CENSUS
IT Security Works

WATER METER CASE STUDY

The present document describes activities performed and results obtained through a security assessment carried out by CENSUS on an Industrial IoT system. Any information considered as identifying has been omitted intentionally in order to maintain confidentiality.

CENSUS conducted a security assessment of a smart residential water meter for a global manufacturer. The assessment was performed as part of the CENSUS Device Security Testing offering. The battery-powered device leveraged ultrasonic technology to collect measurements and supported multiple communication protocols, such as LoRA, SigFox, wMbus and NFC. These communication protocols were used for the remote and nearby control of the device, data collection and firmware updates.

The device vendor was interested in evaluating whether an unauthorized adversary with physical, nearby or remote (i.e. over the network) access to the Industrial IoT system could:

- influence the metering operation,
- influence the water valve operation,
- or steal the vendor's intellectual property.

DEVICE SECURITY TESTING

CENSUS experts performed a security assessment of the complete technology stack of the device, inspecting the product enclosure, hardware, firmware and communications. To carry out this assessment, the experts utilized equipment, tools, processes and technologies of the CENSUS hardware and radio laboratory.

LAB SETUP

CENSUS created a small testbed in the lab for testing the operations of the water meter. The setup would need to ensure that an air-flushed water flow with the required minimum water pressure was present, that the device was functioning correctly under all applicable modes and that metering information was actively collected.

OPENING THE ENCLOSURE

The first phase of a device security assessment concerns the inspection of the enclosure of the device. Taking into consideration that the device is a residential meter, physical access to the device could very well be attainable by adversaries and thus related threats were considered as within the scope of the assessment.

The team investigated which device and vendor assets became exposed when an attacker opened the device enclosure. Furthermore, the assessment investigated whether similar assets were exposed without opening the product enclosure. The enclosure examination revealed that:

- **Sensitive cryptographic material** used for the secure communication over the LoRA protocol, could be captured by gaining physical access to the device, opening the enclosure and interacting directly with the device hardware.

ASSESSING THE HARDWARE ARCHITECTURE

The hardware assessment was conducted in a grey-box manner. The vendor provided CENSUS with the schematics of the device to speed up the hardware reverse engineering process.

The team examined multiple hardware attack vectors that involved directly interfacing with the hardware, meddling with inter-chip communications, and abusing debug interfaces. Off-the-shelf tools and custom-made circuitry were used to uncover secrets (e.g., cryptographic keys), to steal intellectual property (e.g., dump the firmware) and to compromise the integrity of the device operation (e.g., by manipulating meter readings). These tests identified the following issues:

- **The device firmware could be retrieved** through a hardware debugging interface found enabled. Such an action could result in intellectual property theft for the vendor.
- **The device metering function could be modified** in arbitrary ways, through a hardware debugging interface found enabled. This could jeopardize the meter reading integrity along with the device model's metering certification.

INTERCEPTING THE COMMUNICATIONS

Using specialized Software Defined Radio (SDR) equipment, all communication technologies used by the device (incl. LoRA, SigFox and wMbus) were tested against multiple types of attacks, including the interception of transmitted data, the transmission of fraudulent or malicious data, Man-In-The-middle (MITM) attacks, and jamming attacks. An NFC interface that enabled field workers to communicate with the device was also assessed using specialized NFC testing equipment. The testing efforts found that:

- **Lack of read protection** for the NFC interface, would allow adversaries to read non-sensitive data.
- **Lack of write protection** over certain sectors of the NFC interface, would allow adversaries to write non-critical data.

Regarding the other sectors of the NFC chip, password protection was found to be enabled, thus preventing unauthorized write operations. CENSUS performed a password brute-force attack over NFC to assess the password strength, which was found to be sufficient.

ANALYZING THE FIRMWARE

The inspection of firmware started with a black-box phase where the firmware dumped during the hardware assessment phase was reverse engineered and analyzed. This first phase provided the vendor with insights on security issues that could have been discovered (and possibly exploited) by someone that did not have insider information on the product.

On the second phase of the analysis, the team applied white-box (i.e. code-aided) testing, where source code was provided to assist the understanding of certain product components. Access to the firmware source code was beneficial in multiple aspects. It allowed for faster root-cause analysis and validation of any issues previously identified, through reverse engineering or functional testing methods. Furthermore, it allowed for the quick discovery of code artefacts through code review and static analysis, that could not otherwise be identified through functional testing methods. Such issues were:

- **Downgrade to insecure default keys** was found to be possible.
- **Hardcoded keys** were used in multiple modes of operation.
- **Lack of encryption and authentication in the firmware update process,** when this was performed Over-The-Air (OTA) using the wMbus communication medium.

The firmware was found to contain a custom-made security layer for LoRA communications. Two relevant issues that the team identified on this layer were:

- **An anti-replay mechanism could be bypassed** due to an unsigned integer wrapping issue.
- **A remote adversary could potentially execute arbitrary code on the device,** due to a buffer overflow vulnerability.

Testing found that none of the two aforementioned issues were exploitable on the specific device, due to the presence of other controls employed in the codebase. However, as the custom LoRA security layer was shared among multiple products, **the vendor decided to proactively patch** the two vulnerabilities and issue a security hotfix for all of the affected products.

REPORTING

The findings, investigation approaches, testing methods and testing tools were described in a detailed report. CENSUS also conducted a number of presentations, going over the identified issues with the client's development team, highlighting key aspects of the mitigation strategies. Finally, the client received a letter of attestation describing the assessments carried out on the Industrial IoT system.

BENEFITS

Following its Device Security Testing methodology, CENSUS split the security assessment into phases, which helped the vendor understand which part of the engineering process was responsible for the (introduction and) mitigation of each issue.

Different modes of assessment were also used to simulate attackers with and without internal knowledge of the device workings.

The inspection of the device enclosure and relevant controls allowed the vendor to understand which assets should be considered as critical to a device instance and how to best protect them in the case of a physical attack.

The inspection of the hardware architecture provided insights into alternate hardware configuration settings (and technologies) which could have been used to deter low budget attackers with physical access to a device.

The inspection of the device firmware provided the vendor with patterns of vulnerable code which could then be used to identify security issues, not only in the particular model, but also in the firmware of other products of the vendor.

In a similar manner, the inspection of the supported communication protocols suggested both design-level and implementation level work which needed to be carried out across multiple products.

Going over the findings with the vendor, was instrumental in building a pragmatic defense against the identified cybersecurity risks and making the device more resilient to future cybersecurity attacks.

The elaborate process followed allowed the vendor to receive a comprehensive assessment. As all findings were verified by CENSUS, the vendor was able to better prioritize the remediating tasks based on realistic risk evaluations. Finally, the assessment & retesting process, along with its deliverables and attestation letter, allowed the vendor to meet the desired compliance requirements and to better convey both internally and externally the significance of the security program covering the product's lifecycle.

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