Factsheet

KUDELSKI LABS

Kudelski Labs - Device Hardware and Software Penetration Testing

Assess Real-World Attacks to Uncover Vulnerabilities and Strengthen Device Security

Device Hardware and Software Penetration Testing is a black-box Red Team engagement in which Kudelski Labs simulates adversarial actions to assess exposure to threats and identify security weaknesses across hardware, software, and network interfaces.

Our experts follow the typical path of attackers, leveraging current techniques, tools, and threat intelligence, to expose security gaps and assess device resilience. We provide clear, actionable recommendations to strengthen defenses and can perform a short retest phase to validate the correct remediation of identified vulnerabilities.

Comprehensive Device Security Testing

- Real-world adversarial attacks
- Hardware, software, network, remote & local attack coverage
- Actionable insights with remediation retest

Understand How Attackers See Your Device

- Assess the impact of realistic adversarial behavior with a black-box Red Team approach, using state-of-the-art techniques and advanced tools. Leveraging 30 years of experience in connected device assessment
- Uncover weaknesses from Chip to Cloud
- Validate the implementation of the security lifecycle
- Provide actionable insights and remediation guidance to strengthen device security

Our Penetration Testing Approach

Kudelski Labs evaluates your device exactly as an attacker would, using a structured black-box methodology that examines exposed interfaces, hidden attack surfaces, and internal components. This approach identifies exploitation paths and reveals weaknesses that could be used by malicious actors or competitors.

1. Exploration & Reconnaissance

- Analyse the threat and constraints landscape
- Business model analysis
- Technology analysis

2. Hardware & Wireless Penetration Testing

- Discover communication protocols (incl. proprietary)
- Analyse ports, services, APIs, mobile applications
- Perform targeted wireless and hardware attacks

3. Device Teardown & Microcode Extraction

- Physical inspection of PCB, components & memories
- Identify debug/JTAG interfaces
- Extract microcode/firmware for deep analysis

4. Software & Firmware Security Analysis

- Analyse binaries, configuration and anti-tampering mechanisms
- Map identified CVEs and insecure design patterns

5. Security Lifecycle Evaluation

- Assess firmware update mechanism (signing, rollback, versioning)
- Evaluate key provisioning and secure personalization

Penetration Testing insights

Our penetration testing delivers deep technical insights and practical recommendations.

- Real-world attacker simulation via black-box Red Team approach using a proprietary methodology
- Use of state-of-the-art techniques and advanced tools to access code and data
- Hardware, firmware, software, wireless and cloud-interface coverage
- Full device teardown and internal architecture analysis
- Microcode extraction for deep firmware review
- Automated + manual vulnerability analysis including CVE mapping
- Actionable, prioritized recommendations with remediation validation retest

What This Testing Reveals

Our penetration testing highlights:

- Hardware vulnerabilities and exploitable design flaws
- Weaknesses in communication interfaces and exposed services
- Firmware and software misconfigurations
- Cryptographic implementation issues
- Debug interfaces or undocumented access channels
- Risks during provisioning, or firmware update lifecycle

Where This Service Delivers Value

Device Hardware and Software Penetration Testing is used to:

- Validate the resilience of a new device before launch
- Secure devices involved in safety-critical or regulated environments
- Benchmark product security against competitors
- Identify weaknesses in legacy devices before redesign
- Support certification or customer security requirements
- Strengthen security posture for long-lifecycle products
- Prevent high-impact product failures, data and code exposure (breach, cloning), costly fixes and recalls
- Create competitive advantage, achieves regulatory compliance
- Protect long-term revenue streams, intellectual property, brand reputation and customer trust
- Improve product design and engineering efficiency

Strategic Intelligence. Impactful Action.

Our embedded security expertise is rooted in more than three decades of hardware, software and cybersecurity experience. We use our expertise and technology to protect all key assets - devices, identity, data, decisions, commands and actions throughout the lifetime of the device and its ecosystem.

Explore Our Innovations

Contact Us

info@kudelskilabs.com | www.kudelskilabs.com

KUDELSKI LABS