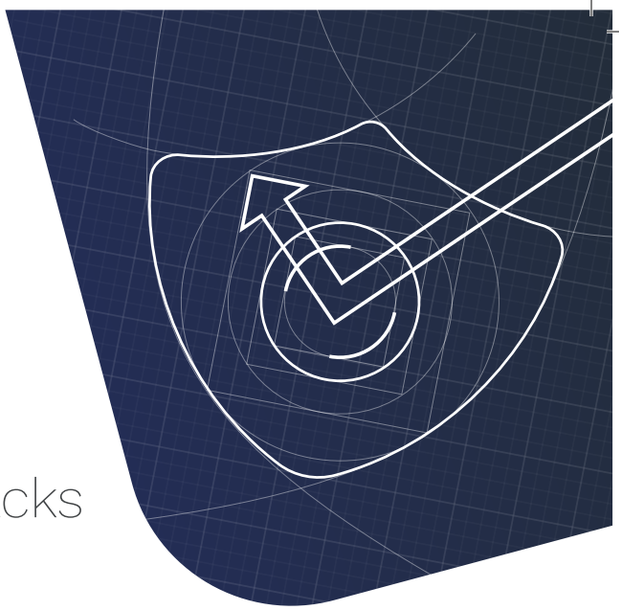
KUDELSKI IOT THINGS

IoT Security **Workshop**

Equip yourself to defend your IoT product & ecosystem against attacks



WHY ATTEND A HANDS-ON IoT SECURITY WORKSHOP?

Learn to protect your products from threats in three days

The key outcome of the Security Workshop is a strong awareness of IoT threats and mitigation techniques that can be used to protect your IoT ecosystem from harm.

YOUR CHALLENGE

- The security of your IoT solution could have a large impact on your project's success or failure.
- You may not have the in-house knowledge required to effectively plan, implement and manage IoT security.
- It's especially hard to keep up to date because attacks and cyberthreats are constantly evolving.

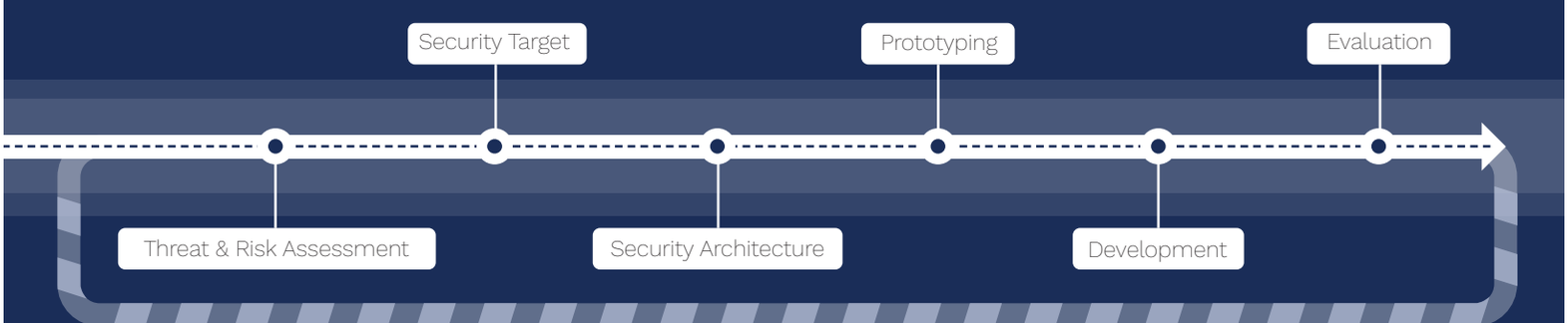
OUR SOLUTION

- We train you to assess the primary threats to your IoT projects, ecosystems and devices.
- Learn how to design products to mitigate those threats during the entire lifecycle of the product.
- Get practical experience in executing common attacks - and how to protect against them.

LEARN SECURITY BY DESIGN

Design, prototype and maintain a secure IoT architecture

Our experts teach a methodology that will allow you to get IoT security right from the start. Topics covered in the workshop will include:



Correcting security faults in the field is 60-80x more expensive than fixing them before launch.

KEY OUTCOME: THREAT AWARENESS

Discover how to manage the top 5 attack categories to your IoT ecosystem

You will learn to assess and rank the primary threats for your own system and context. This allows you to focus the investment in security measures based on the specific application and on the specific business context.

1

Remote attacks

The attacker carries out the attack from a remote location and can generally compromise multiple devices in a short amount of time. This is the worst nightmare for whoever operates IoT devices in the field. In some instances, the attack can occur on the cloud device manager, giving full control to the attacker over the system.

VULNERABILITY DISCOVERY

- Documentation and intelligence review
- Security domains identification
- CVE identification
- Device & backend penetration testing

2

Network attacks

The media and protocol that the IoT devices use to communicate are often wrongly trusted. If these channels are compromised, the devices could in turn be compromised as well. Wireless telecommunication networks can be jammed and even spoofed. Same goes for local wireless protocols like WiFi and Bluetooth. In certain cases, feeds like GPS can be tampered with as well.

VULNERABILITY DISCOVERY

- Communication protocol identification, proprietary interfaces and debug ports
- Wireless communication penetration testing
- Mobile app

3

Local attacks

With physical access to a device, the attacker may be able to compromise it with low-cost equipment and basic skills. The memory of the device could be extracted and modified through interfaces or through direct access to the flash memory. Such attacks are local but in some cases, they can be used as a stepping stone to mount remote attacks (each device has credentials to access the cloud where ALL devices are managed).

VULNERABILITY DISCOVERY

- Tear-down, PCB inspection, design analysis
- Memory dump (partial reverse-engineering)
- Analysis of anti-tampering mechanisms
- Software attacks

4

Elementary hardware attacks

Attackers with average skills and entry-level equipment can perform attacks typically meant to extract encryption keys and cloud credentials giving access to the backend. This allows cloning devices and accessing the cloud, much like local attacks, except that in this case the device manufacturer had good security practices but used weak hardware.

VULNERABILITY DISCOVERY

- Low-cost non-invasive hardware attacks
- e.g. Single electrical glitch fault injection
- e.g. Simple power side-channel analysis

5

Advanced hardware attacks

Skillful and well-equipped attackers will have the ability to carry out attacks on devices with a good level of security, both in software and hardware. While this is not a threat that should be considered for all systems, the most critical ones are at risk. In some cases, an initial compromise may require an advanced attack, but it will then open the door to cheap and easy attacks for all other devices in the system.

VULNERABILITY DISCOVERY

- Advanced non-invasive attacks such as electrical and electromagnetic glitch
- Differential power side-channel analysis
- Semi-invasive hardware attacks (laser fault injection)

Our security-by-design methodology will encourage you to design your products with the top 5 attack categories in mind, starting from the beginning, at the architecture phase.

WHO IS THE WORKSHOP FOR?

Product Managers | Technical Managers | R&D Experts | Product Owner | CISO

PRE-REQUISITE KNOWLEDGE

Participants should come to the IoT Security Workshop with a good basic understanding of general technology principles like networking, programming and hardware.

NUMBER OF ATTENDEES

Minimum 3 - Maximum 10. Mixed audience.
Upon request: dedicated session for a single company to maintain confidentiality.

WORKSHOP AGENDA

DAY 1

Attack classes (1 & 2)
- Remote Attacks
- Local Attacks

Workshop
- IoT communication analysis (BLE, MQTT ...)
- Pentest, fuzzing and remote attacks

Introduction to IoT security
- Keys security principles
- Overview of the five classes of IoT attacks

DAY 2

Attack class (3)
- Network Attacks
- Embedded Attacks

Workshop
- Exploration of the attack surface
- Reverse-engineering and exploitation
- Jtag / Debug port

Product security lifecycle
- Threat assessment
- Security architecture
- Secure SW development
- Evaluation, monitoring
- Incident management

DAY 3

Attack classes (4 & 5)
- Elementary Hardware Attacks
- Advanced Hardware Attacks
- Low-cost Hardware Attacks

Workshop
- Disabling readout protection using voltage fault injections
- EM and laser fault injections presentation
- AES key retrieval using side-channel attack

- Visit of our assessment lab
- Final hands-on wrap-up exercise

LOCATION

The 3-day training takes place in the Kudelski IoT Labs in Cheseaux-sur-Lausanne, Switzerland (a 40-minute drive from Geneva Airport). During the training in Switzerland, we will use the facilities of our advanced labs to illustrate specific attacks.

KUDELSKI IoT LABS

Our advanced labs help more than 100 customers per year conduct threat assessments, design secure devices and ecosystems, and assess the security, of new or existing devices in order to ensure they are robust against identified threats.