KUDELSKI IOTHINGS

RA Ecosystem Partner Solution

Kudelski IoT Device Security Discovery

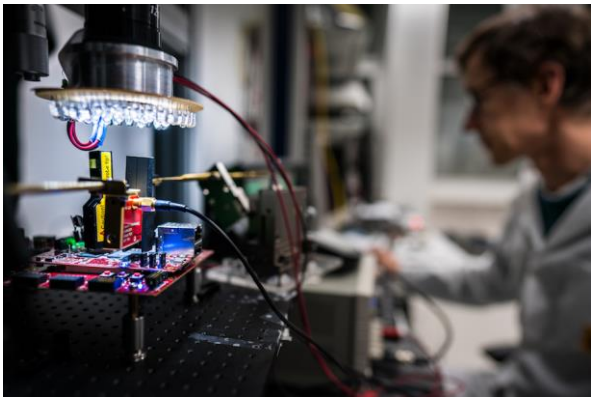
Solution Summary

Kudelski IoT Labs evaluates devices, systems, and semiconductors to highlight the security gaps that could impact integrity, availability, or data confidentiality and ensure the security lifecycle is properly managed over time. We take a 360° approach to device security to help you create a security architecture that addresses your key threats, test your product against defined security requirements (often determined in a threat assessment) to identify vulnerabilities and provide an evaluation report containing mitigation recommendations to improve security and address identified risks. The use of secure chipsets like the RA family of MCUs in combination with Device Security Discovery gives device manufacturers a powerful tool to meet the security requirements of standards and regulations.

Features/Benefits

- 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

Diagrams/Graphics



Target Markets and Applications

- IoT devices and systems

Enhancing IoT Device Security

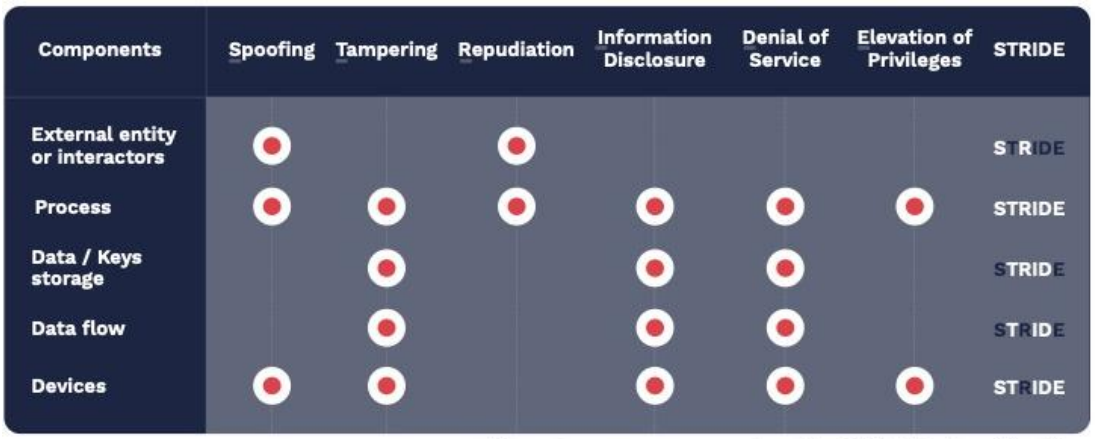
2024.04

KUDELSKI IOT THINGS

Kudelski IoT Security Labs Services

360° Approach to Device Security

For more than 30 years, Kudelski IoT Labs have helped companies ensure their products are secure by design. Embedding the right security features can protect against threats and enable new business models and opportunities. For product developers, it is essential to take a security-by-design approach, starting way earlier than just having a Device Security Discovery. Kudelski IoT's Threat Assessment service is the first step to understanding the potential threats to your business, their likelihood, and business impact so we can provide you with a clear focus for security development.



Threats on components with STRIDE classification

To support product developers throughout the entire process of designing and developing products which are sufficiently robust against attacks relevant to their use case, Kudelski IoT Security Labs offer:

- **Threat Assessment and Risk Analysis:** Defined threat scenarios, their impact, the likelihood of a successful attack occurring, and the appropriate security target to achieve.
- **Security Architecture Review:** Outline of appropriate measures to protect the most critical assets and reach business objectives.
- **Device Security Discovery:** Red team advanced penetration testing within a fixed time period.
- **Security Evaluation:** Hardware, software, & crypto evaluation based on a target of evaluation.
- **Source Code Security Analysis:** Validation that HW and SW attacks cannot be carried out by validating common secure coding standards are applied with a threat mitigation approach.
- **Conformity checking:** Analyze to what extent a product and its development environment complies with security requirements in standards and regulations.
- **Tailored Research:** Demonstration of the potential of new attack techniques on semiconductors.

Contact: https://www.kudelski-iot.com/#contact

www.kudelski-iot.com