

“Practical security analysis of German smart metering systems”

28th September 2021

Rigoev, Ivan, M.Sc.

About SMI - Smart Meter Inclusif project



Artificial intelligence
to support the
proactive
management
of energy
consumption
by end users



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



Federal Office
for Information Security

- 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

government

-  Bundesministerium für Wirtschaft und Energie
-  Bundesamt für Sicherheit in der Informationstechnik
-  Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
-  Bundesnetzagentur
-  **PTB** Physikalisch Technische Bundesanstalt
Bundesforschung und -metrologie

associations & organisations

-  **bdew**
Bundesverband der Energie- und Wasserwirtschaft e.V.
-  **VKU BEE**
Bundesverband Erneuerbare Energie e.V.
-  **BITKOM**
-  **DKE**
VDE DIN
-  **verbraucherzentrale**
Bundesverband
-  **FNN**
-  **ZVEI**
-  **GMS**
-  **bne**
Bundesverband Neuer Energieanbieter
-  **TeleTrust**
Pioneers in IT security.
-  **GdW**
-  **vaim**
Verband der Anbieter von Telekommunikations- und Mehrwertdiensten e.V.
-  **DVGW**
-  **figawa**
Firmen im Gas- und Wasserfach

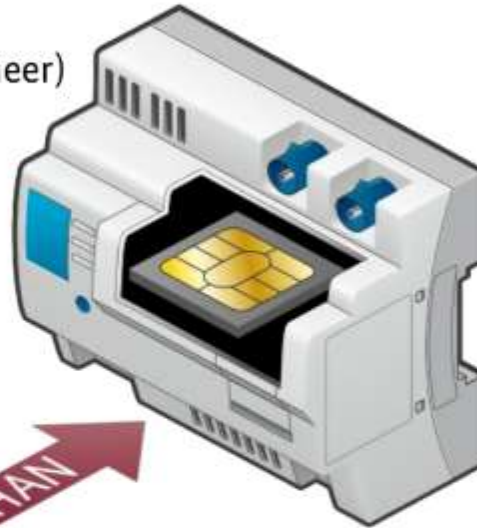
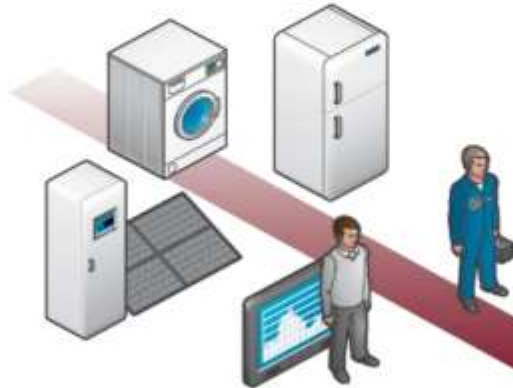
gateway manufacturers

-  **Dr. Neuhaus**
-  **Landis+Gyr**
-  **EMH metering**
-  **devolo**
-  **efr**
-  **PPC**
Power Plus Communications
-  **KIWIGRID**
CONNECTING ENERGY
-  **theben**

SMGW - Smart-Meter-Gateway

Home Area Network (HAN)

Authorized clients (consumers, service engineer)
Controllable Local Systems (CLS)



Wide Area Network (WAN)

Authorized clients (energy and service providers, SMGW Admin)



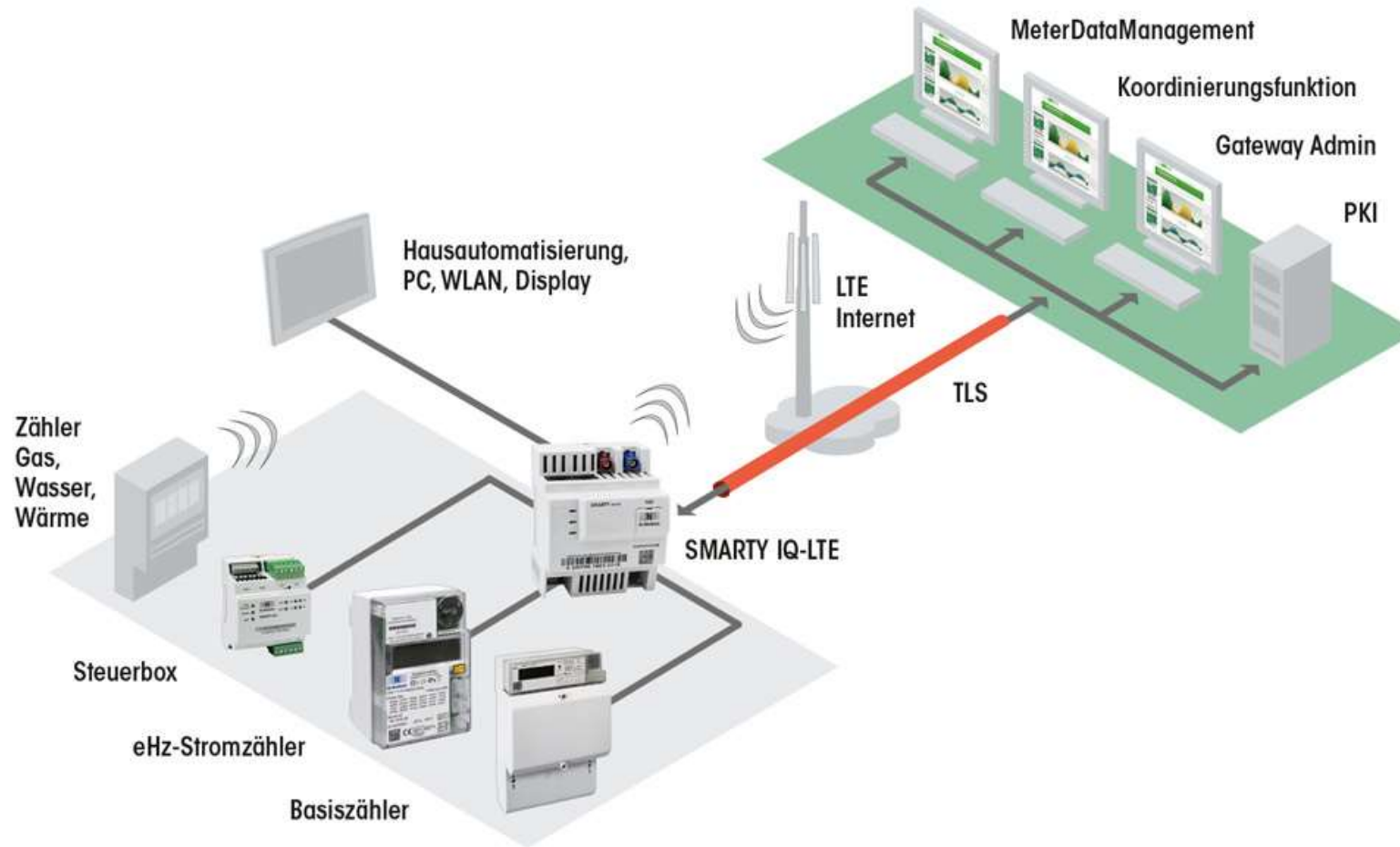
Local Metrological Network (LMN)

Registered meters

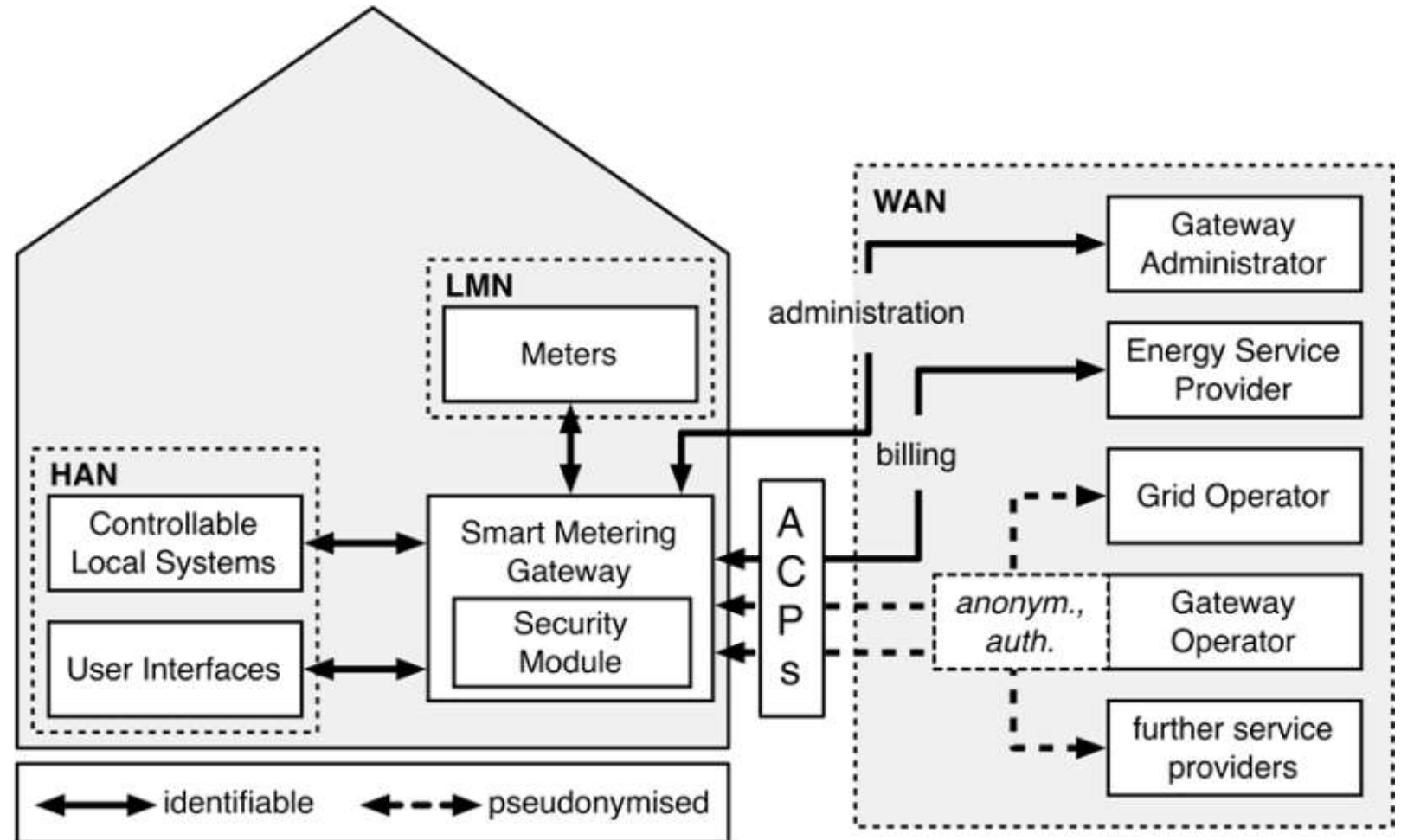
Secure communication platform for the Smart Grid

- Transparency of consumption data and privacy compliant transfer of measured data
- Control of consumption and power generation units (load / feed-in management)

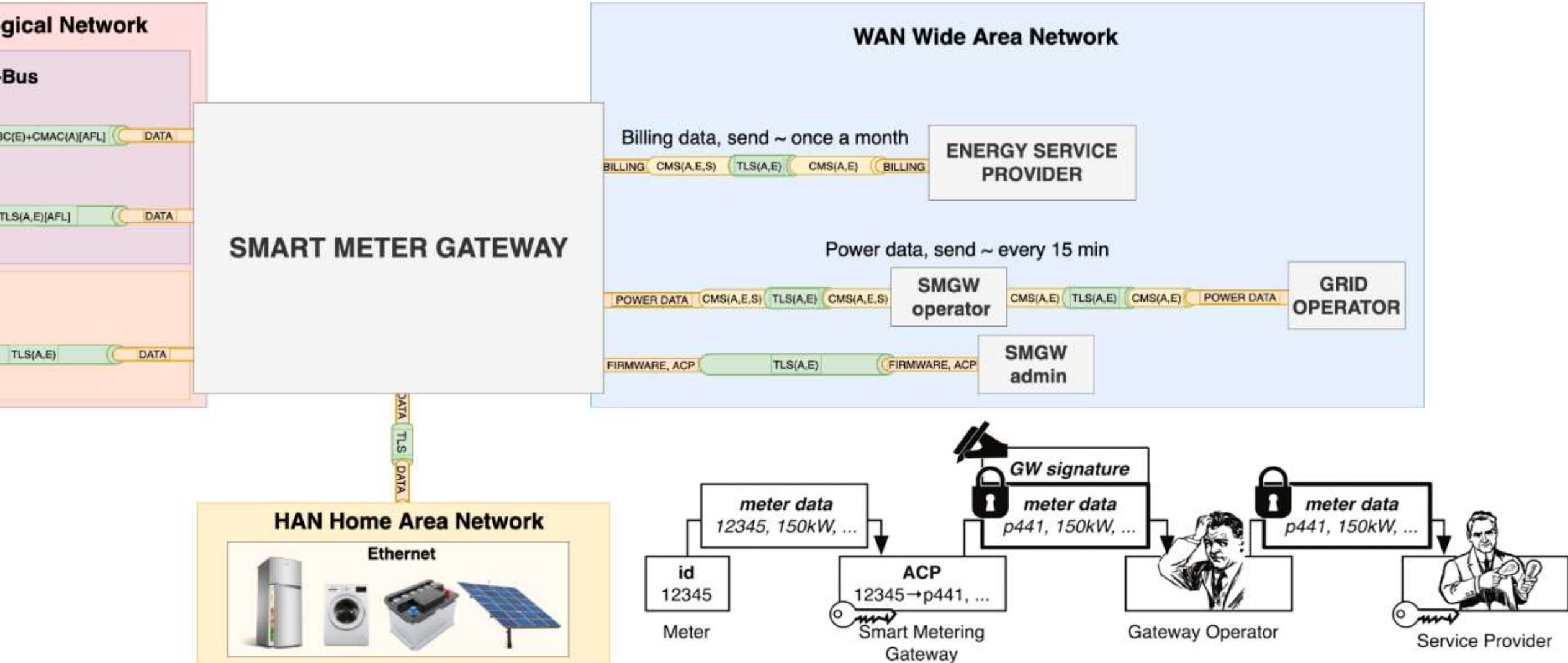
SMGW smart metering system architecture



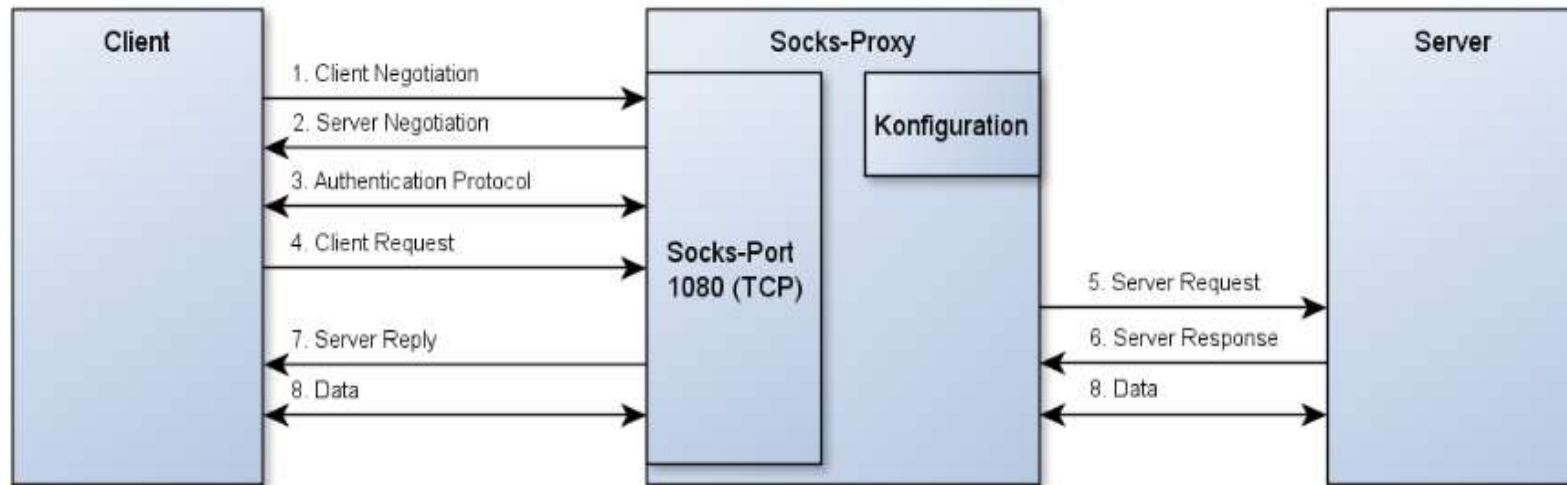
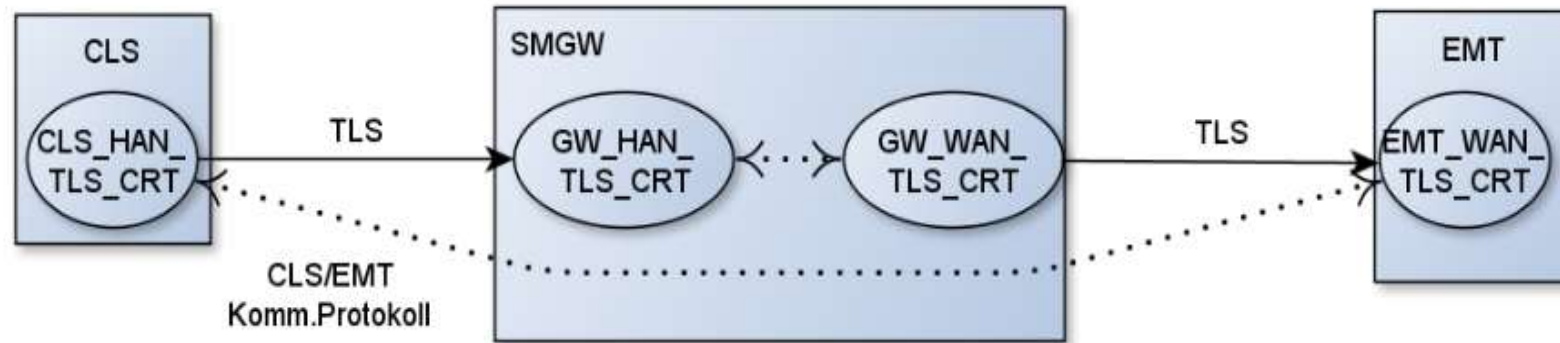
Market participants, their tasks, and types of data



WAN communication

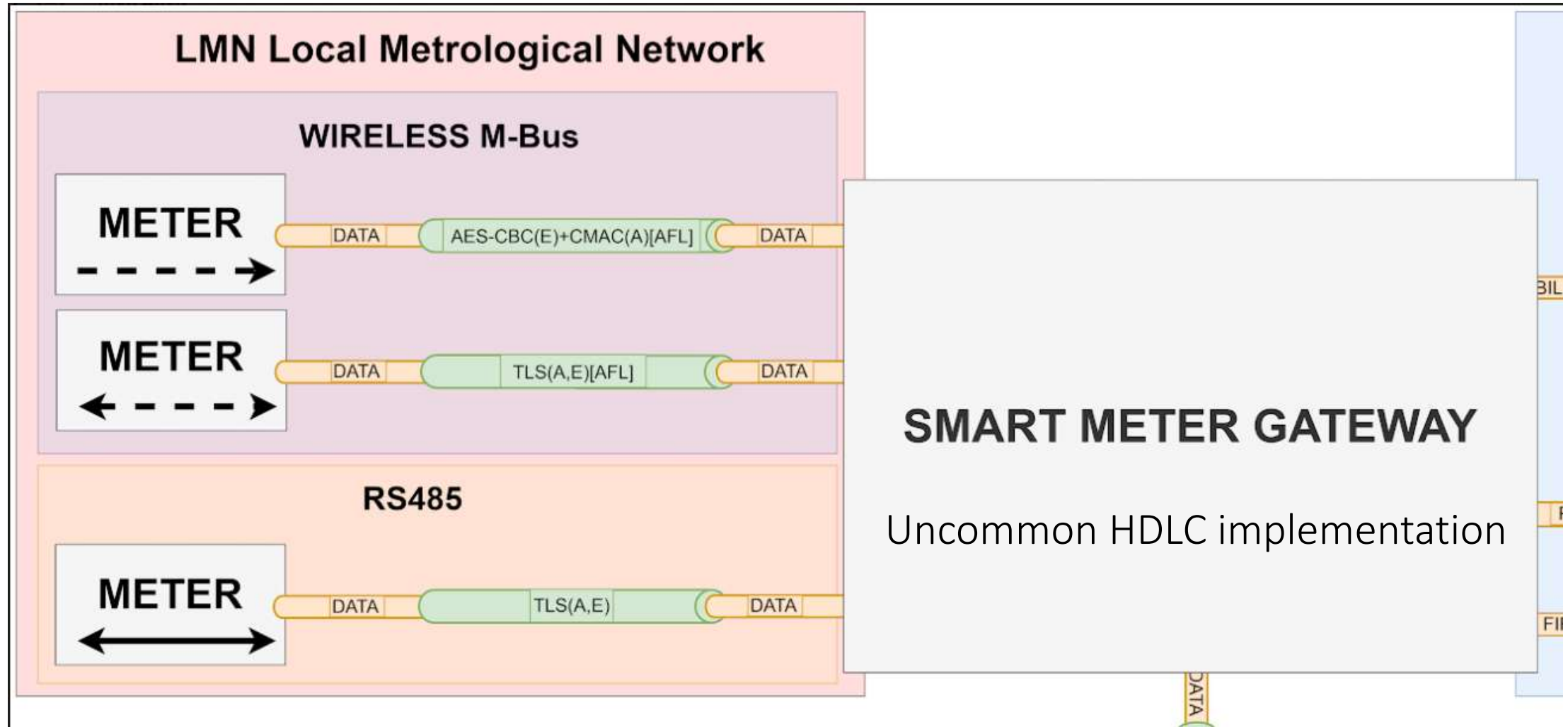


HAN communication scenarios



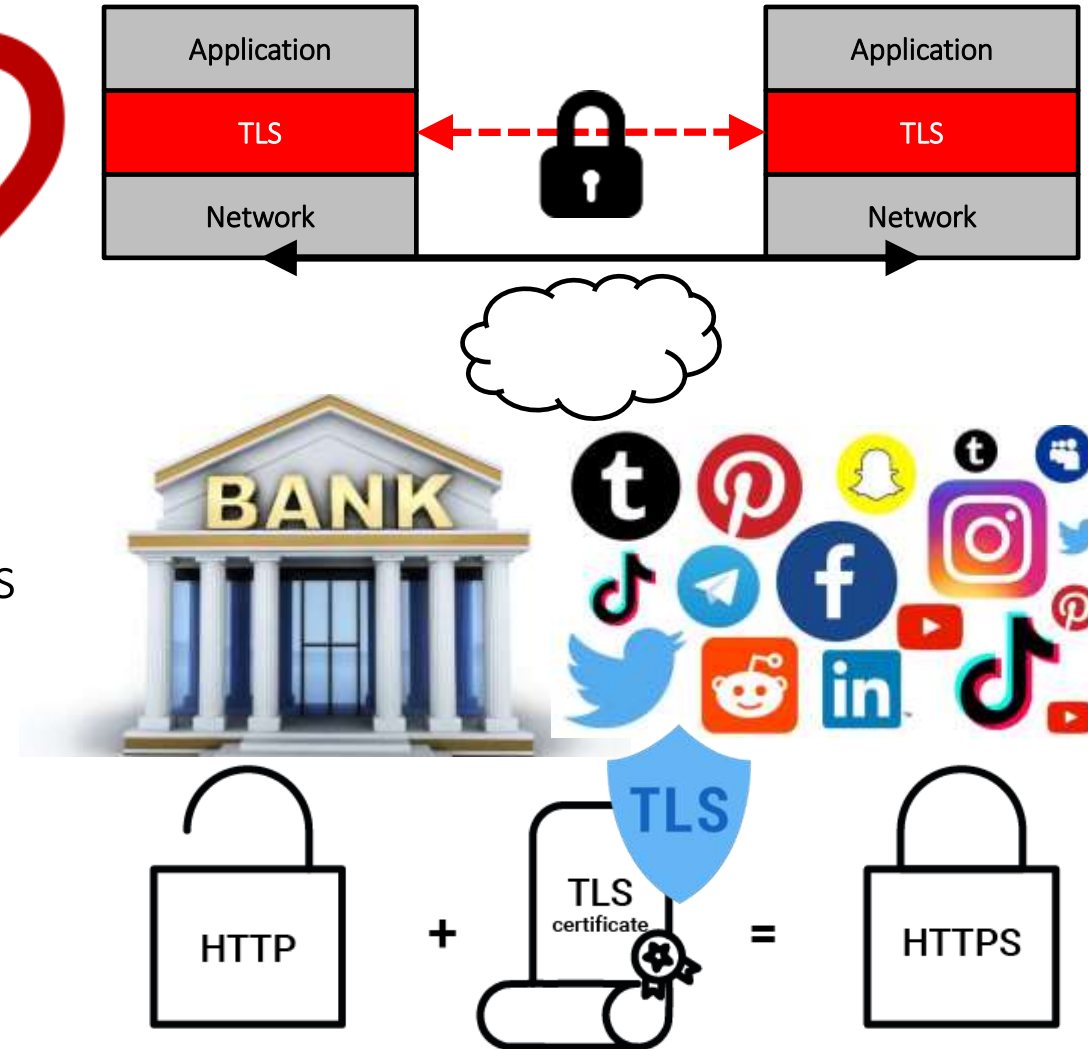
- HKS1: Bidirectional communication in the HAN with authentication using HAN certificates (service)
- HKS2: Bidirectional communication in the HAN with authentication using a unique identifier and password
- HKS3: Transparent channel initiated by CLS
- HKS4: Transparent channel initiated by EMT
- HKS5: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

LMN communication

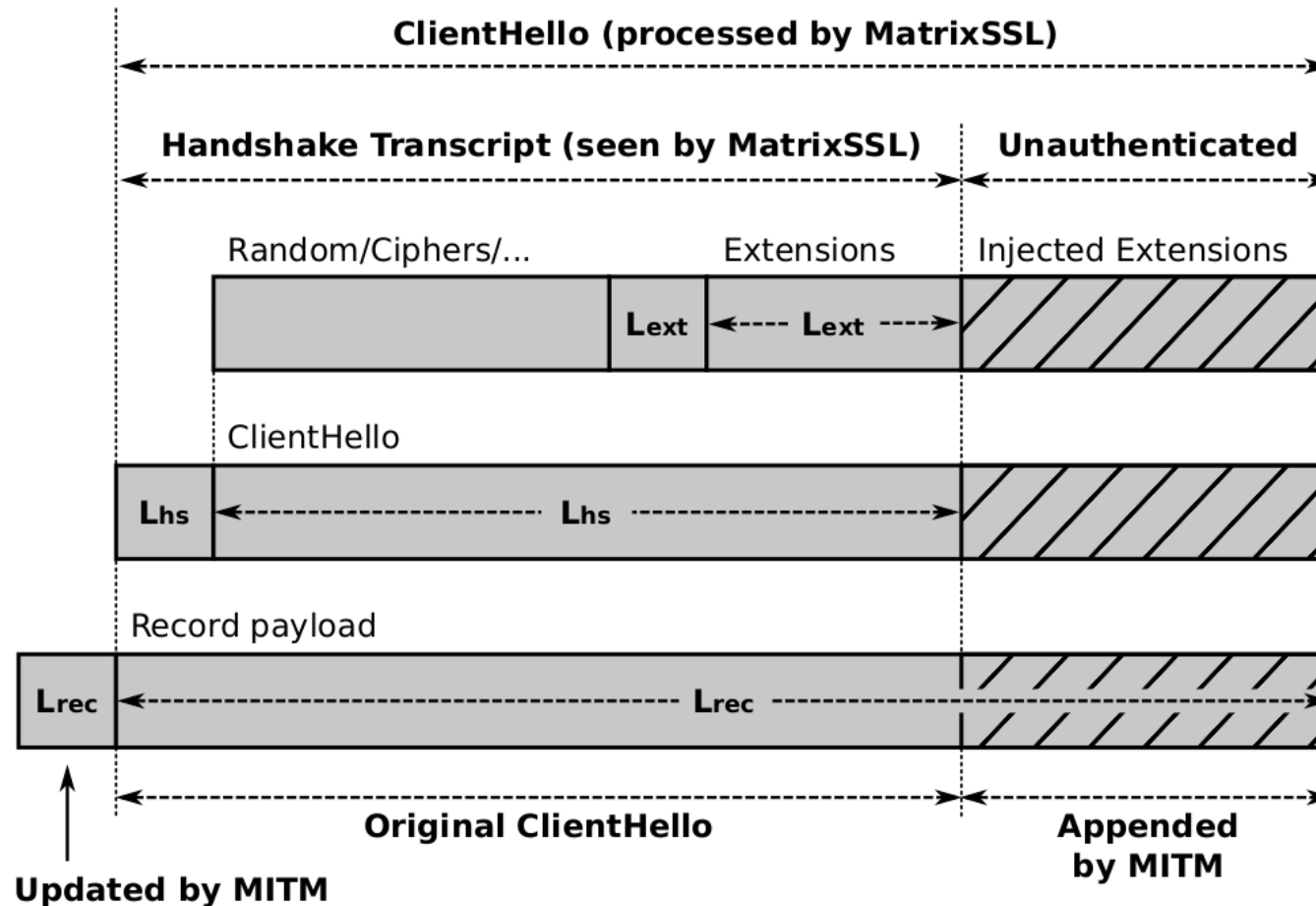


Transport Layer Security (TLS)

- TLS = Transport Layer Security
 - Client/server protocol
 - End-to-end security
 - Authenticity, confidentiality, integrity
- The TLS protocol is complex
 - Specified in more than 80 non-formal documents (RFCs)
 - Complex protocol messages with deep nesting
 - Rich parameter space (versions, ciphers, extensions, optional features, ...) with dynamic negotiation



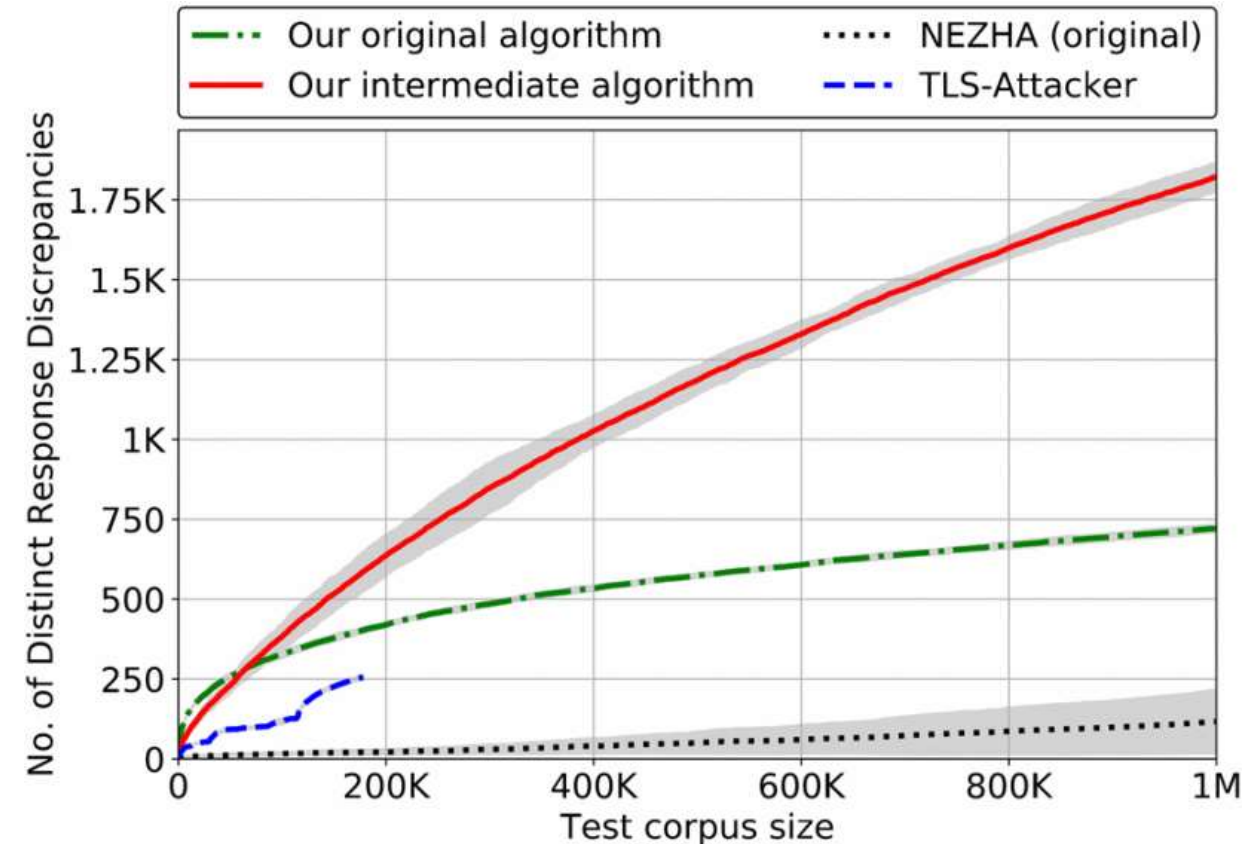
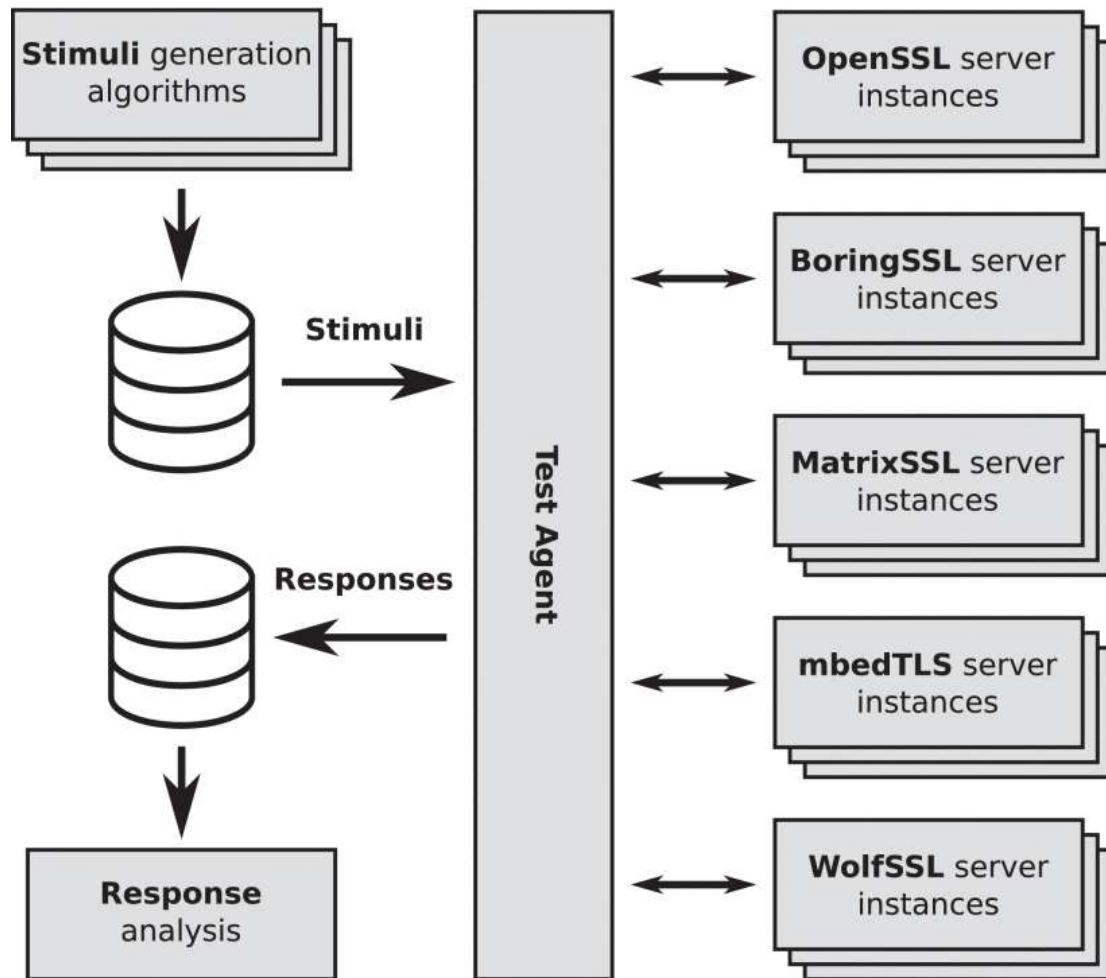
Fuzzing technology



```
Wireshark_Stackexchange.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Hel
Apply a display filter ... <Ctrl-/>

[Checksum Status: Unverified]
Urgent pointer: 0
> [SEQ/ACK analysis]
> [Timestamps]
TCP payload (349 bytes)
Secure Sockets Layer
  TLSv1.3 Record Layer: Handshake Protocol: Client Hello
    Content Type: Handshake (22)
    Version: TLS 1.2 (0x0303)
    Length: 344
  Handshake Protocol: Client Hello
    Handshake Type: Client Hello (1)
    Length: 340
    Version: TLS 1.2 (0x0303)
    Random: 7e4926d7fe2eb42e3de30f088470f1462e0d2e4640997632...
    Session ID Length: 32
    Session ID: a91979b426fc255b35f5be4616bc6bb151d834359857be0e..
    Cipher Suites Length: 2
    Cipher Suites (1 suite)
      Cipher Suite: TLS_AES_256_GCM_SHA384 (0x1302)
    Compression Methods Length: 1
    Compression Methods (1 method)
    Extensions Length: 265
    Extension: server_name (len=24)
    Extension: status_request (len=5)
    Extension: supported_groups (len=18)
    Extension: signature_algorithms (len=30)
    Extension: signature_algorithms_cert (len=30)
    Extension: application_layer_protocol_negotiation (len=14)
    Extension: supported_versions (len=3)
      Type: supported_versions (43)
      Length: 3
      Supported Versions length: 2
      Supported Version: TLS 1.3 (0x0304)
    Extension: psk_key_exchange_modes (len=2)
    Extension: key_share (len=103)
Supported Version (ssl.handshake.extensions.supported_version), 2 bytes
```

New TLS server fuzzer based on Response-Guided Differential Fuzzing approach



TLS implementation fingerprinting

Client Hello

- Secure Sockets Layer
 - TLSv1 Record Layer: Handshake Protocol: Client Hello
 - Content Type: Handshake (22)
 - Version: TLS 1.0 (0x0301)
 - Length: 214
 - Handshake Protocol: Client Hello
 - Handshake Type: Client Hello (1)
 - Length: 210
 - Version: TLS 1.0 (0x0301)
 - > Random
 - Session ID Length: 0
 - Cipher Suites Length: 120
 - > **Cipher Suites (60 suites)**
 - Compression Methods Length: 1
 - > Compression Methods (1 method)
 - Extensions Length: 40
 - > **Extension: ec_point_formats**
 - > **Extension: elliptic_curves**
 - > Extension: SessionTicket TLS
 - > Extension: Heartbeat

Possible TLS Servers



True Server

OpenSSL
(v: 1.0.1r)

PPC and conexa SMGW testing results

PPC SMGW

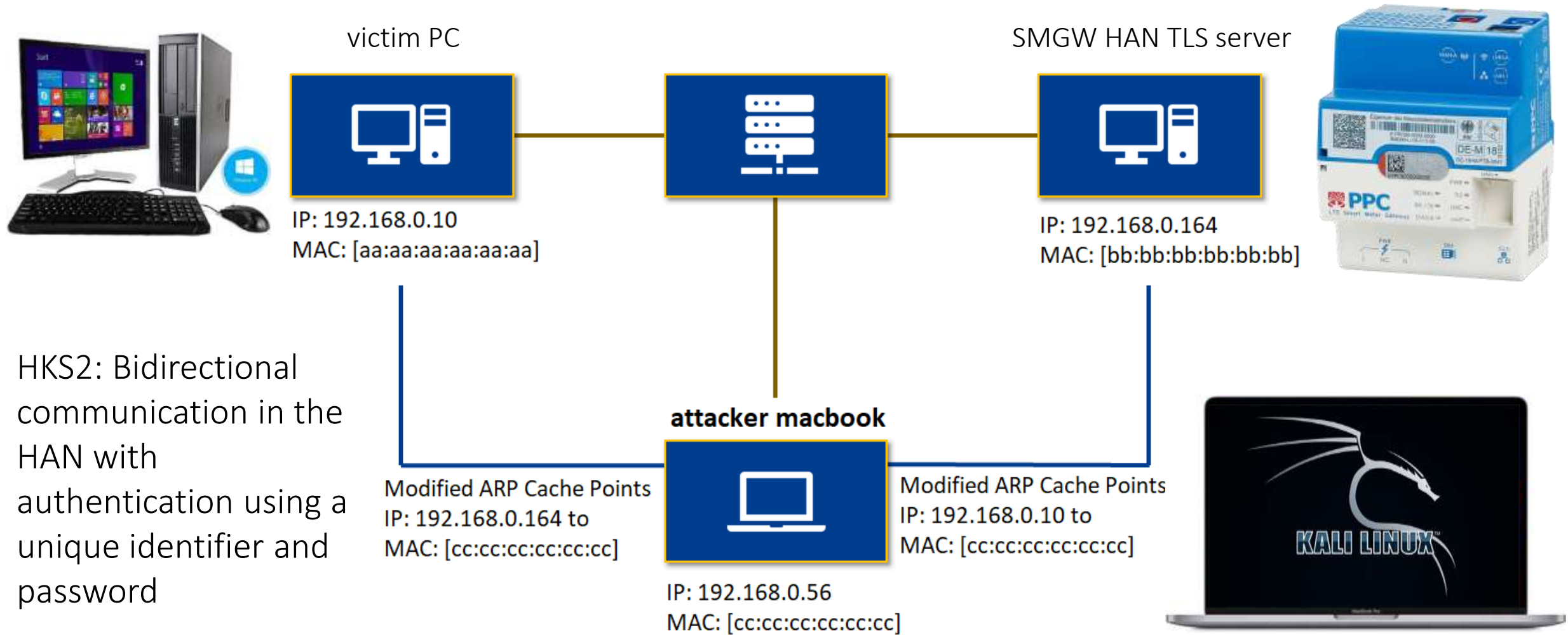
- HAN TLS server implementation GNUTls 3.7.x
- Have working SSH with (public key, password) authentication
- Got SSH user list via malformed package technique (checked on raspberry pi with same dropbear SSH 2017.75)
- Tried different brute force software – hydra is the most fast in this case
- Tried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

Conexa SMGW

- HAN TLS server implementation mbedtls 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

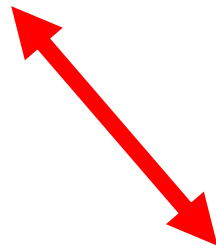


Current work. LTE WAN traffic sniffing



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



Ivan Rigoev

Scientific Employee
Institute of Reliable Embedded Systems and Communication Electronics

Telefon +49 (0)781 205-4713 Badstraße 24
Fax +49 (0)781 205-45 4713 77652 Offenburg
saeed.abdolinezhad@hs-offenburg.de www.hs-offenburg.de



Heiko Bühler M.Sc.

Institute of Reliable Embedded Systems and Communication Electronics

heiko.buehler@hs-offenburg.de Badstraße 24
77652 Offenburg
www.hs-offenburg.de



Prof. Dr.-Ing. Axel Sikora Dipl.-Ing. Dipl.-Wirt.-Ing.

Scientific Director
Institute of Reliable Embedded Systems and Communication Electronics

Telefon +49 (0)781 205-416 Badstraße 24
Fax +49 (0)781 205-45 416 77652 Offenburg
axel.sikora@hs-offenburg.de www.hs-offenburg.de



Andreas Walz

Institute of Reliable Embedded Systems and Communication Electronics

andreas.walz@hs-offenburg.de Badstraße 24
77652 Offenburg
www.hs-offenburg.de

- 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.

