KUDELSKI SECURITY

IoT Security Center of Excellence

Getting IoT Security Right

Kudelski Security enables the protection of IoT products and services throughout their full lifecycle

The Internet of Things (IoT) is expanding dramatically, with an anticipated 25 billion devices connected by 2020[1]. While IoT has an undisputed role in driving innovation and growth, serious questions remain over the security of the devices, the IoT ecosystems within which they operate, and the privacy and integrity of data that is transmitted. Technology vendors and integrators must respond to these concerns as ineffective security will ultimately limit product and service adoption and impact their brand reputation and return on investment.

Our IoT Center of Excellence takes an end-to-end approach to the security of IoT devices and their ecosystems, from the design and architecture phase to post launch. We draw on 20+ years' experience of successfully securing over 400 million PayTV devices around the world and are uniquely able to offer the assurance that stakeholders along the IoT value chain seek.

Our unique approach to securing a smart world

Securing our smart world is not simple. The IoT attack surface is huge, comprising a vast ecosystem of devices and technologies, different communication protocols, platforms, applications, and infrastructures.

Kudelski Security has rich digital security expertise and technological capabilities to ensure devices and systems meet desired security levels at all stages of their lifecycle, before and after launch.

Our security assurance goes beyond hardware and software security assessments and evaluations, to include recommendations and implementation of effective security controls, and the creation of proactive and reactive countermeasures to mitigate risks and protect investments throughout the lifecycle. Our legal services offer additional assurance by providing support for litigation in the event that intellectual property is infringed.

1. IoT Security Design and Assessment:

We work with clients to build security into the design and architecture of their projects. Right from the start, security is optimized, reducing risks throughout the lifecycle. For clients with existing products, we carry out in-depth assessments and evaluations to determine security levels of chipsets, HW and SW components in IoT devices and ecosystems. Our advanced labs experts use industry standards, best practices and proprietary methodologies to create security recommendations supporting business objectives.

2. IoT Security Posture Improvement:

Once we have identified vulnerabilities, flaws and weaknesses that may affect your IoT product ecosystem, we use best-in-class technologies and patented mechanisms to implement security controls in embedded systems, software/ firmware, communication protocols, platforms and applications.

3. IoT Cybercrime Countermeasures:

We provide prompt advice and access to response services in the event of sustained attacks or emerging threats targeting your deployed IoT products and services. We can embed sleeper countermeasures into devices that can be activated against threats and carry out rapid prototyping of countermeasures powered by threat intelligence from our Cyber Fusion Center. Should your intellectual property be infringed, our legal teams can provide support for litigation.

KEY BENEFITS

- ✓ Strike the right balance between IoT security measures, risk and cost; accelerate time to market
- ✓ Get the right security for the full IoT product/services lifecycle – protect your customers and reputation
- ✓ Access legal and subject matter expertise – defend your valuable IP

[1] *Gartner Forecast: IoT Security, Worldwide, April 2016*

MANAGING THE IOT SECURITY LIFECYCLE

THE IOT ECOSYSTEM

SECURITY DESIGN AND ASSESSMENT

- Architecture design
- Firmware and application
- Wireless protocols
- Device and infrastructure

- Security recommendations at design stage
- In-depth security evaluations (side channel, fault injection, imaging and IC modification)
- Reverse engineering
- Source code audit, deobfuscation, fuzzing, cryptography implementation audit (e.g White Box crypto), software vulnerability verification
- Advanced penetration testing (device, application, network)
- Assessment of wireless protocols through in-house LPWAN lab (e.g. Sigfox, LoRa, NB-IOT) and of short distance communication protocols

SECURITY POSTURE IMPROVEMENT

- Hardware security
- Software security
- Key management

- Software code and data obfuscation against tampering, reverse engineering and code lifting
- Portfolio of application-specific secure elements and custom crypto
- IC Embeddable Hardware IP blocks for hardware Roots of Trust
- White Box cryptography to protect secret keys and algorithms
- Security device management and vulnerability patching
- Multi-level key management system (provisioning, authentication, authorization, rights management)

CYBERCRIME COUNTERMEASURES

- Hardware built-in protection mechanisms
- Proactive implementation to mitigate new vulnerabilities
- Reactive implementation in case of breach

- IOT threat intelligence from our Cyber Fusion Center
- Ability to create technical countermeasures that mitigate the impact of emerging threats or breaches
- Verification of the efficiency of the selected countermeasures at our in-house LPWAN lab
- Global network delivery legal support for litigation

The IoT Security Center of Excellence helps IoT technology vendors and integrators across different industries to secure their investments through an end-to-end approach that goes beyond security assessments.

KUDELSKI SECURITY

Lausanne, Switzerland

Zurich, Switzerland

Madrid, Spain

Phoenix, AZ, U.S.

Atlanta, GA, U.S.

Minneapolis, MN, U.S.

info@kudelskisecurity.com | www.kudelskisecurity.com