






Device Security Testing

In-Depth Security Testing for Connected Devices

Connected device capabilities and adoption are growing exponentially, changing the way we engage with our customers and providing significant operational benefits. The nature of low-cost devices makes them vulnerable to large-scale, automated attacks. Connected, or “IoT”, devices have historically been at a disadvantage in addressing common security challenges such as:

- Lack of security in the device design lifecycle
- Inadequate security testing processes
- Need for frequent updates and security patches
- Inability to predict and manage vulnerabilities
- Transfer of sensitive data
- Weak authorization and authentication of devices

How Protiviti Can Help

-  Device Security Assessment
-  Protocol Security Assessment
-  Platform Security Assessment
-  Firmware Reverse Engineering
-  Advanced Hardware Attacks
-  New Technology Security Review

Protiviti’s device-specific testing approach helps clients tackle these top device security challenges by identifying security vulnerabilities and potential attack vectors up and down the stack and throughout the device lifecycle. From device documentation review, to physical and interface testing through findings and recommendations, we help you proactively improve your device’s security posture.

Business Value

A comprehensive device security program, including device-specific security testing, reduces risk and provides organizational benefits such as:

- **Data Protection:** Protect device generated data including PII, PHI and intellectual property from cyber criminals’ malicious intents.
- **Data Privacy:** Secure sensitive user data from cyber criminal exploitation and reduce regulatory risk.
- **Operational Resilience:** Minimize business disruption from compromised network connected devices and prevent exfiltration of sensitive information.
- **Consumer Trust:** Increase consumer trust through a comprehensive device security program.

Device Security Testing

Our Device Testing Services

Device Security Assessment

Test and identify cybersecurity vulnerabilities associated with a given device. With open-source and proprietary tools we analyze the physical interfaces, wireless interfaces, and any firmware identified on the device.

Firmware Reverse Engineering

We reverse engineer a given a firmware image to determine if sensitive data can be exposed including, but not limited to, intellectual property, credentials, PII and/or debug interfaces.

Protocol Security Assessment

Through an in-depth security assessment, we evaluate physical and/or wireless communication protocols focusing on secure end-to-end design, development and deployment best practices.

Advanced Hardware Attacks

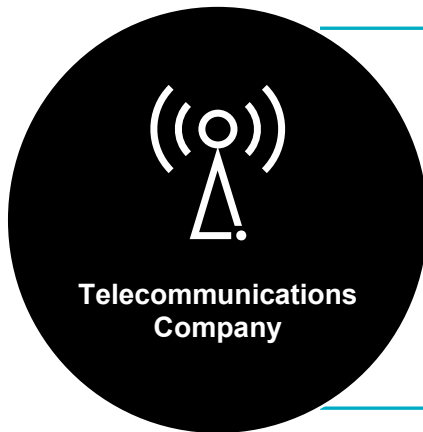
Evaluate the security posture of a device from an advanced hardware testing perspective including voltage and clock glitching, power analysis, cold-booting, chip decapsulation, etc.

Platform Security Assessment

We simulate a real-world threat scenario related to a device and any associated applications, infrastructure, manufacturing facility, etc.

New Technology Security Review

Considering an emerging technology? Protiviti assesses and evaluates the security implications providing product development teams with a detailed overview of the security controls or vulnerabilities.



Business Requirement

With over 1 million untested devices within their fleet, this organization needed to quickly assess if these devices posed risks to their backend network, the devices themselves, or end customers. Any identified risks needed to be mitigated immediately.



Solution Delivered

Through device-specific penetration testing methods, Protiviti discovered several significant vulnerabilities, one of which allowed complete, unauthorized remote control of the devices. The client's full fleet received remote configuration updates, applied risk mitigation techniques and security detection and prevention training for engineers.



Business Results

By identifying the severity of the issue, the client was able to remediate the vulnerabilities and dramatically reduce both legal and reputational risk to their organization. The client achieved comprehensive network security including but not limited to their fleet of devices and future risk exposure was prevented.

Let's Transform Together.



Protiviti.com/TechnologyConsulting



TechnologyConsulting@Protiviti.com



TCblog.Protiviti.com