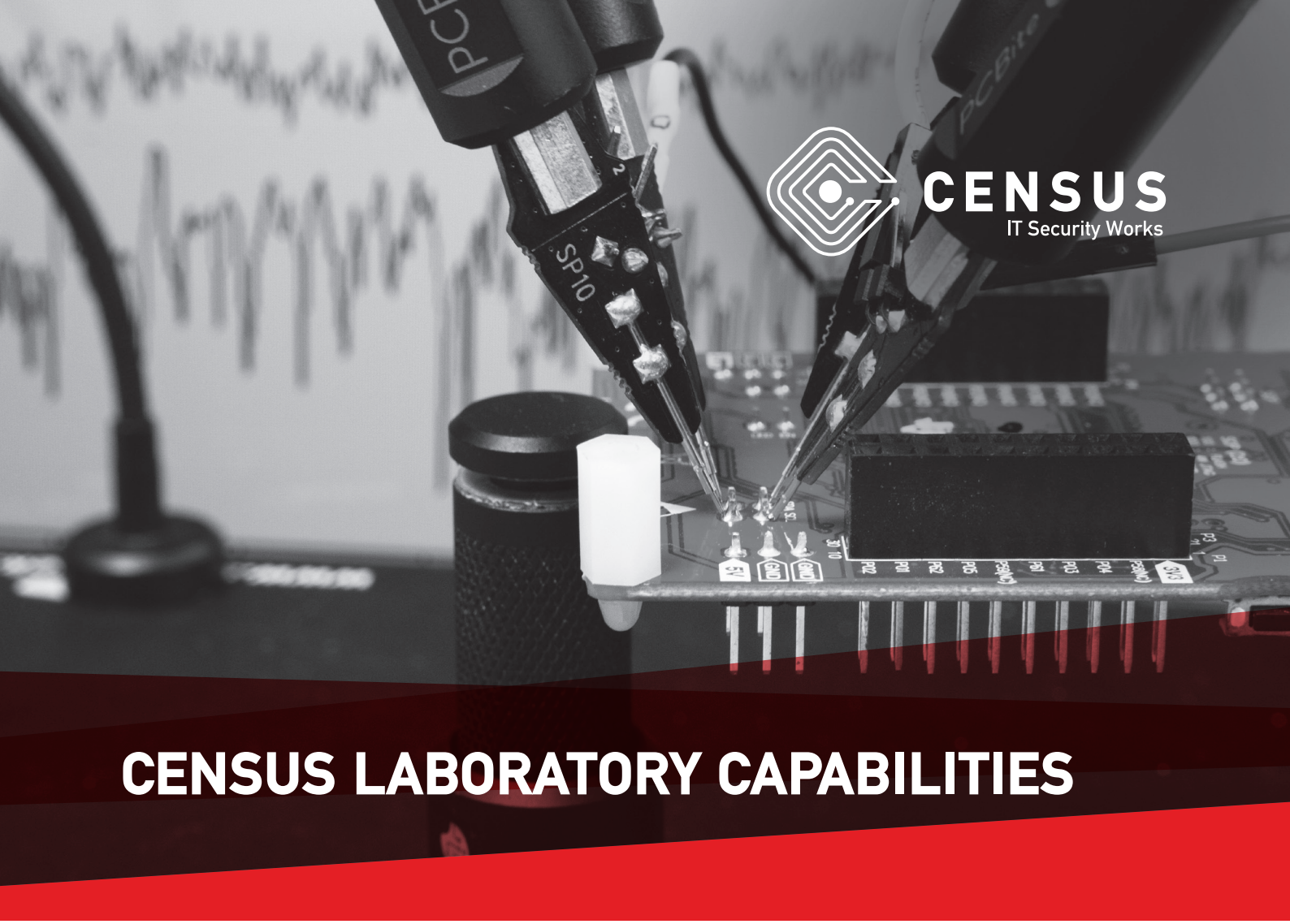


CENSUS LABORATORY CAPABILITIES

INTRODUCTION

CENSUS operates **Hardware and Radio Laboratory facilities** for the security assessment of **electronic devices** and the development of **custom hardware / radio equipment** for use in experiments conducted during the CENSUS security assessment services.

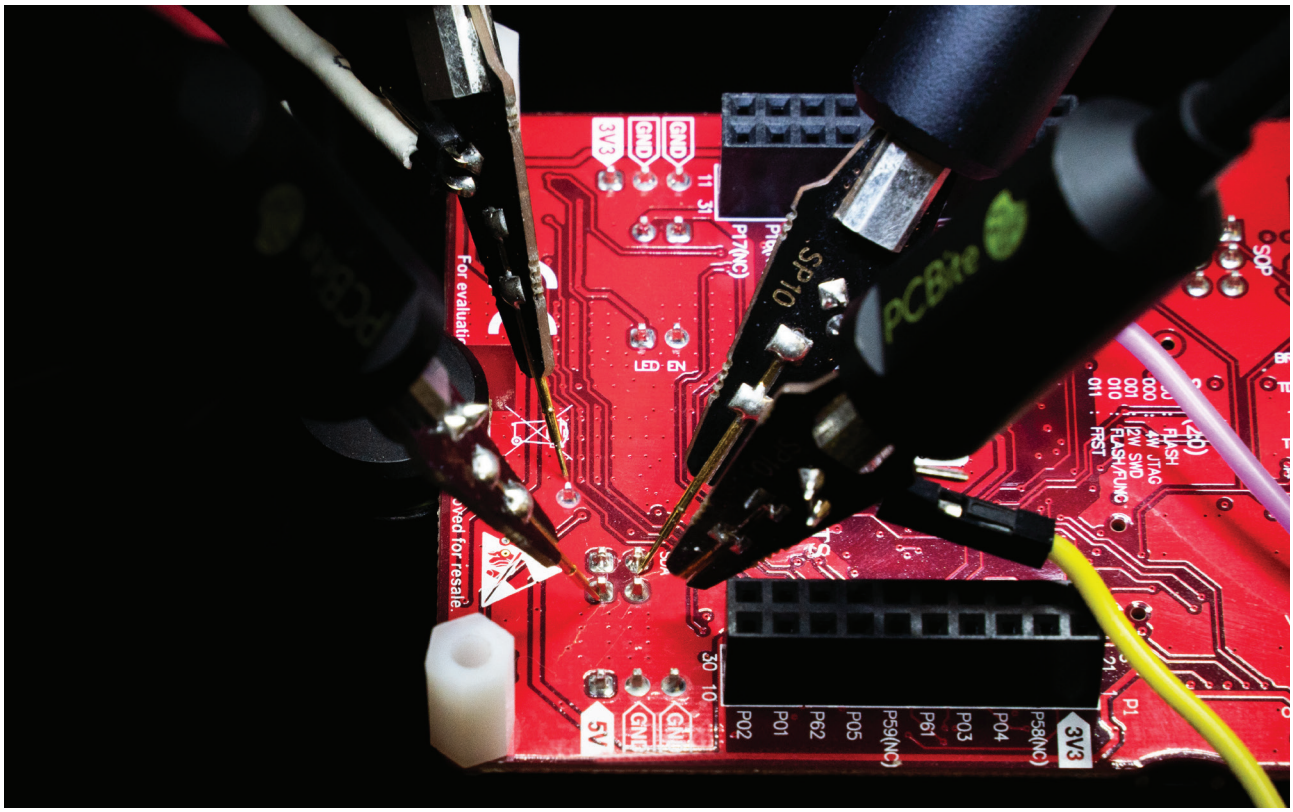
RADIO LABORATORY CAPABILITIES

CENSUS uses its radio laboratory environment to run a series of tests on **radio communications**, including:

- The interception of transmitted data
- The transmission of fraudulent or malicious data
- Man-in-the-middle attacks
- Jamming attacks

These tests enable CENSUS engineers to identify (or reverse-engineer) the low-level **communication protocols** used by devices along with the higher-level protocols that may be used by software running on these devices. Using **specialized SDR (software defined radio)** equipment, CENSUS performs demodulation and decodes information ("symbols") from the captured signals. The communication protocols embedded in this information are then further studied by means of a **protocol analyzer** (or similar custom-developed software).

Once interesting parts of a protocol have been identified, the team creates an **experimental setup** to force the device to yield such a communication. This may be essential for capturing **sensitive data transmitted** in cleartext. The experimental setup may require the introduction of custom development boards (and possibly the interfacing with the device or a device module), the introduction of a testbed network (such as a dummy cellular network), the introduction of an appropriate receiver, the establishment of a common time source, the



triggering of some functionality through software, etc. In some cases, it may be enough to capture the transmitted traffic in the examined device's processor or communication module, rather than after it has been transmitted by the device antenna.

The **transmission of fraudulent or malicious data** may be performed through a similar setup. However, when the transmission involves **black-box fuzz testing activities** (such as GSM fuzzing), it is essential that an efficient setup has been established and that sufficient instrumentation has been applied on the examined communication module. When instrumentation capabilities are not available, CENSUS applies **custom techniques based on feedback-driven approaches** (or based on its reverse engineering / electronic engineering expertise).

Although standard Man-in-the-Middle attacks are carried out with appropriate hardware communication modules (for Bluetooth, WiFi, NFC communications, etc.), custom protocols may require the **processing of signals through SDR.** CENSUS employs both high-end and low-end SDR equipment to weigh on the capabilities that must be available to an attacker in order to **realistically conduct such an attack.**

To limit interference in the laboratory environment, CENSUS uses Faraday cages, while to subject a device to a geographically restricted network (e.g., the network of a mobile carrier in a certain country), CENSUS uses specialized equipment acting as network repeaters.

When testing **organization infrastructure**, it is sometimes useful to examine **radio jamming** attacks. These attacks can tear up fundamental communications channels and may also downgrade the communication quality to non-secure (i.e., backup channel) alternatives. CENSUS prepares in the hardware laboratory specialized boards to carry out signal jamming attacks on the relevant frequencies (and protocols).

Radio-related tests are typically conducted as part of Device Security Testing services to inspect the radio communication capabilities of a device. They can also be useful in Mobile Application Security Tests to examine the **communication of an app with**

other devices over the air (using Bluetooth, NFC, etc.). Product Infrastructure Penetration Testing and assessments of the Organization Security Testing family of services may also include such tests, as parts of the infrastructure possibly communicate over the air (which is often the case in OT environments). Indeed, during Physical Security Testing, it is often useful to inspect an alarm's over-the-air signals to identify potential leakage of sensitive information or remote-control capabilities.

The examination of **WiFi setups and WiFi client configuration,** as well as the introduction of **radio-controlled network implants** to a target network in the context of a Tiger Team / Red Teaming / Penetration Testing engagement may sometimes involve the use of custom-built radio equipment that will guarantee enhanced access capabilities for CENSUS on the target network. The development of this custom equipment is carried out by electronics specialists in CENSUS laboratory environment.

Finally, as part of the **Physical Security Testing** services, CENSUS engineers examine the possibility of forging **RFID / NFC tag transmissions** for tags used in a client's infrastructure for access control purposes. A similar investigation is performed during Device Security Testing when a system is configured (or performs authentication) through such a tag or similar key fob device.

HARDWARE LABORATORY CAPABILITIES

The hardware laboratory environment supports the inspection of a **device's security architecture** and the **rapid prototyping of custom hardware** for use in multiple security assessment domains.

During **Device Security Testing** services, the engineers use the laboratory equipment to:

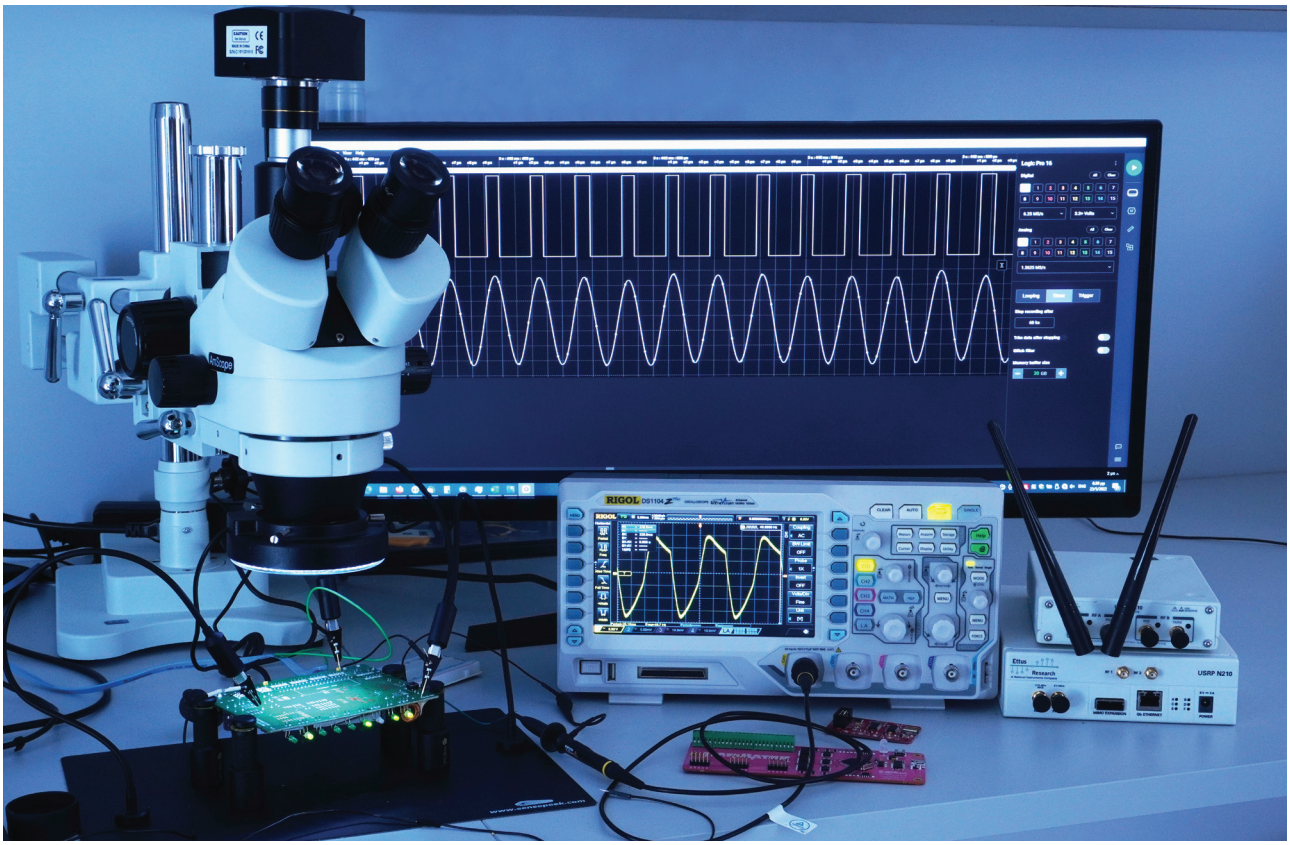
- Inspect the enclosure of a device, enumerating the exposed I/O interfaces and investigating the existence of **anti-tamper mechanisms.**
- Identify information regarding the device **components**, circuitry, and their use during device operation.
- Inspect inter-chip **communication protocols** (e.g., SPI, I2C, UART) by means of an oscilloscope and logic analyzer.
- Interface with the device components through UART, JTAG, SWD etc. connections using specialized equipment (BusPirate, Tigard, J-Link etc.) and dump the related **firmware** (where possible).
- Desolder, if needed, various **types of ICs** (e.g., BGA, SOIC, QFT etc.) and access their memory through specialized equipment (Dataman 48 pro etc.).
- Implement custom circuitry (and software) using embedded development boards (Raspberry, FPGAs, etc.) to inject malicious data or to **fuzz-test** a device's interface.
- Implement custom circuitry (and software) to **power-glitch** a device.
- Implement custom circuitry (and software) to measure indicators for **side-channel information leaks.**

Side-channel and glitch attacks may also be useful in Vulnerability Research to bypass security controls implemented in software.

In Tiger Team, Red Teaming, Social Engineering, and Physical Security Testing engagements, it is often useful to attach a **Human Interface Device (HID)** on a victim's host. This type of device can be designed in the form of a USB dongle, with special communication capabilities build in the hardware laboratory and, once attached to a host, it works as a backdoor to the customer's systems and network.

In similar engagements, there may also be a need for simulating a scenario of **device theft**; In this case, the device is sent to the hardware lab to examine the possibility of hard drive decryption through a set of hardware attacks. A similar exercise may be carried out to test so-called **"evil maid" scenarios** where certain information, software, or even hardware has been altered on the stolen device which, when returned to its original owner, will (upon use) effectively compromise the security of the owner's data.

Finally, in Physical Security Testing services, it may be possible to completely **clone an RFID / NFC tag** used for authentication to a client's infrastructure. The relevant technique may range from a simple attack that can be conducted by an engineer with access to the appropriate equipment to a more elaborate attack (e.g., **side-channel attack**) that requires an **experimental setup** at the hardware laboratory facility.



SUMMARY

The list below summarizes the ways that the various CENSUS services utilize the hardware and radio capabilities of the laboratory environment:

Design Level Review

- Use the hardware / radio lab engineers' experience to conduct design level security review of device architectures and device communications.

Threat Modeling and other Security Documentation

- Use the hardware / radio lab engineers' experience to record **state-of-the-art threats** in a product threat model.

Source Code Auditing

- Evaluate the **exploitation potential** of a finding identified in the source code through experimentation in the hardware/radio lab.

Device Security Testing

- **Inspection** of device enclosure, external attack surface and anti-tamper mechanisms.
- **Mapping** of device components and communications.
- Inspection of inter-chip communications (e.g. SPI, I2C, UART) by means of an **oscilloscope and logic analyzer.**
- Investigation of internal device attack surface.
- **Firmware dumping** (after interfacing through UART, JTAG, SWD, etc.) with device components, using specialized hardware (e.g., BusPirate, Tigard, J-Link etc.).
- Desoldering of various **types of ICs** (BGA, SOIC, QFT, etc.) and memory dumping using specialized equipment (Dataman 48 pro, etc.).
- Capture and reverse engineering of **device communications** through SDR, protocol analyzers, and custom developed software (e.g., Lora, LoraWAN, NFC, Zigbee, wmbus, WiFi, cellular).
- Development of an experimental setup to trigger (and capture) **over-the-air** device communications.
- **Man-in-the-middle** attacks to radio communications through special purpose equipment.
- Recreation of a cellular testbed network for cellular communication testing.

- Capture of device communications through MCU transmitted data.
- Use of custom boards (e.g., custom FPGA / embedded devlopment boards) to efficiently **fuzz device interfaces** (e.g., in-vehicle CAN bus fuzzing).
- Component and firmware instrumentation to efficiently collect fuzz-testing output data.
- Device radio isolation through **Faraday cage**.
- Device radio coverage extension through **repeaters**.
- Peripheral fuzzing (e.g., Bluetooth, NFC, Serial communication, etc.) for **peripherals** compatible with Mobile Apps and Desktop software.
- Setup of **hardware glitch attacks** to circumvent software security controls.
- Deployment of experimental setups to measure **side-channel leaks** in device components.

Application Security Testing

- Investigation of **communications** made by applications to peripheral components (e.g., USB, Bluetooth, NFC, etc.).
- Investigation of **specialized hardware** (e.g., TPM chip) in use by examined system components (kernel drivers, system libraries, etc.).

Product Infrastructure Penetration Testing (and Network and Cloud Infrastructure Testing)

- Development of custom equipment to interface and test **OT networks**.
- Development of custom equipment to interface and test **radio communications** used in a product infrastructure.

Tiger Team, Penetration Testing and Red Teaming

- Simulate the theft of a device (e.g., laptop) and **extract secrets** (e.g., BitLocker key, content from flash memories, data extraction from JTAG interface, inter-chip communication eavesdropping, examination of TPM).
- Copy employee RFID tags that are used in **access control** of buildings.
- Capture and analyze wireless authentication data in order to penetrate the **corporate wireless network.**
- Prepare **custom, in-house developed, hardware devices** for specialized attacks (e.g., HID attacks for users).
- Prepare custom equipment to act as "**backdoors**" to the client network.
- Development of custom equipment to conduct **jamming attacks**.

Mobile Application, Client-side Software and MDM Testing for Organizations

- Peripheral communication investigation and **fuzz testing** (for Bluetooth, NFC, USB communications, etc.).
- Setup of **hardware glitch attacks** to circumvent software controls.
- Investigation of **specialized hardware** (e.g., TPM chip) in use by examined system components (kernel drivers, system libraries etc.).

Social Engineering

- Prepare custom, in-house developed, hardware devices for **specialized attacks** (e.g., HID attacks for users).
- Inject **tampered firmware** in employee devices (e.g., for "evil maid" attacks).

Physical Security Testing

- Copy employee RFID tags that are used for **access control** in buildings.
- Lock picking & magnetic **locks bypass**.
- Circumvention of physical anti-tampering protection mechanisms (**anti-tamper switches**).
- Development of custom equipment to interface and test radio **communications made by alarm systems**.

Vulnerability Research

- Deploy custom hardware and software to efficiently **fuzz-test low-level system components**.
- Setup of **hardware glitch attacks** to circumvent software protections.
- Deployment of experimental setups to measure **side-channel leaks** in device components.

For more information regarding CENSUS services and examples of its laboratory capabilities, please visit: www.census-labs.com

CENSUS
IT Security Works

www.census-labs.com

USA
607 Boylston Street,
Suite 165L, Boston, MA 02116
T. +1 617-448-5050
E. usa@census-labs.com

EUROPE
128, Leoforos Andrea Syggrou,
11745, Athens, Greece
T. +30 210 220 8989-90
E. eu@census-labs.com

UK
4th floor, The Pinnacle,
Station Way, Crawley RH10 1JH
T. +44 (0) 1293 763 336
E. uk@census-labs.com