praetorian

DATA SHEET

IoT Penetration Testing

KEY BENEFITS

Assess the IoT ecosystem, from backend systems and business processes to hardware and mobile devices

Identify security risks associated with design, implementation, and manufacturing

Receive solutions to mitigate identified vulnerabilities

YOUR CHALLENGE

Your organization's products transmit data over the Internet, and severe vulnerabilities can arise anywhere along the transmission flow from the hardware itself to backend systems or other data aggregation points. You need assurance that your data and that of your clients is as secure as possible every step along the way, and that your products meet any applicable industry regulatory requirements.

OUR SOLUTION: CAPABILITIES OVERVIEW

Praetorian's Internet of Things practice follows data flows that begin at hardware devices and terminate in a backend cloud environment, potentially transiting mobile devices, WiFi access points, or cellular gateways along the way. We can orient an assessment around an established industry or government standard—such as OWASP ISVS, the IIC Industrial IoT Security Framework, or FDA requirements—or create a customized threat model for the device in question. Either way, our team uses a creative approach to identify attack paths to critical assets.

For each engagement, our engineers review source code (subject to availability), API specifications, and technical standards or whitepapers to understand where weaknesses are likely to arise, and tailor their testing accordingly. We then use tools–both commercially available and bespoke from Praetorian Labs–to identify vulnerabilities, demonstrate attacks, analyze protocols, and enumerate the attack surface.

- **A core of hardware security.** Our engineers use your exemplar hardware to simulate usage conditions and carefully tap into debugging, network, or wireless interfaces. This provides us a detailed understanding of the device's inner workings and how it might be attacked.
- **Optional destructive testing.** Depending on your security needs, the team can perform optional destructive testing to exploit the exemplar hardware more thoroughly.
- **Optional backend attacks.** Praetorian can scope an engagement to include attacks against both data in transit and data at rest in the backend cloud environment. Our engineers have expertise related to numerous IoT PaaS and cloud IoT registries, as well as the asynchronous messaging systems commonly used in conjunction with them.

SPECIFIC SERVICE OFFERINGS

Design Advisory

- Threat Modeling
- Secure Design Advisory
- Program Maturity Analysis

Security Testing

- Hardware Penetration Testing
- Firmware Analysis & Reverse Engineering
- Wireless Protocol Analysis
- Supply Chain Security Review
- Network Traffic Analysis

Compliance Assessments

- CVE “CBOM” Analysis
- Primary Controls Verification

WHY PRAETORIAN

At Praetorian, we provide a timely, tailored, and thorough assessment of your product’s cybersecurity from the backend to the user interface and everywhere in between. We have industry-specific experience involving medical devices, automotive security, ICS/SCADA, carrier-grade network appliances, and home automation. You can rely on us to emulate attackers to provide you with an offensive perspective, and provide direct, actionable feedback on what we find. Our team focuses on providing the best possible client experience while partnering with you to strengthen your security posture.

WHO NEEDS THIS SERVICE

- **Device manufacturers:** Companies that design or manufacture connected devices or firmware.
- **Device users:** Organizations in the process of deploying connected devices as part of their critical infrastructure.
- **PaaS providers:** Companies that develop IoT infrastructure for use by device manufacturers.

SAMPLE THREAT MATRIX

DELIVERABLES

Executive Summary

Concise explanation of engagement goals, significant findings, business impacts, and strategic recommendations

→ Upon request, a letter of attestation

Engagement Outbrief Presentation

Similar to the executive summary, presented to the audience of your choosing

Technical Findings Report

Detailed description of issues and the methodology used to identify them, as well as an impact assessment for each

Praetorian Security, Inc.
6001 W Parmer Ln, Ste 370, PMB 2923
Austin, TX 78727 USA
info@praetorian.com

To learn more about Praetorian, visit: www.praetorian.com

ABOUT PRAETORIAN

Praetorian is an offensive security engineering company whose mission is to make the digital world safer and more secure. Through expertise and engineering, Praetorian helps today's leading organizations solve complex cybersecurity problems across critical enterprise assets and product portfolios.