CyberDanube:
Smart Meter Pentesting

In-Depth Technical Security Assessments of Modern Smart Meter Hardware

Electrical power grids in context of manufacturing companies as well as private households are connected and managed in a smart way nowadays. Therefore, their protection plays a significant role, not only for business continuity but also for our daily life

Preparation

- Kick-off Appointment
- Typical three hardware devices
- Additional client software or hardware

The preparation phase of a smart meter technical security assessment includes a scope definition during a kick-off appointment. Frame conditions like the number of available smart meters or availability of client software are also clarified during such a meeting. A comprehensive technical smart meter security test contains hardware and firmware security testing as well as security testing of the used (fat) client software, if available.

Technical Assessment

Testing in the Security Lab in Vienna

- Physical Manipulation Testing
  (Alarm Contacts/Tampering Protection)
- Hardware Pentesting
  (Debug interfaces, Microcontroller Glitching, Data extraction)
- Technical Firmware Assessments
- Digital Twins
- Client testing (Fatclient)
- Data connections to cloud

CyberDanube’s outstanding service, namely building a digital twin, has also been leveraged multiple times when testing devices like smart meters. This way, much deeper hidden vulnerabilities can be uncovered in such devices in contrast to testing only on the real hardware.

During the technical assessment of a smart meter device, the full stack from electronic components up to the firmware and client software is tested. This includes testing of tampering protection, debug interfaces on the electronic components with different techniques, reveres engineering of firmware and testing of client software. Moreover, there is an increasing number of smart meter with connections to the Cloud or APIs. Such attack vectors are also covered by the tests if needed by the customer.

Date | Version: 24.10.2023 | 1.0 |
Responsible: T. Weber

Typical Challenges

The smart meter tampering protection sensors are sometimes easily overseen during disassembling the first device. Such protection can be effectively tested on a second device, which is one of the reasons why more than just one smart meter is needed. Other challenges are hardware interfaces and removing/interfacing memory chips from the circuit board. Such issues do not pose a problem for CyberDanube experts in the hardware lab in Vienna.

Typical Findings

- Manipulation Contact bypass
- Insecure Data Storage
- Management Interface Vulnerabilities (Command Injection, XSS)

Unfortunately, most found vulnerabilities in smart meter devices do not differ from other IoT Devices. Vulnerabilities like Command injection, XSS, CSRF, insecure data storage, etc. are omnipresent even in well-known brads. But sometimes, the tamper protections sensor is also weakly implemented and can be bypassed easily, which poses a difference to all other devices.

Experts Contact

Thomas Weber

Founder &
Technical Director

About CyberDanube

CyberDanube is a specialized cyber security company, offering OT, (I)IoT & Embedded Security testing services. CyberDanube provides a unique security toolset & technical consulting, e.g. penetration testing capability with a dedicated hardware lab for in-depth product analysis. With a proven track record in pentesting, research and published advisories including zero-day vulnerabilities, CyberDanube is a trusted authority (CNA) which operates independently from manufactures & investors as trustworthy partner in the security industry.

If you need an Industrial Cyber Security Pentest (e.g. Smart Meter)

Contact us via : ✉ office@cyberdanube.com

This Whitepaper has been inspired by real word projects.