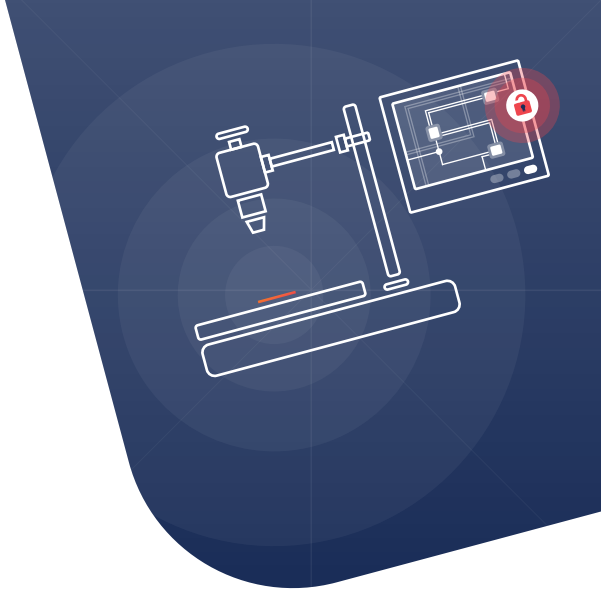
KUDELSKI IOT THINGS



IoT Device Security Discovery

Understand the security level of your devices so you can fix identified security gaps.

360° APPROACH

Comprehensive, multidisciplinary expertise

We follow the typical path of hacker attacks, taking into consideration current technologies and knowledge to highlight the strengths and vulnerabilities of the system. Our Hardware, Network, Software and Crypto security teams collaboratively address the following critical aspects of your device:

- **Authenticity**
  Prevent data falsification by masquerading identity.
- **Integrity**
  Avoid malicious modification of a device.
- **Non-repudiation**
  Provides proof of the integrity and origin of data.
- **Confidentiality**
  Verify that data and code does not leak, meet GDPR requirements.
- **Availability**
  Ensure a service can be reached.
- **Authorization**
  Prevent unauthorized actions.

ENGAGEMENT PHASES

Actionable insights into the security of your device

By considering the system as a whole, our security experts will go beyond a standard penetration testing by covering the most probable local and remote attack vectors.

1	Exploration phase	Secure IP Secure IoT foundations for your SoC enabling the IoT use cases customers require. In-Field Provisioning Effortless, efficient, zero-touch provisioning of IoT devices to end-user networks. Secure Firmware Update (FOTA) A proven system to enable secure device updates while protecting them from attack.
2	Wireless & Hardware penetration testing	Secure IP Secure IoT foundations for your SoC enabling the IoT use cases customers require. In-Field Provisioning Effortless, efficient, zero-touch provisioning of IoT devices to end-user networks. Secure Firmware Update (FOTA) A proven system to enable secure device updates while protecting them from attack.
3	Device teardown	The device tear-down will allow physical inspection and internal architecture and components review. The device design analysis consists in inspecting the PCB, identifying all chips, external memories and interconnections, as well as locating JTAG and debug interfaces.
4	Micro-code extraction	Micro-code extraction by chip-off is an intrusive method applied to acquire a non-volatile image from microcontrollers and external memories of the device. Obtaining an image of the memory contents enables the analysis of the software and the anti-tampering mechanisms. Based on the memory contents, a list of known Common Vulnerabilities Exposures (CVE) can also be established.
5	Device security lifecycle	The last step of the investigation involves the analysis of the device security lifecycle. The security of the firmware or software upgrade functionality (signature, anti-rollback, versioning), as well as the device customization and personalization (key provisioning, factory settings) will be assessed.

NEXT STEPS

Engagement inputs & deliverables

Engagement **inputs**

- Two or three samples are required for analysis. If required, the hardware analysis might be destructive in nature.
- Any relevant documentation making the evaluation more efficient shall be provided as well.
- Firmware file, user account credentials.

Engagement **deliverables**

- The actionable improvement recommendations resulting from the analysis will make easier to reach the expected security level.
- Detailed technical report in PDF format describing the evaluation steps, providing details on the methodology. The detailed description of security gaps and misconfigurations is a baseline to improve the security level of the device.
- An executive summary with key strengths and weaknesses of the device.

OUR PROVEN METHOD

Three steps to IoT success

We have been designing and testing secure devices for our clients for decades. With our help, you can take new products to market with confidence using our proven methodology for IoT security threat identification, mitigation and validation.

IoT THREAT ASSESSMENT

We help you understand potential threats to your business, their likelihood and impact in order to focus security development.

SECURITY ARCHITECTURE REVIEW

We create a security architecture that addresses key threats defined during the Threat Assessment exercise.

LAB SECURITY ASSESSMENT

We test products against defined security requirements and spot any potentially business-impacting vulnerabilities.

ABOUT KUDELSKI GROUP

Kudelski IoT is the Internet of Things division of Kudelski Group and provides end-to-end IoT solutions, IoT product design, and full-lifecycle services to IoT device manufacturers, ecosystem creators and end-user companies.

These solutions and services leverage the group's 30+ years of innovation in digital business model creation; hardware, software and ecosystem design and testing; state-of- the-art security lifecycle management technologies and services and managed operation of complex systems.

$100B
revenues enabled annually

32
offices worldwide

3250
employees

$779M
revenues (2021)

500M
users

70
years of innovation