CENSUS
Cybersecurity Engineering

DEVICE SECURITY TESTING

WHAT IS DEVICE SECURITY TESTING?

Device Security Testing is a security assessment method that identifies vulnerabilities in electronic devices. During Device Security Testing, security engineers with or without information about a device, attempt to analyze all aspects of the device from a security perspective, and report any identified issues and required countermeasures. The assessment is usually based on reverse engineering methods and covers multiple aspects of the product, such as the product enclosure, hardware architecture, product firmware and device communications.

WHEN IS DEVICE SECURITY TESTING APPROPRIATE?

Device Security Testing examines the whole stack of a product, from hardware to software, thus enabling device manufacturers to address a wide range of security vulnerabilities. Within a Secure Systems Development Lifecycle, Device Security Testing can verify if product components have been integrated and configured securely. Its “black box” approach is also well suited for the investigation of third-party components for which detailed specs might not be available. Finally, when conducted by an independent external entity, it helps build confidence in the quality of the product. This is the case especially in regulated markets (such as the medical device market) where the assessment result is considered an integral part of the pre-market submission material.

CENSUS DEVICE SECURITY TESTING SERVICES

CENSUS provides comprehensive Device Security Testing services covering the complete technology stack of modern electronic devices. Past projects include medical IoT systems, smart meters, ATMs, POS devices, cryptocurrency wallets, access control systems, network security appliances, VoIP phones, mobile phones, SCADA systems, sensors, programmable robotic arms, in-vehicle infotainment systems and semiconductor IP cores.

THE TEAM

CENSUS has invested in building a unique team of experts to analyze the security of electronic devices. The team includes **electronic engineers** capable of inspecting hardware and radio components at a very low level and building custom circuitry to demonstrate novel attacks, **embedded security engineers** capable of analyzing the security of complex embedded system architectures and proposing solutions according to industry standards, and last but not least **software security engineers** with extensive experience in reverse engineering, protocol analysis, code auditing and security testing.

THE LAB

Device Security Testing at CENSUS is conducted in a laboratory environment using specialized equipment for **board assembly/disassembly** (microscope, soldering station, BGA rework tools etc.), **radio analysis** (SDR equipment, NFC/RFID/Bluetooth analysis equipment, GSM network simulation equipment etc.), **signal analysis** (oscilloscope, logic analyzer etc.), **interface analysis** (for JTAG, SWD, SWP, SPI, UART, I2C etc. communications) and **custom board development** (Arduino, FPGA, SoC dev. boards etc.).

ENCLOSURE INSPECTION

When considering threat actors that may have physical access to a device, it is essential to investigate which assets become exposed when an attacker opens the device enclosure, but also what attack surface is exposed without opening the product enclosure. During this investigation, CENSUS also examines the effectiveness of tamper-protective controls and/or tamper-evident sealing used in the product.

HARDWARE INSPECTION

Following the mapping of a product's components and their use during device operation, CENSUS proceeds to the investigation of the device architecture, first collecting information through existing interfaces and then interfacing with interesting components through custom circuitry. The goal here is to establish points in the device architecture where the team can draw useful information from (component communications, firmware data, cryptographic secrets etc.), but also points where the team can meddle with the device operation. Meddling with the device state can range from introducing unexpected new data on an interface (or I/O device) and abusing debugging interfaces, to more experimental techniques, such as performing glitch attacks. Through this process, the team identifies vulnerabilities in the hardware architecture that allow an attacker with physical access to the device to compromise its security.

FIRMWARE INSPECTION

Firmware extracted from the device (or delivered by the customer) is examined through manual and automated methods to identify security vulnerabilities. Manual methods include reverse engineering, source code auditing and functional testing, while automated methods include static analysis, dynamic analysis, and fuzz testing. CENSUS brings in its extensive experience in software security assessments to deliver high quality firmware testing services. The testing process prioritizes on critical device components, and typically touches on multiple layers of the codebase, such as the boot loader, main firmware code, device configuration code, OS / SDK code and other third-party code.

COMMUNICATIONS INSPECTION

Modern devices (especially IoT devices) come with a plethora of communication capabilities, such as serial communication (e.g. USB), wired networking (e.g. Ethernet, CAN, MODBUS), wireless communication (e.g. Wi-Fi, LoRa, Zigbee), cellular communication (e.g. GSM, LTE-M) and custom protocol communication capabilities. CENSUS intercepts and examines these communications to report relevant vulnerabilities.

Device Security Testing can be combined with **Software Security Assessment** services to cover other parts of the product ecosystem (e.g. cloud APIs, companion apps), and with **Hardware Design Review** and **Threat Modeling** services to gain early insights on applicable cybersecurity risks.

For more information about the CENSUS Device Security Testing services please visit:
www.census-labs.com

CENSUS
Cybersecurity Engineering
www.census-labs.com

USA
607 Boylston Street, Suite
165L, Boston,
MA 02116
T. +1 8882 029 846
E. usa@census-labs.com

UK
Unit 2.15 Barley Mow Centre
10 Barley Mow Passage
W4 4PH, London
T. +44 1293 324 069
E. uk@census-labs.com

EUROPE
128 A. Siggrou Ave.,
Athens 117 45, Greece
T. +30 2102 208 989
T. +30 2102 208 990
E. eu@ census-labs.com

ABU DHABI
Office 110 - First Floor
Incubator Building
Masdar City, Abu Dhabi
United Arab Emirates
T. +971 8003 110 047
E. uae@census-labs.com

DUBAI
Unit GA-00-SZ-L1-RT-201,
Level 1, Gate Avenue - South
Zone, Dubai International
Financial Centre, Dubai
United Arab Emirates
T. +971 8003 110 047
E. uae@census-labs.com