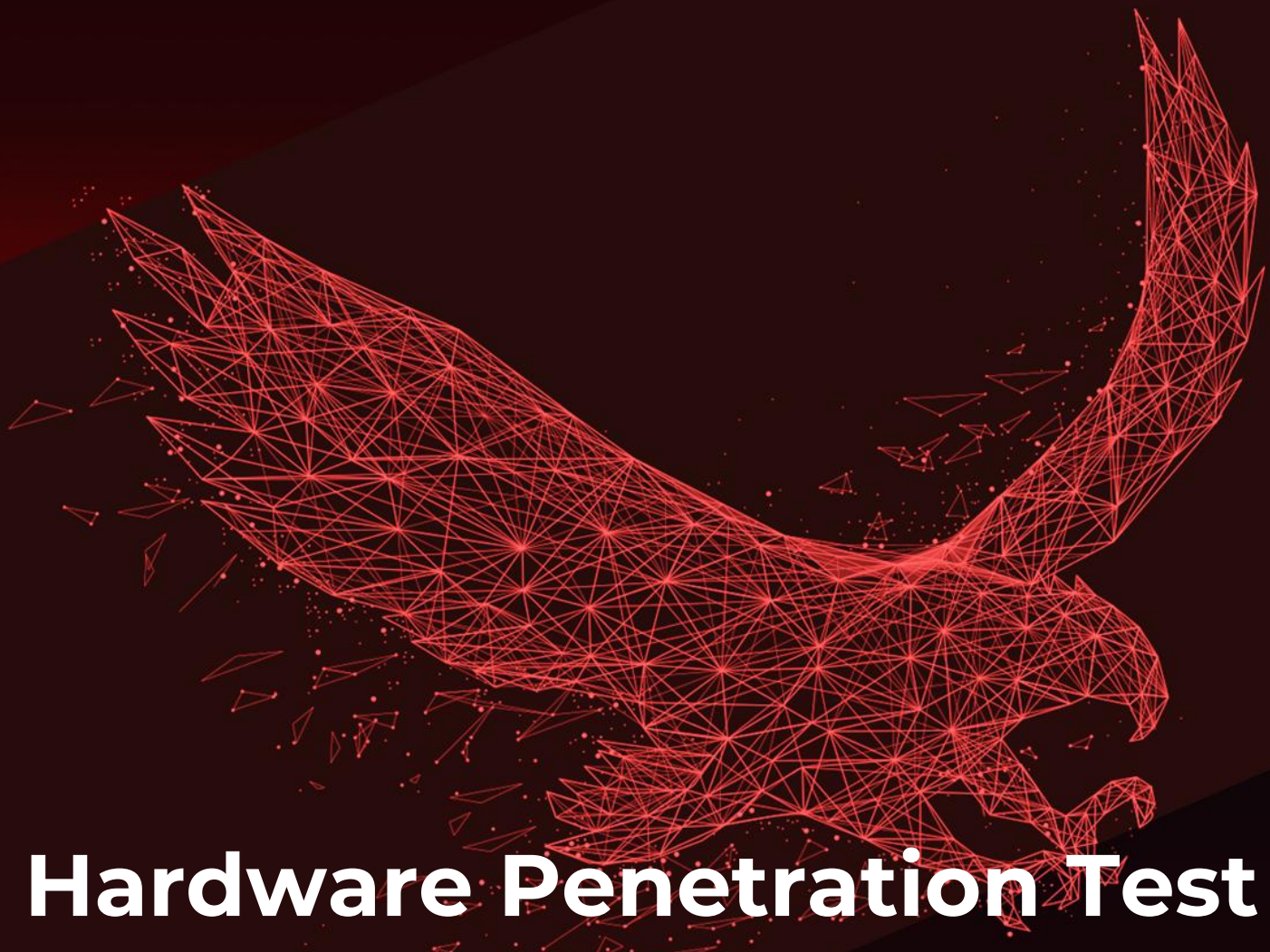
Privia SECURITY



Hardware Penetration Test Service

Professional Offensive Security Services

"From Firmware to Chip, Security at Every Layer!"

The information contained in this document is related to the Professional Offensive Services provided by Privia Security Information and Consulting Services and is of a general nature. All information presented in this document is publicly available.

Queen Elizabeth Olympic Park, 14 East Bay Lane, Plexal, London, England, UK, E20 3BS

info@priviasecurity.co.uk

www.priviasecurity.co.uk

“Hardware penetration testing minimizes security risks by revealing vulnerabilities to unauthorized access and manipulation in all components of hardware (chip, backdoor, firmware and circuitry).”

Hardware penetration testing is a comprehensive testing process performed to reveal the security vulnerabilities of physical hardware. Hardware Penetration Testing covers a wide range from ECS (SCADA), IT, IoT hardware to network equipment, embedded systems and critical infrastructure hardware. During the test, the ports, chips, data paths, embedded operating system and firmware layers of the hardware are examined to identify risks such as unauthorized access and data manipulation.

The increasing importance of physical threats requires strong security not only at the software layer but also at the hardware layer. With Hardware Penetration testing, the PCB circuits, connection points, possible backdoors and hardware-based authentication mechanisms of the hardware are analyzed from an attacker's perspective. Side-Channel attacks, Tampering/Forgery and Reverse Engineering techniques are used to conduct audits in accordance with international standards. Especially focusing on firmware security, critical elements such as updateability and integrity are also reviewed.

With this comprehensive service, companies and organizations (law enforcement agencies, public and private companies with critical infrastructures) can increase the resilience of their hardware and be prepared for potential threats. By identifying vulnerabilities in advance, hardware penetration testing makes it possible to eliminate security gaps and comply with legal regulations. Thus, infrastructure security and system continuity are ensured by developing strong defense strategies.

Service Components

Physical Examination and Manipulation Tests

In this phase, the outer casing, connection points and internal components of the hardware are analyzed in detail. It is determined whether labels, seals or physical protection measures have been manipulated. The physical integrity of the hardware is assessed by examining threats such as the addition of counterfeit hardware parts and interference with cable entries.

Port and Ports Security Tests

Unauthorized access or exfiltration attempts through ports such as USB, Ethernet, JTAG, UART and SPI are tested. The presence of open ports and unnecessary services are checked to see if attackers can access the system using these paths. Configuration errors of the hardware's external ports are identified and security vulnerabilities are uncovered.

Firmware Analysis and Reverse Engineering

In this phase, the firmware of the hardware is examined and tested to see if fake updates can be installed. The firmware is analyzed for the presence of backdoors or malicious code. Reverse engineering techniques are used to assess the leakability of sensitive data (passwords, keys) in the firmware. In addition, the security of the update mechanism is examined and data integrity is maintained.

Side-Channel Analysis and Electromagnetic Tests

Hardware's power consumption, timing differences and electromagnetic emissions are analyzed to test its resilience to Side-Channel attacks. Such attacks are aimed at obtaining encryption keys or sensitive information by using clues to the physical performance of the hardware. With the studies carried out, the security of information that can be intercepted by Side-Channel attacks is ensured.

Testing of Authentication and Security Mechanisms

Security technologies, authentication processes, identity storage methods and protection mechanisms used on hardware are examined. The reliability of secure boot, TPM and biometric authentication systems are tested. In addition, the hardware's anti-counterfeiting detection systems and physical integrity protection measures are evaluated. All these checks are performed to determine how resistant the hardware is to unauthorized access.

FAQ

What is hardware penetration testing?

Hardware penetration testing is a security audit to detect vulnerabilities in the physical and digital components of hardware. It is a test method that reveals the current state of hardware against ports, firmware and side-channel attacks.

Why do a hardware penetration test?

It prevents data leaks, backdoor risks and system failures by detecting potential attacks at the hardware level. Hardware penetration tests are carried out in many different areas such as military systems, critical infrastructures, weapon systems, defense infrastructures, power generation facilities, natural gas exploration equipment and are an important service in ensuring national security.

What tools are used in hardware penetration testing?

The tools used in hardware penetration testing span a wide range at both the software and hardware layer. As network analysis tools, Wireshark and tcpdump are used to monitor data traffic to detect which protocols hardware is running, the presence of open ports and suspicious network activity. At the same time, tools such as THC Hydra can be used to crack hardware authentication systems.

In physical interface testing, JTAG and UART analyzers provide direct access to hardware components, allowing the internal structure of the hardware to be debugged and backdoors to be detected. In analyzing side-channel attacks, oscilloscopes and electromagnetic field measurement equipment are used to examine power consumption and signal propagation. In firmware analysis, tools such as Binwalk and Ghidra are used to reverse engineer the internal software of the hardware.

How long does a hardware penetration test take?

The duration of testing varies depending on the complexity and scope of the hardware. The process usually takes a few days to a few weeks and includes discovery, testing and reporting.

Which types of hardware require penetration testing?

Hardware with critical infrastructure such as IT, OT and IoT hardware, network hardware, smart cards, industrial control systems and embedded systems should be subject to penetration testing.

What does the penetration test report contain?

The reports contain details of the vulnerabilities identified, their potential impact and suggested solutions. It also describes which components of the hardware have security vulnerabilities and the measures to be taken.

Your Trusted Partner in Cybersecurity

Founded in 2018 with a vision for the future of cybersecurity, Privia Security has been committed to delivering high-quality services to its clients from day one. With a strong and capable team, we provide the most reliable and comprehensive solutions across all areas of cybersecurity, ensuring our clients are well-protected in today's digital landscape.

As cyber threats continue to evolve rapidly and grow in complexity, combating them becomes increasingly challenging. At Privia Security, we offer both defensive and offensive cybersecurity strategies powered by cutting-edge technology to meet our clients' evolving needs. Through our innovative R&D products and strategic consultancy, we aim to enhance organizations' cybersecurity maturity and deliver proactive, tailored solutions. We are proud to be safeguarding the digital assets of more than 300 major organizations.

Global and Local Cybersecurity Solutions

Privia Security delivers cybersecurity services across a broad geographical scope, including Europe, Asia, the Middle East and the Americas. Our specialized teams in Offensive, Defensive and Forensic operations develop bespoke solutions for organizations operating in diverse sectors such as critical infrastructure, avionics systems, corporate networks and the military.

In addition, our innovative cyber warfare simulation platform, PriviaHub, offers comprehensive solutions for nations seeking to strengthen their cyber defense capabilities. PriviaHub enables the testing of cyber warfare strategies, execution of simulations and assessment of expert competencies. Designed to meet the exercise needs of private sector entities, academic institutions and military organizations, it bridges the gap between training and real-world readiness.

A Secure Future Through Advanced Technology

With R&D centers located in Istanbul, Ankara, London and at Cumhuriyet Technopark, we are continuously developing value-driven projects for our clients. From penetration tests and red team operations to cybersecurity training and custom enterprise solutions, we are redefining the standards in our industry. Through our slogan "Privacy For You," we bring a fresh, innovative perspective to security and privacy—

Privia
SECURITY