
Applus+ can evaluate the security of IoT solutions under Common Criteria. There are also a number of other IoT certification schemes currently under development. Please contact us to find out more about these new schemes.

Independent cybersecurity evaluations:
Well aware of the wide variety of applications that exist within the IoT field, our experts can create an evaluation to suit the particular features of the product in question, taking into account the nature of the product, the type of IoT solution it is intended to form part of and the type of data it will process. A smart light bulb, a gateway that manages a hotel's lighting system and an electricity company's smart meter do not all share the same criticality. Our evaluations look at the following aspects, but are always tailored to the client's needs:

- **Data protection:** IoT devices are able to store and share sensitive information such as cryptographic keys and personal data that must be protected. As such, we evaluate communications security for all protocol types (BLE, Zigbee, Wi-Fi, LTE, etc.), as well as the security of the storage mechanisms (asset protection).
- **Interface security:** All of an IoT device's access interfaces need to be identified and their levels of protection evaluated, along with their authentication/identification mechanisms: web interfaces, network interfaces (unsafe open ports), physical interfaces (JTAG, UART, etc.), API Cloud and API Mobile.
- **Secure updates:** What is the mechanism for carrying out updates securely? Is there a protocol for validating the integrity and authenticity of a new binary ? Our experts evaluate the device's update systems and patching protocols.
- **Safe boot:** What is the device's boot/reboot system mechanism? We evaluate the equipment's boot protocol to ensure that it is secure and reliable.

Methodologies and good practice guides: Most countries are still in the process of developing their IoT regulations/standards. In the meantime, there exist several methodologies and good-practice guides on which evaluations can be based, including:

- GSMA IoT Security Guidelines and Assessment
- OWASP IoT Top 10
- Code of Practice for consumer IoT security
- ENISA Baseline Security Recommendations for IoT.

Do not hesitate to get in touch if you are interested in an evaluation in accordance with one of these methodologies/guides.

CYBERSECURITY EVALUATIONS OF IOT SYSTEMS

The security of an IoT system goes beyond protecting each of its constituent devices. Although these may be individually secure, once they are deployed and connected, new system threats can surface. Similarly, management of the supply chain is crucial as the security of a system relies heavily on being able to trust in its various components.

Supply chain security assessments:
A single vulnerable device can compromise an entire system. Manufacturers need to have confidence in the devices and solutions making up their systems and for this they need dependable supply chains. How can Applus+ help them achieve this?

- By assessing the risks and threats inherent in a given supply chain
- By carrying out security audits on development and production plans
- By security-testing solutions that do not hold a recognised security certificate
- By assessing a system's inherent risks and threats
- By evaluating the different layers (cloud, fog, remote mobile controllers) and their interfaces

Note: Because Applus+ Laboratories is accredited as a third-party laboratory by several evaluation and certification schemes, and in order to guarantee its impartiality, Applus+ engineers are never involved in actual product development or solutions implementation.