“Practical security analysis of German smart metering systems”

28th September 2021

Rigoev, Ivan, M.Sc.
About SMI - Smart Meter Inclusif project
Our part of SMI project

Work package 4: Security concepts for distributed Smart Grids

4.1. Comparative security analysis

4.2. SMI solutions penetration testing
German SMI systems

- BSI is commissioned by Federal Ministry for Economic Affairs and Energy
- Technical standards have been developed by the BSI together with industry, federal associations, Federal Data Protection Commissioner, Federal Network Agency and National Metrology Institute
Secure communication platform for the Smart Grid

- Transparency of consumption data and privacy compliant transfer of measured data
- Control of consumption and power generation units (load / feed-in management)
SMGW smart metering system architecture
Market participants, their tasks, and types of data
WAN communication
HAN communication scenarios

- HKS1: Bidirectional communication in the HAN with authentication using HAN certificates (service)
- HKS2: Bidirectional communication in the HAN with authentication using a unique identifier and password
- HKS3: Transparent channel initiated by CLS
- HKS4: Transparent channel initiated by EMT
- HKS5: Transparent channel initiated by SMGW
LMN communication

**LMN Local Metrological Network**

**WIRELESS M-Bus**

**METER**

SMART METER GATEWAY

Uncommon HDLC implementation
Transport Layer Security (TLS)

• TLS = Transport Layer Security
  o Client/server protocol
  o End-to-end security
  o Authenticity, confidentiality, integrity

• The TLS protocol is complex
  o Specified in more than 80 non-formal documents (RFCs)
  o Complex protocol messages with deep nesting
  o Rich parameter space (versions, ciphers, extensions, optional features, ...) with dynamic negotiation
<table>
<thead>
<tr>
<th>ClientHello (processed by MatrixSSL)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Handshake Transcript (seen by MatrixSSL)</td>
</tr>
<tr>
<td>Unauthenticated</td>
</tr>
</tbody>
</table>

Random/Ciphers/... Extensions Injected Extensions

### Record payload

<table>
<thead>
<tr>
<th>Lhs -----------</th>
<th>Lhs -----------</th>
</tr>
</thead>
<tbody>
<tr>
<td>ClientHello</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Lhs</th>
<th>Lhs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Record payload</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Original ClientHello</th>
<th>Appended by MITM</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Updated by MITM</th>
</tr>
</thead>
</table>
New TLS server fuzzer based on Response-Guided Differential Fuzzing approach

Stimuli generation algorithms

OpenSSL server instances

BoringSSL server instances

MatrixSSL server instances

mbedTLS server instances

WolfSSL server instances

Test Agent

Responses

Stimuli

Response analysis

No. of Distinct Response Discrepancies

Our original algorithm

NEZHA (original)

Our intermediate algorithm

TLS-Attacker

Test corpus size

0 200K 400K 600K 800K 1M

Practical security analysis of German smart metering systems

Ivan Rigoev

Hochschule Offenburg

Institut für verlässliche Embdedded Systeme und Kommunikationselektronik

Hahn Schickard

28.09.2021
Ivan Rigoev

Practical security analysis of German smart metering systems
28.09.2021

TLS implementation fingerprinting

Client Hello

Possible TLS Servers

True Server

Cipher Suites (60 suites)
Compression Methods: 1
Compression Methods (1 method)
Extensions Length: 10
Extension: ec_point_formats
Extension: elliptic_curves
Extension: SessionTicket TLS
Extension: Heartbeat

OpenSSL
(seq: 1.0.1r)

gnuTLS

wolfSSL

matrixSSL

Hahn Schickard
PPC and conexa SMGW testing results

PPC SMGW
- HAN TLS server implementation GNUtls 3.7.x
- Have working SSH with (public key, password) authentication
- Got SSH user list via malformed package technique (checked on raspberry pi with same dropbear SSH 2017.75)
- Tried different brute force software – hydra is the most fast in this case
- Tried 14 344 407 passwords (in more than 2 months). None is correct

Conexa SMGW
- HAN TLS server implementation mbedtlsls in range of versions from 2.7.x-2.24.x
- Documented Socks5 for HKS3. Accept only “Secure Sockets Layer for SOCKS Version 5” authentication.
- Find undocumented fuzzing protection (tcpwrapped after 25 incorrect TLS client hello messages.)
Other possible attacks. ARP spoofing + MITMproxy for HKS2

HKS2: Bidirectional communication in the HAN with authentication using a unique identifier and password.
Current work. LTE WAN traffic sniffing

CMW500 wideband radio communication tester and 2 other SDR LTE base stations

Raspberry pi with LTE hat
Future plans. Use registered for CLS socks5 proxy to connect to EMP network
Thank you for your interest

• All currently found vulnerabilities belong to the systems information disclosure (no remote code execution, data tampering).
• Consumption data sniffing in HAN is possible only when hackers intrude on a local network.
• Both PPC and Conexa SMGW devices could be deemed secure at the current moment of our research.