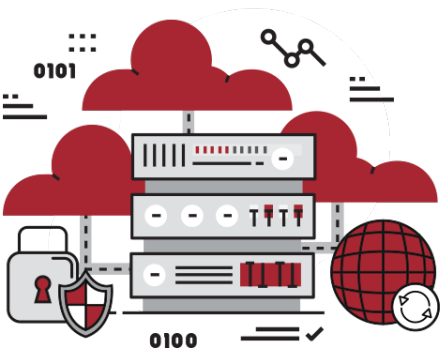
INTERNET OF THINGS (IOT)

Find Critical Vulnerabilities in Your Device

RHINO SECURITY LABS

An estimated 5.5 million devices are added to the Internet of Things (IoT) every day. These devices range from coffee makers in your home to respiratory machines in your hospital and cars on the highway. The variety of environments and networks IoT devices operate within make them a novel target for attackers.

Rhino Security Labs employs a range of unique penetration testing tools for testing IoT devices, going beyond automated vulnerability scanning. Our device assessment strategy mimics real-world hacking techniques that uncover hidden vulnerabilities in your device.



HARDWARE ASSESSMENT

Our hardware experts have extensive experience reverse engineering a range of devices, including medical, retail, and physical security systems. This process allows assessors to gain access to hidden storage, identify hardcoded secrets, and bypass software-enabled security protections.

SOFTWARE ASSESSMENT

Once the firmware and unique subsystems are extracted, those are passed to software specialists to fuzz and identify security flaws in the code. Attack vectors here include insecure storage, command injection, authentication and session handling flaws, and more.

INTERNET OF THINGS NETWORK TARGETS

Even if the IoT device doesn't handle sensitive data or processes, it's still a new device in the environment. Compromised IoT devices act as a gateway for attackers to obtain access to valuable data or systems that live on your network. Conducting an IoT assessment can pinpoint risks associated with the device as well as the company's resilience to an attack.

While embedded devices may provide a clandestine backdoor to sensitive networks, they can also be harnessed en masse to attack other systems, such as a DDOS attack. Neglecting security best practices for IoT devices can result in regulatory fines, legal risk, accountability and reputation impact.

- *Understand the environment the device operates*
- *Reverse engineer the software to uncover hardcoded sensitive data*
- *Dismantle hardware components and examine for vulnerabilities*
- *Exploit access to additional network assets*

info@RhinoSecurityLabs.com | 888.944.8679

464 12th Ave, Suite 300 | Seattle, WA 98122

ASSESSMENT DETAILS AND METHODOLOGY

At Rhino Security Labs, our IoT penetration assessments target the entire device include the hardware, software, and the environment in which it operates. Each assessment follows these steps:

Take apart hardware to find veiled information

1. Hardware Analysis

Each IoT engagement begins by thoroughly disassembling the physical device to understand how it works and where vulnerabilities may lie. We specialize in a range of physical attack vectors, including subverting secure boot capabilities and side-channel attacks on crypto-algorithms.

Reverse engineer firmware and software

2. Software Reverse Engineering

Once the hardware analysis is complete, we move up the stack to firmware and software examination. By mapping out custom code and identifying associated vulnerabilities, we ensure coverage of all attack vectors and a more comprehensive engagement.

Identify and map vulnerabilities

3. Vulnerability Discovery

Once the target has been fully enumerated, Rhino Security Labs uses both vulnerability scanning tools and manual analysis to identify security flaws. With decades of experience and custom-built tools, our security engineers find weaknesses automated scanners miss.

Safe and controlled exploitation of vulnerabilities

4. Attack and Post-Exploitation

At this stage of the assessment, our consultants review all previous data to identify and safely exploit identified device vulnerabilities. Once access has been obtained, focus turns to escalation to identify total business impact.

Detailed, risk prioritized report with remediation outline

5. Assessment Reporting

Once the engagement is complete, Rhino Security Labs delivers a detailed analysis and threat report, including remediation steps. Our consultants set an industry standard for clear and concise reports, prioritizing the highest risk vulnerabilities first.

ABOUT RHINO SECURITY LABS

Rhino Security Labs is a top penetration testing and security assessment firm, with a focus on web applications, cloud/AWS, network, mobile apps and phishing testing. With manual, deep-dive engagements, we identify and demonstrate security vulnerabilities which put clients at risk.

Endorsed by industry leaders, Rhino Security Labs is a trusted security advisor to the Fortune 500.

info@RhinoSecurityLabs.com | 888.944.8679

464 12th Ave, Suite 300 | Seattle, WA 98122