Hardware Hacking

Threats exist beneath the software layer. We examine firmware, embedded controllers, and connected devices to expose risks that traditional scans overlook. Our hardware specialists use side-channel analysis, chip-level probing, and reverse engineering to protect critical infrastructure and consumer products alike.

FIRMWARE INSPECTION

Extract and dissect device firmware to find hidden backdoors, hardcoded secrets, and insecure update mechanisms. We also evaluate secure boot implementations for bypass risks.

PHYSICAL INTERFACE PROBING

Test debug ports and communication buses - UART, JTAG, SPI, I2C, USB - for unauthorized access paths that let attackers bypass software protections entirely.

WIRELESS & RF ANALYSIS

Assess WiFi, Bluetooth Low Energy, and proprietary radio protocols for pairing weaknesses, encryption gaps, and replay vulnerabilities that could leak data or grant control.

NETWORK & API TESTING

Examine how devices communicate over the network and with cloud backends, checking for weak authentication, unencrypted traffic, and insecure API endpoints.

SIDE-CHANNEL ATTACKS

Leverage power draw, electromagnetic emissions, and timing behavior to recover encryption keys and secrets from chips - techniques often missed by conventional assessments.

FULL IOT ECOSYSTEM REVIEW

IoT security spans more than hardware. We scope assessments to cover device firmware, companion mobile apps, web dashboards, and cloud APIs as one connected system.

WHY BARCODE SECURITY

Hardware flaws often go unnoticed until exploited in the wild. Our engineers combine electrical engineering know-how with offensive security expertise to catch vulnerabilities that software-only testing simply cannot reach.

PROTECT YOUR HARDWARE & IOT. **Request an assessment today.**