# Energy Fraud and Orchestrated Blackouts

## Issues with Wireless Metering Protocols (wM-Bus)

**Black Hat USA 2013, Las Vegas, July 31st - Aug 1st 2013**

**cyrill.brunschwiler@csnc.ch**

Compass Security AG
Werkstrasse 20
P.O. Box 2038
CH-8645 Jona

Tel +41 55 214 41 60
Fax +41 55 214 41 61
team@csnc.ch
www.csnc.ch

# Agenda

## Intro

- Making Of
- Smart Grids
- Smart Metering

## Wireless M-Bus

- Application
- Protocol Stack
- Communication Modes
- Protocol Overview (Frames, Transport Layer, Data Headers, Relaying)
- Protocol Analysis (Privacy, Confidentiality, Integrity)
- Attack Scenario

## Demo

## Conclusion, Outlook

# Intro

Compass Security AG
Werkstrasse 20
P.O. Box 2038
CH-8645 Jona

Tel +41 55 214 41 60
Fax +41 55 214 41 61
team@csnc.ch
www.csnc.ch

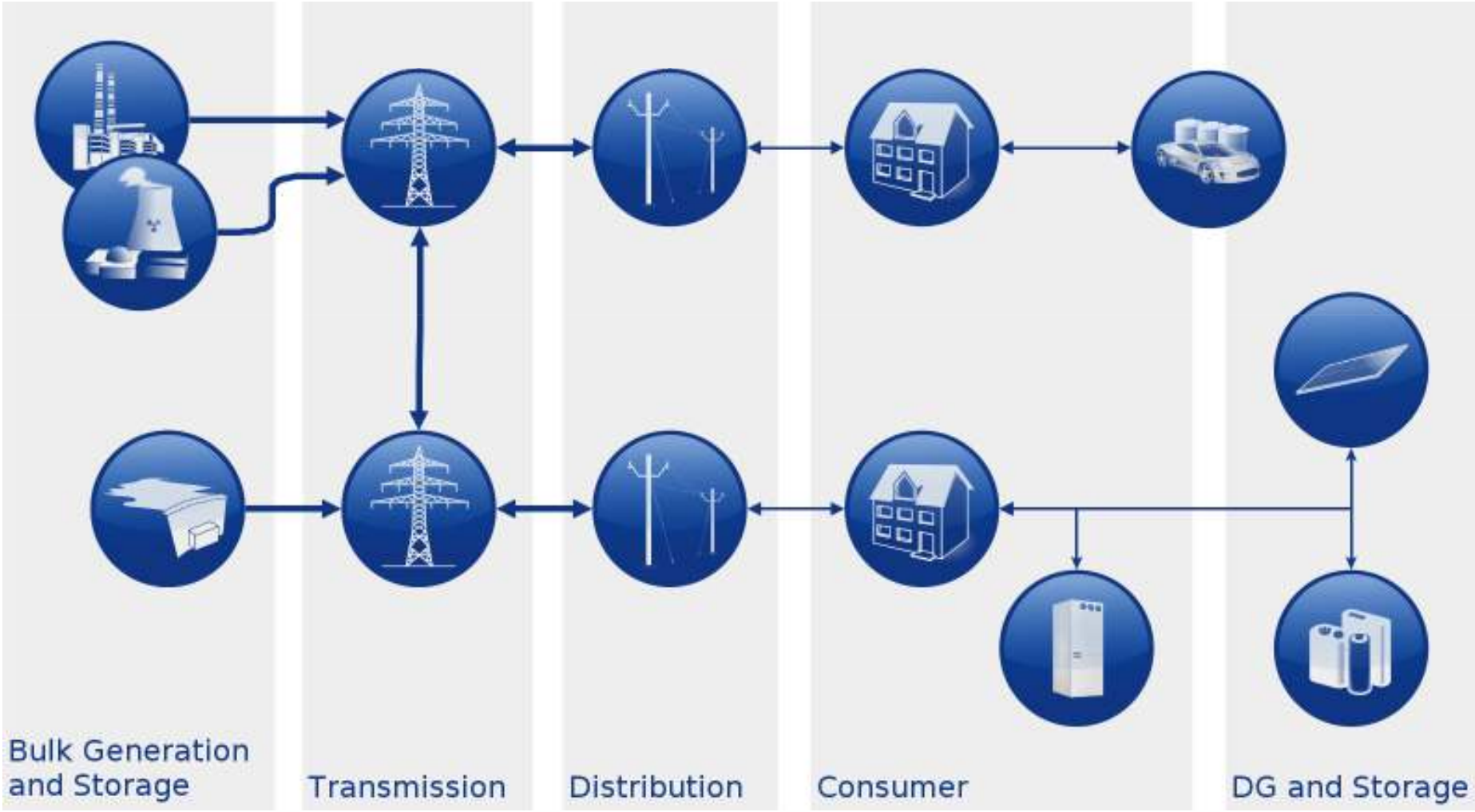
# Intro – Making Of

## Timeline

- Summer 2011: Got attention of wireless M-Bus in smart metering
- Autumn 2012: Started MSc thesis on smart meters and wireless M-Bus
- X-mas 2012: German BSI/OMS group published „Security Report“
- X-mas 2012: Short mention of M-Bus being „inadequate“ at CCC in Hamburg, Germany
- February 2013: Spent some time digging through EN paperwork
- February 2013: Spent some time in an M-Bus lab environment
- March 2013: Finished analysis of M-Bus current resp. draft standards
- March 2013: German BSI mentions wM-Bus security being insufficient
- Summer 2013: Publication at Black Hat USA

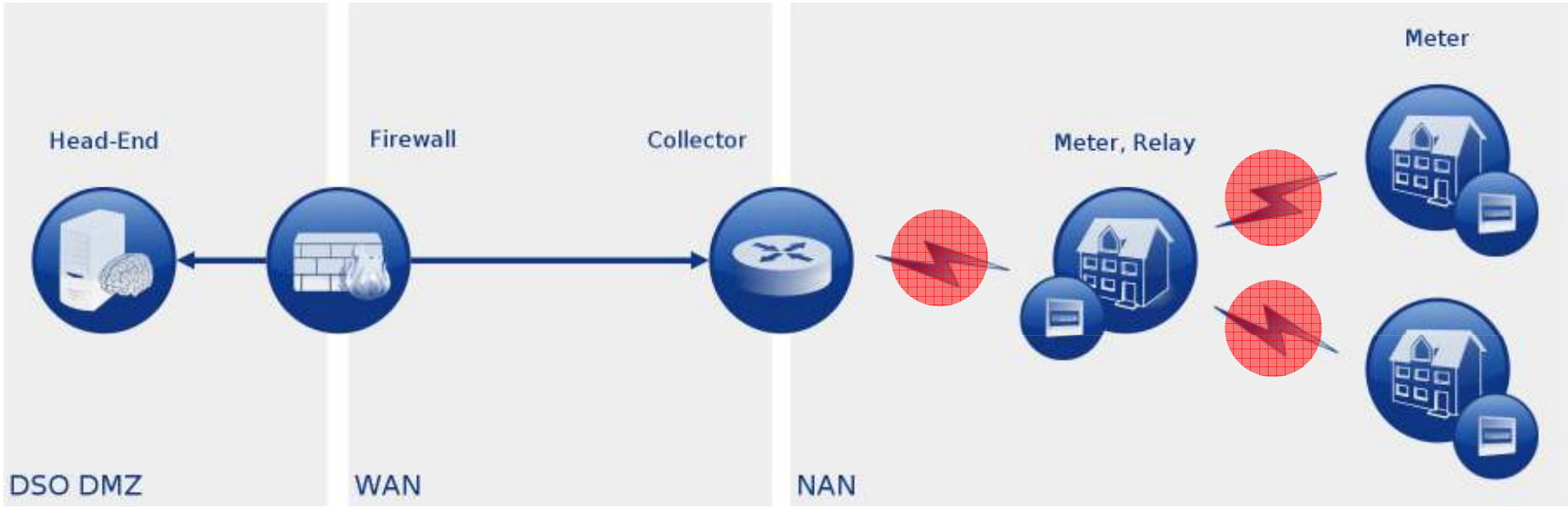
# Intro – Smart Grids

## Smart Grid Blue Print



# Intro – Smart Metering

## Smart Metering Blue Print

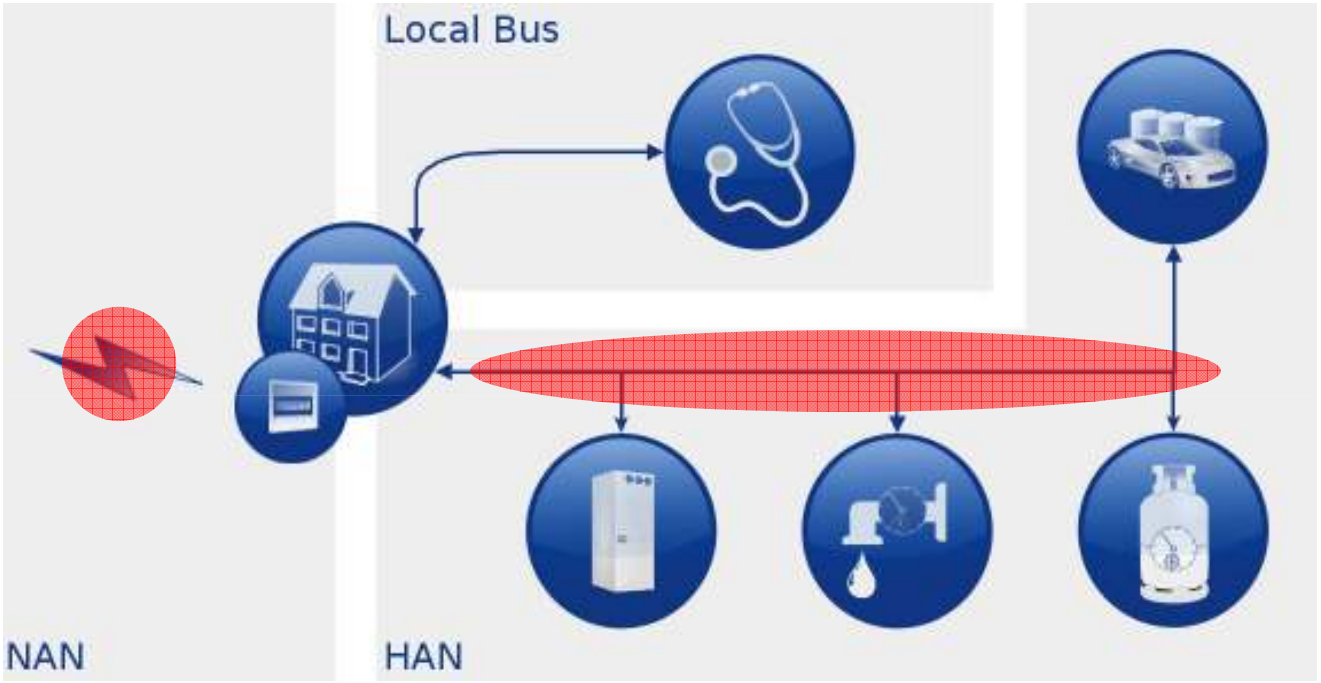



## Legend

- DSO Distribution System Operator
- NAN Neighbourhood Area Network
- Wireless M-Bus

# Intro - Smart Metering

## Home Installation




## Legend

- HAN Home Area Network
- Wired and Wireless M-Bus

# Wireless M-Bus

Compass Security AG
Werkstrasse 20
P.O. Box 2038
CH-8645 Jona

Tel +41 55 214 41 60
Fax +41 55 214 41 61
team@csnc.ch
www.csnc.ch

# Application

## Market segment

- Popular in remote meter reading
  - Heat, Water, Gas, Electricity
- 15 million devices deployed (figures from 2010)
- Mainly spread across Europe

## Usage

- Remote meter reading
- Drive-by meter reading
- Meter maintenance and configuration
- Becoming popular for smart metering applications
  - Tariff schemes, real-time-pricing
  - Demand-response
  - Pre-payment
  - Load-limit
  - Remote disconnect

# Communication Modes

## Modes

- **Stationary Mode (S)** is to be used for communication with battery driven collectors. Specific modes exist for one-way and two-way communication.
- **Frequent Transmit Mode (T)** is optimised for drive-by readout. Mode T does provide specific modes for one-way and two-way communication.
- **Frequent Receive Mode (R2)** allows for simultaneous readout of multiple meters. Mainly used for gateways and drive-by meter reading.
- **Compact Mode (C)** is comparable to mode T but allows for increased data throughput. This is achieved by using NRZ for line coding.
- **Narrowband VHF Mode (N)** is optimised for transmission within a lower frequency narrow band. It is intended for long range repeater use and does specify modes for one-way, two-way and relay communication.
- **Frequent Receive and Transmit Mode (F)** is optimised for long range communication and is also split into one-way and two-way sub modes.
- **Precision Timing Protocol Mode (Q)** provides distribution of time information taking network latency and battery optimised nodes into account.
- **Router based Protocol Mode (P)** changes addressing to include source and destination to allow for real routing

# Protocol Stack

## Involved Standards

| Layer | Standard | Description |
|---|---|---|
| Application | prEN 13757-3 | M-bus dedicated application layer (specified application layer security) |
| Network | EN 13757-5 | Wireless relaying (optional for meters supporting the router approach) |
| Data Link | prEN 13757-4 | Wireless meter readout (specifies link layer security) |
| Physical | prEN 13757-4 | Wireless meter readout (specifies use of 868MHz, 433MHz, 169MHz bands) |

## Legend

- EN European Norm
- pr Draft Standard

# Protocol Overview

Compass Security AG
Werkstrasse 20
P.O. Box 2038
CH-8645 Jona

Tel +41 55 214 41 60
Fax +41 55 214 41 61
team@csnc.ch
www.csnc.ch

# Protocol Overview

## Physical Layer

- Line coding (depends on communication mode)
  - 3 of 6 code (constant-weight code)
  - Manchester coding
  - NRZ coding

## Data Link Layer

- Frames
  - Device addressing
  - Specification of payload (CI field)
  - Cyclic redundancy checks (polynomial is 0x3d65)
  - Types A and B (B has less redundancy checks)
- Extended Link Layer
  - Provides encryption (AES-128 in CTR mode)

# Protocol Overview

## Data Link Layer: CRC calculation using reveng

```
cbrunsch@tortuga: ~/Documents/rhul/thesis/software/reveng-1.1.0
$ ./reveng -h
CRC RevEng, an arbitrary-precision CRC calculator and algorithm finder
```

....

```
         -D list preset algorithms       -e echo (and reformat) input
         -s search for algorithm         -v calculate reversed CRCs
         -h | -u | -? show this help

Copyright (C) 2010, 2011, 2012, 2013  Gregory Cook
This is free software; see the source for copying conditions.  There is NO
warranty; not even for MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.
Version 1.1.0                                 <http://reveng.sourceforge.net/>
$
$ ./reveng -D | grep 13757
width=16  poly=0x3d65  init=0x0000  refin=false  refout=false  xorout=0xffff  check
=0xc2b7  name="CRC-16/EN-13757"
$
$ ./reveng -m CRC-16/EN-13757 -c 01FD1F01
cc22
$ ./reveng -m CRC-16/EN-13757 -c 01FD1F00
f147
$
```

# Protocol Overview

## Data Link Layer, First Block

Example Capture (Sent by meter, CRCs removed)

**1E 44 2D 2C 07 71 94 15 01 02** 7A B3 00 10 85 BF
5C 93 72 04 76 59 50 24 16 93 27 D3 03 58 C8

| Field | Value | Interpretation |
|---|---|---|
| Length | 1E | 30 bytes frame length (exclusive length byte) |
| Control | 44 | Indicates message from primary station, function send/no reply (SND-NR) |
| Manuf. ID | 2D 2C | Coded for Kamstrup (KAM) calculated as specified in prEN 13757-3. ID is managed by the flag association. |
| Address | 07 71 94 15 01 02 | Identification: 15 94 71 07 (little-endian)<br>Device Type: 02 (electricity meter)<br>Version: 01 |

# Protocol Overview

## Data Link Layer, Control Information Field

Example Capture (Sent by meter, CRCs removed)

```
1E 44 2D 2C 07 71 94 15 01 02 7A B3 00 10 85 BF
5C 93 72 04 76 59 50 24 16 93 27 D3 03 58 C8
```

## Types

- Response from device (consumption value …)
- Command to device (open/close valve or breaker …)
- Error from device (cmd unknown, encryption mode unsupported …)
- Alert from device (power low, tamper switches, permanent failure …)
- Time sync (update time service on device)
- Application reset (reset app values, tariff, instantaneous values, calibration…

# Protocol Overview

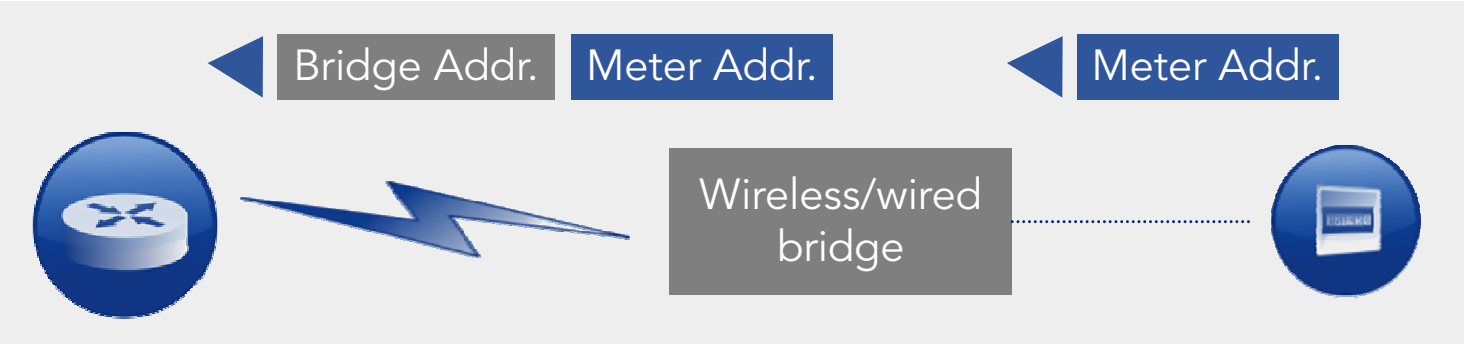
## Network Layer (Relaying)

- Protocol using Routers
  - Allows for full routing
  - Communication mode P
  - Introduces dual addressing
  - Introduces network mgmt functions (maintain routes, detect broken links)
  - Not compatible with EN 13757-5 unaware devices
- Protocol using Gateways
  - Makes use of address translation
  - Supports EN 13757-5 unaware devices
  - Introduces management functions to manage node lists, trusted gateways and end-nodes

# Protocol Overview

## Application Layer (data headers)

- No header
- Short header
  - Indicates access number (frame number)
  - Signals errors and alerts
  - Indicates data encryption supporting several modes
- Long header
  - See short header
  - Additionally propagates a device address
  - Signals addresses behind bridges or virtual devices



# Protocol Overview

## Data Header Example

```
Example Capture (Sent by meter, CRCs removed)
1E 44 2D 2C 07 71 94 15 01 02 7A B3 00 10 85 BF
5C 93 72 04 76 59 50 24 16 93 27 D3 03 58 C8
```

| Field | Value | Interpretation |
|---|---|---|
| Access nrumber | B3 | Current access number is 179. The standard mandates to choose a random number on meter start. The standard suggests to use timestamps and sequence counters since ACC is insufficient to prevent replay. |
| Status field | 00 | Message is meter initiated and there are no alarms or errors. |
| Configuration | 10 85 | Encryption mode is $5_h$ which is AES-128 in CBC mode. $10_h$ indicates a single encrypted block containing meter data (without signature). The field further indicates a short window where the meter listens for requests ($8_h$) |

# Protocol Overview

## Application Layer (data records)

- Data records are structured using data information fields (DIF) and value information fields (VIF) incl. relvant extensions (DIFE, VIFE)

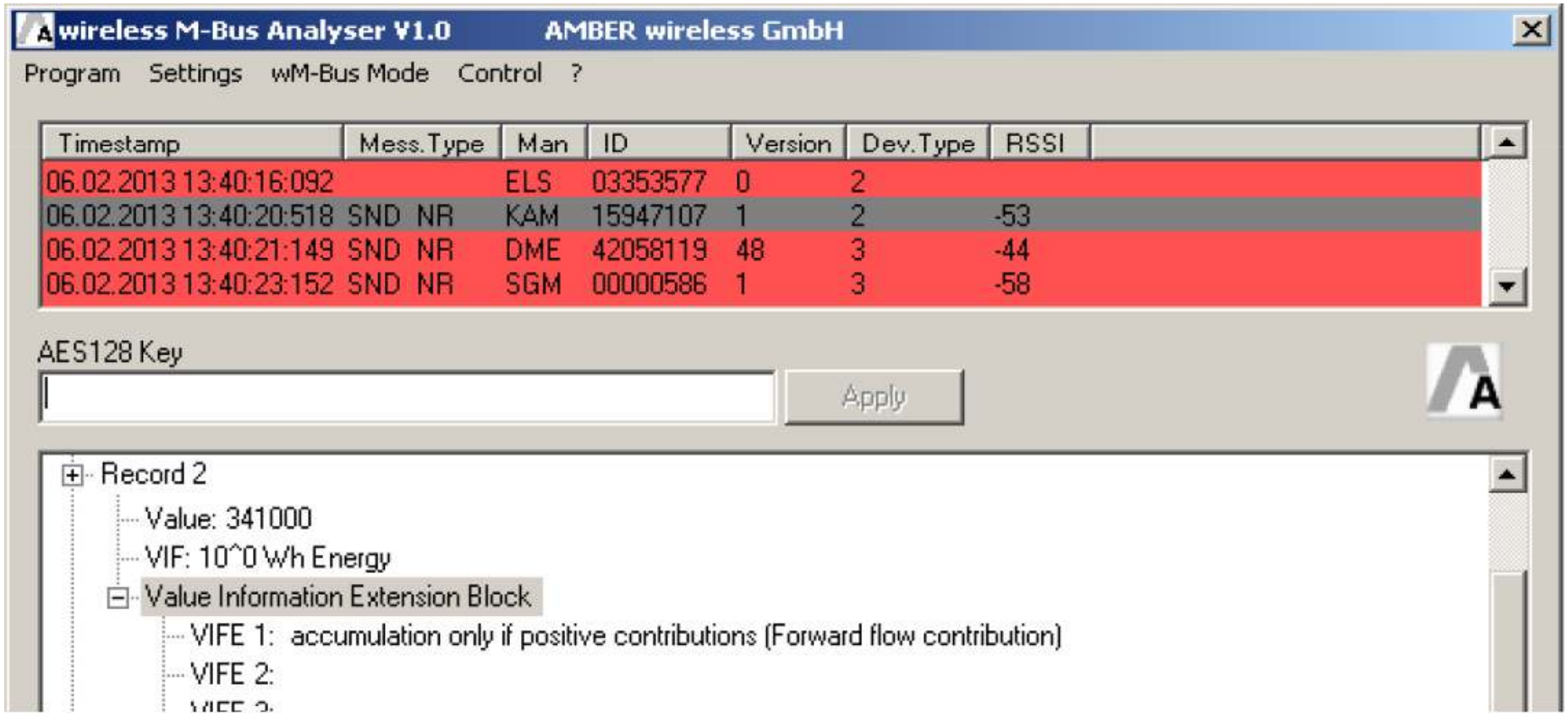
## Data Record Example

```
04 83 3B 08 34 05 00
```

| Field | Value | Interpretation |
|---|---|---|
| DIF | 04 | Instantaneous readout value, no extension fields |
| VIF | 83 | Primary VIF, Unit: Energy $10^0$ Wh, has extension (VIFE0) |
| VIFE0 | 3B | Forward flow contribution only |
| Data | 08 34 05 00 | The value is coded LSB first and it represents a value of 341000 respectively: 341 kWh |

# Protocol Overview

**Protocol sniffers neatly display wireless M-Bus data record contents provided you know the key. The standard suggests "at least 8 bytes of the key shall be different for each meter"**



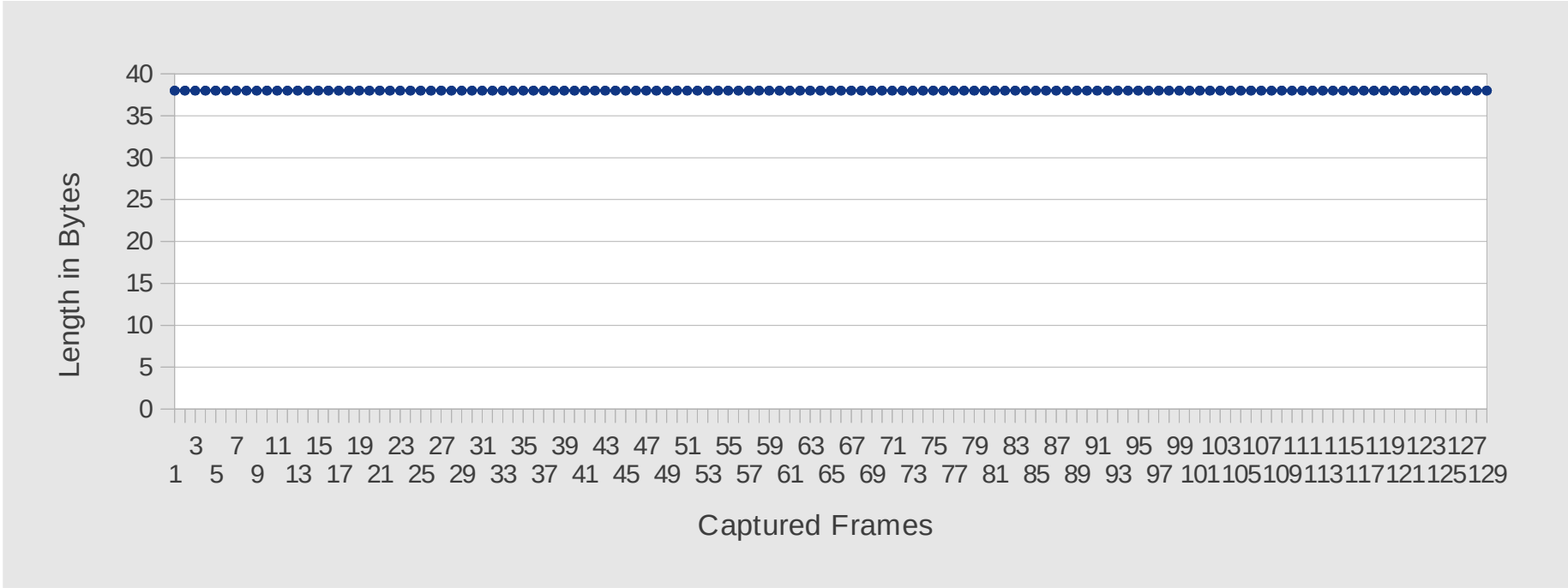
# wM-Bus Protocol Analysis

Compass Security AG
Werkstrasse 20
P.O. Box 2038
CH-8645 Jona

Tel +41 55 214 41 60
Fax +41 55 214 41 61
team@csnc.ch
www.csnc.ch

# Privacy Analysis

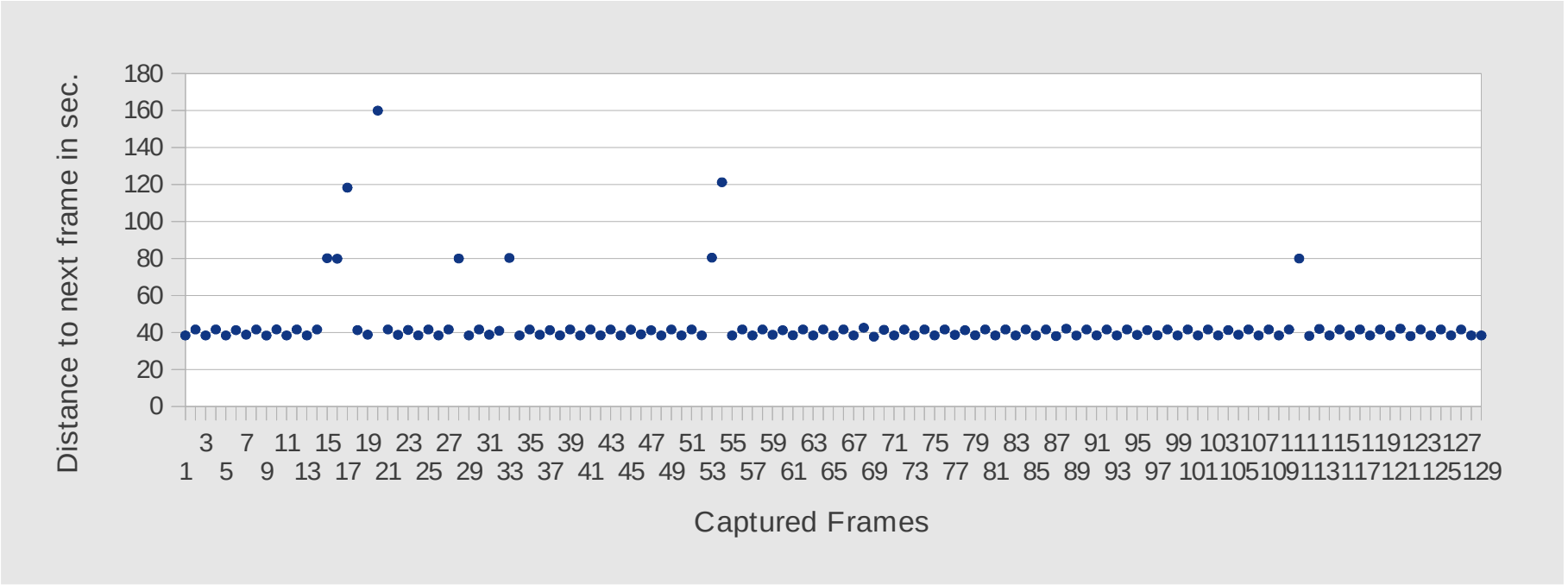
## No privacy issues with packet length




## Adversaries cannot conclude on consumption behaviour by analysing the wireless packet length

# Privacy Analysis

## No privacy issues with transmission intervals




## An adversary cannot conclude on the consumption behaviour by analysing the transmission intervals

# Confidentiality Analysis

## Dedicated Application Layer (DAL) Encryption Modes

- 0 no encryption
- 1 reserved
- 2 DES in CBC mode, zero IV
- 3 DES in CBC mode, non-zero IV
- 4 AES-128 in CBC mode, zero IV
- 5 AES-128 in CBC mode, non-zero IV
- 6 reserved for future use
- 7ff reserved

## Extended Link Layer (ELL) Encryption Modes

- 0 no encryption
- 1 AES-128 in CTR mode

# Confidentiality Analysis

## Padding

- Plaintext is prefixed with the values 2Fh 2Fh
- Padded with 2Fh for the remaining bytes of the block

## Padding Example

```
2F 2F 04 83 3B 08 34 05 00 2F 2F 2F 2F 2F 2F 2F
```

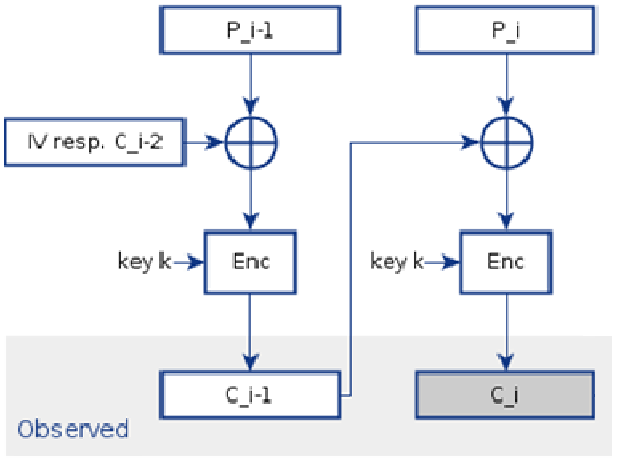
## Padding Oracle

- DIF/VIF structure exactly defines the length of the data record => no need to verify the trailing 2Fs
- Padding Oracle does not apply

# Confidentiality Analysis

## DAL Encryption Mode 4 (AES-128 in CBC mode, all-zero IV)

- Uses static key k
- $C_1 = Enc_k(P_1 \oplus IV)$
  $= Enc_k(P_1 \oplus 00\ 00\ \ldots\ 00\ 00)$
  $= Enc_k(P_1)$
- Equal plaintexts result in equal ciphertexts




## Standard workaround

- Standard mandates to prefix value with date and time record
- Date and time (record type F) maximum granularity is minutes
- User expect response of displays within two seconds

## Side note

- Type I and J records allow for a granularity of seconds

# Confidentiality Analysis

## DAL Encryption Mode 5 (AES-128 in CBC mode, non-zero IV)

- Uses static key k
- IV built from frame info and data header

## Mode 5, IV Example

Example Capture (Sent by meter, CRCs removed)

1E 44 **2D 2C 07 71 94 15 01 02** 7A **B3** 00 10 85 BF
5C 93 72 04 76 59 50 24 16 93 27 D3 03 58 C8

| Initialization Vector (IV) | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Manuf. | | Address | | | | | | Padding with Access Number | | | | | | |
| 2D | 2C | 07 | 71 | 94 | 15 | 01 | 02 | B3 | B3 | B3 | B3 | B3 | B3 | B3 | B3 |

# Confidentiality Analysis

## ELL Encryption Mode 1 (AES-128 in CTR mode)

- Predictable IVs result in 85-bits due to time-memory trade off attacks
- IV in encryption mode 1

| Manuf. | Address | CC | SN | FN | BC |
|---|---|---|---|---|---|
| 2 bytes | 6 bytes | 1 byte | 4 bytes | 2 bytes | 1 byte |

- Half of the IV serves as a salt and limits TMTO to a single device
- CC Signal communication direction, prioritise frames ...
- SN Encryption mode, time field, session counter (4 bits)
- FN Frame number
- BC Block counter

## Keystream repetition in CTR mode

$$P_a \oplus P_b = C_a \oplus C_b$$

# Confidentiality Analysis

## Example of Keystream Repetition (cropped padding)

$P_a$ = 04 83 3B **08 34 05 00** 2F... (341'000 Wh)

$P_b$ = 04 83 3B **14 34 05 00** 2F... (341'012 Wh)

$C_a \oplus C_b$ = 00 00 00 **1C** 00 00 00 00...

## Calculation of consumption difference (0x1C)

```
Max. difference:  0001 1100 = 28
                 -0000 0000 =  0
                            = 28

Min. difference:  0001 0000 = 16
                 -0000 1100 = 12
                            =  4
```

# Confidentiality Analysis

## Encryption in Special Protocols

- Alarms and errors
  - Signalled within status byte
  - Header is not subject to encryption
- Application resets (CI $50_h$)
  - Special upper layer protocol
  - Security services of the DAL and ELL do not apply
- Clock updates
  - Special upper layer protocol
  - Set, add and subtracts (TC field)

| CI | Long Data Header | Check Bytes | TC | Payload | Cmd Verify |
|---|---|---|---|---|---|
| 1 byte | 12 bytes | 2F 2Fh | 1 byte | 9 byte | 2F 2F 2F 2Fh |

# Confidentiality Analysis

**How to get the key stream to repeat?**

- Cause device to reuse the same IV
- If someone could adjust the device time the IV could be repeated
- Time syncs are neither integrity protected nor authenticated

# Integrity, Authentication Analysis

## General

- There are two mention on how one could approach authentication. However there are neither authentication methods nor protocols specified

## DAL Integrity Protection

- CRCs
  - There are CRCs at the frame level
  - CRCs are not considered integrity protection
- Signatures
  - Encryption mode 5 and 6 can signal digitally signed billing data
  - No widely used => due to meter display has precedence in disputes
- MACs
  - Not available

## Manipulation of Ciphertexts or IVs

- In CBC mode, the manipulation of ciphertexts is pointless
- Manipulation of the IV is difficult but feasible

# Integrity Analysis

## Examples of IV (frame header, data header) manipulation

| | B1 | B2 | B3 | B4 | B5 | B6 | B7 | B8 | B9 | B10 | B11 | B12 | B13 | B14 | B15 | B16 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| IV | Manuf. ID | | Device Address | | | | Vers. | Type | ACC | ACC | ACC | ACC | ACC | ACC | ACC | ACC |
| P1 | Leading 2F | | DIF | VIF | VIFE | Consumption Value | | | | Trailing 2F | | | | | | |

## Issues

- Manipulation of manufacturer or address => key not found
- Manipulation of version, type => key not found (receiver specific)
- Manipulation of ACC => destroys trailing 2F (receiver specific)
- What if devices share the same key?

# Integrity Analysis

## Example of Consumption Value Manipulation

$P_1' = Dec_k(C_1) \oplus IV'$

$Dec_k(C_1) = P_1' \oplus IV' = P_1 \oplus IV$

$IV' = P_1' \oplus P_1 \oplus IV$

## In Bits and Bytes

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $C_1$ | C6 | A0 | 79 | B1 | 66 | 0B | BF | 8F | 65 | BC | 4A | 43 | 37 | 8D | DF | BE |
| k | AB | AD | 1D | EA | AB | AD | 1D | EA | AB | AD | 1D | EA | AB | AD | 1D | EA |
| IV | 2D | 2C | 07 | 71 | 94 | 15 | 01 | 02 | B3 | B3 | B3 | B3 | B3 | B3 | B3 | B3 |
| IV' | 2D | 2C | 07 | 71 | 94 | 15 | 01 | **05** | B3 | B3 | B3 | B3 | B3 | B3 | B3 | B3 |
| $P_1'$ | 2F | 2F | 04 | 83 | 3B | **08** | **34** | **02** | **00** | 2F | 2F | 2F | 2F | 2F | 2F | 2F |

- Original value read from meter display 341 kWh (08 34 05 00 )
- P1' 144'392 Wh (08 34 02 00)

# Integrity Analysis

## DAL Expansion Attack

- DAL allows for partial encryption
- How does the receiver handle doubled data records?

## DAL Expansion Attack Example

```
Value in CT: 04 83 3B 08 34 05 00 (341'000 Wh)

1E 44 2D 2C 07 71 94 15 01 02 7A B3 00 10 85 BF
5C 93 72 04 76 59 50 24 16 93 27 D3 03 58 C8

Value attached: 04 83 3B 08 34 02 00 (144'392 Wh)

25 44 2D 2C 07 71 94 15 01 02 7A B3 00 10 85 BF
5C 93 72 04 76 59 50 24 16 93 27 D3 03 58 C8 04
83 3B 08 34 05 00
```

# Integrity Analysis

## ELL Integrity Protection

- CRC at the frame level
- Another CRC at the ELL level (subject to encryption)
- No MACs, no signatures

## ELL CRC calculation

| CRC | | DIF | VIF | VIFE | CMD |
|---|---|---|---|---|---|
| CC | 22 | 01 | FD | 1F | 01 |

# Integrity Analysis

## ELL Manipulation Example

$P_a$ = CC 22 01 FD 1F 01

**$P_b$ = F1 47 01 FD 1F 00**

$C_a$ = E7 8E 1B 7B 9D 86

$C_b = C_a \oplus P_a \oplus P_b$

$C_b$ = E7 8E 1B 7B 9D 86 $\oplus$
CC 22 01 FD 1F 01 $\oplus$
F1 47 01 FD 1F 00

**$C_b$ = DA EB 1B 7B 9D 87**

# Integrity Analysis

## Integrity with Special Protocols

- No integrity protection at all
  - Alarms and errors
  - Application resets
  - Clock synchronization
  - Commands
  - Network management
  - Precision timing

# Key Management Analysis

## Key Management

*"When keys are being supplied or updated, consideration should be given to using the three pass exchange method."*

## Three pass exchange

A => B: $Enc_a(secret)$

B => A: $Enc_b(Enc_a(secret)) = Enc_a(Enc_b(secret))$

A => B: $Dec_a(Enc_b(Enc_a(secret))) = Enc_b(secret)$

# Protocol Analysis

## Man-in-the-Middle attack

A => C: $Enc_a(secret)$

C => A: $Enc_c(Enc_a(secret))$

A => C => B: $Dec_a(Enc_c(Enc_a(secret)))$

B => C: $Enc_b(Enc_c(secret))$

C => B: $Dec_c(Enc_b(Enc_c(secret)))$

## Reflection attack

A => C: $Enc_a(secret)$

C => A: $Enc_a(secret)$

A => C: $Dec_a(Enc_a(secret)) = secret$

# Attack Scenario

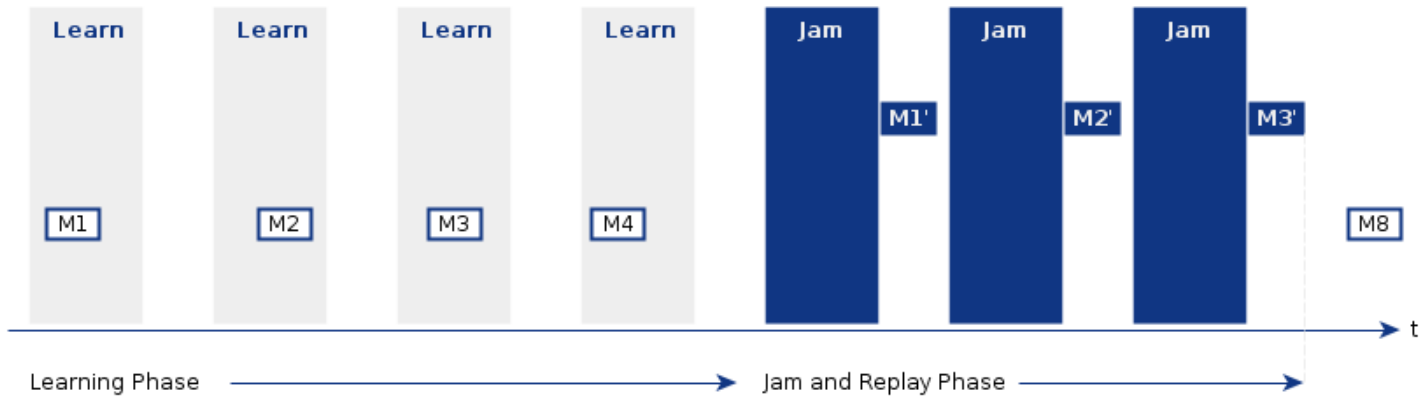
## Man-in-the-Middle

- Network management protocol could be abused to become MitM
- In manually configured nets, only valid relays could be impersonated (shield)

## Shield and Replay

- Capture messages from original device
- Shield device and replay messages
- Shield device, have a receiver with the device and submit manipulated messages to collector

## Jam and Replay



# Demo

Compass Security AG
Werkstrasse 20
P.O. Box 2038
CH-8645 Jona

Tel +41 55 214 41 60
Fax +41 55 214 41 61
team@csnc.ch
www.csnc.ch

# Conclusion

Compass Security AG
Werkstrasse 20
P.O. Box 2038
CH-8645 Jona

Tel +41 55 214 41 60
Fax +41 55 214 41 61
team@csnc.ch
www.csnc.ch

# Conclusion

## Major Questions

- Does wM-Bus defeat eavesdropping and preserve the consumer's privacy?
- Does wM-Bus prevent unauthorised modification of data in transit?
- Does wM-Bus avoid impersonation and man-in-the-middle attack scenarios?
- Does M-Bus ensure proper key management?

## The short Answer

- No, no, no, no

# Conclusion

## The long answer

- The standard recommends to choose half of the key unique to each meter which reduces key size to 64 bits
- Inappropriate key and IV use allows for zero consumption detection
- Inappropriate key and IV derivation may disclose plaintexts including consumption values
- Missing integrity protection allows for manipulation of consumption values in transit
- Missing integrity protection allows for manipulation of valve and breaker open/close commands
- Lack of authentication with clock updates may lead to key stream repetition
- Lack of authentication for network management could allow adversaries to become a rogue relay
- Plaintext error and alarm notifications allow an adversary to recognise if tamper switches have been triggered
- Disclosure of device manufacturer, meter type and version ID simplify identification of vulnerable targets
- Loose specified key update mechanism leads to key disclosure

# Outlook

## Counter Measures

- Efforts of the OMS Group and the German Federal Office for Information Security (BSI Germany)
  - Integrity-preserving authentication and fragmentation layer (AFL),
  - Additional encryption mode relying on AES-128 in CBC mode using ephemeral keys
  - TLS 1.2 support for wM-Bus
  - Published on X-Mas 2012
- Looks promising, no independent public analysis so far

# Battery pack empty.