Energy Fraud and Orchestrated Blackouts

Issues with Wireless Metering Protocols (wM-Bus)

Hack in Paris, June 27th 2014

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

- Smart Grids
- Smart Metering

Wireless M-Bus

- Application
- Protocol Stack
- Protocol Overview (Frames, Transport Layer, Data Headers)
- Protocol Analysis (Privacy, Confidentiality, Integrity)

Demo

- Setup
- Attacks and Issues

Conclusion

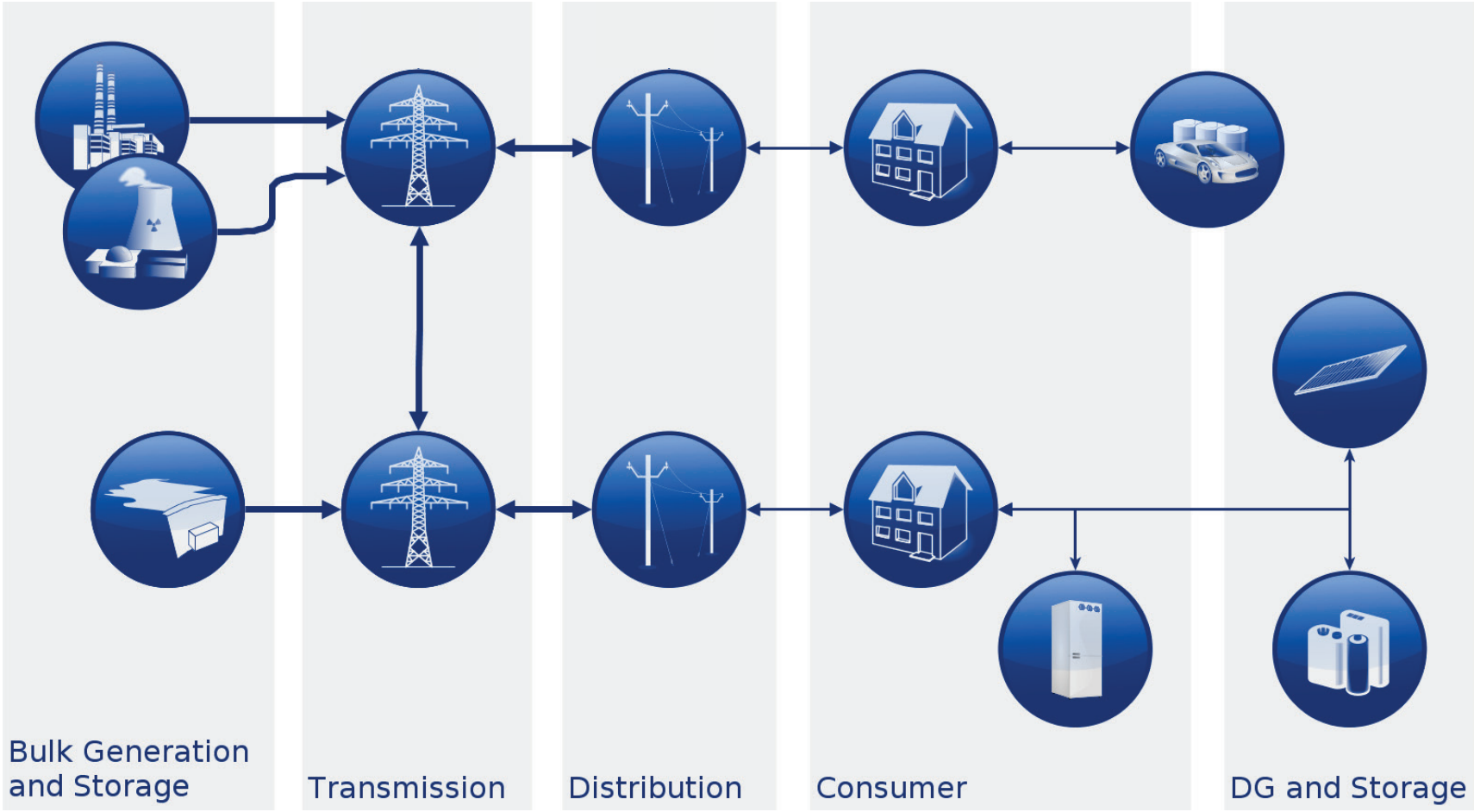
Intro

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

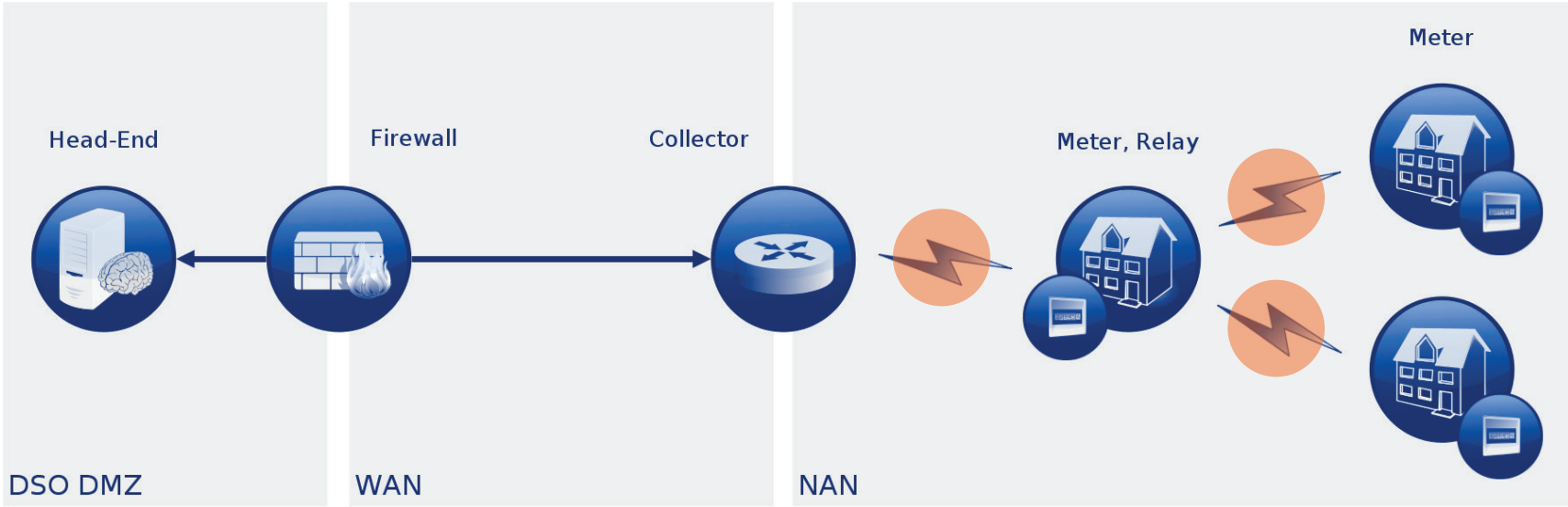
Intro – Smart Grids

Smart Grid Blue Print



Intro – Smart Metering

Metering Infrastructure Blue Print



Legend

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

Intro – Smart Metering – Collector

Collectors

- Various Vendors
- Neuhaus is just an example of a Multi Utility Controller (MUC)

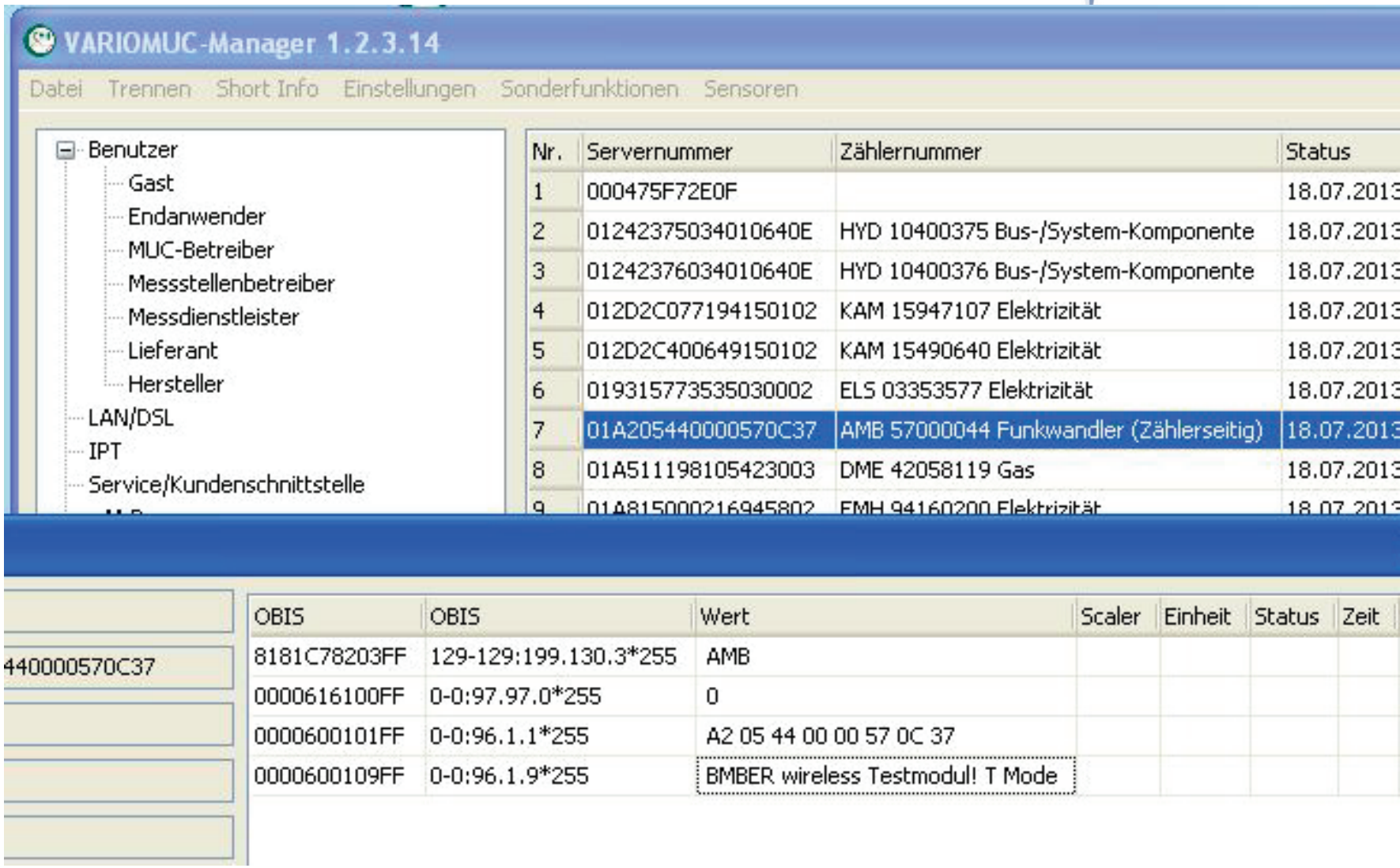
Support Head-end side

- GPRS
- Ethernet (Web Interface)
- WLAN
- WiMAX

Support Meter side

- Wired Serial (RS-485)
- Wired M-Bus
- ZigBee
- Wireless M-Bus

Intro – Smart Metering – Collector GUI



Intro – Smart Metering – Meter

Electricity Meters

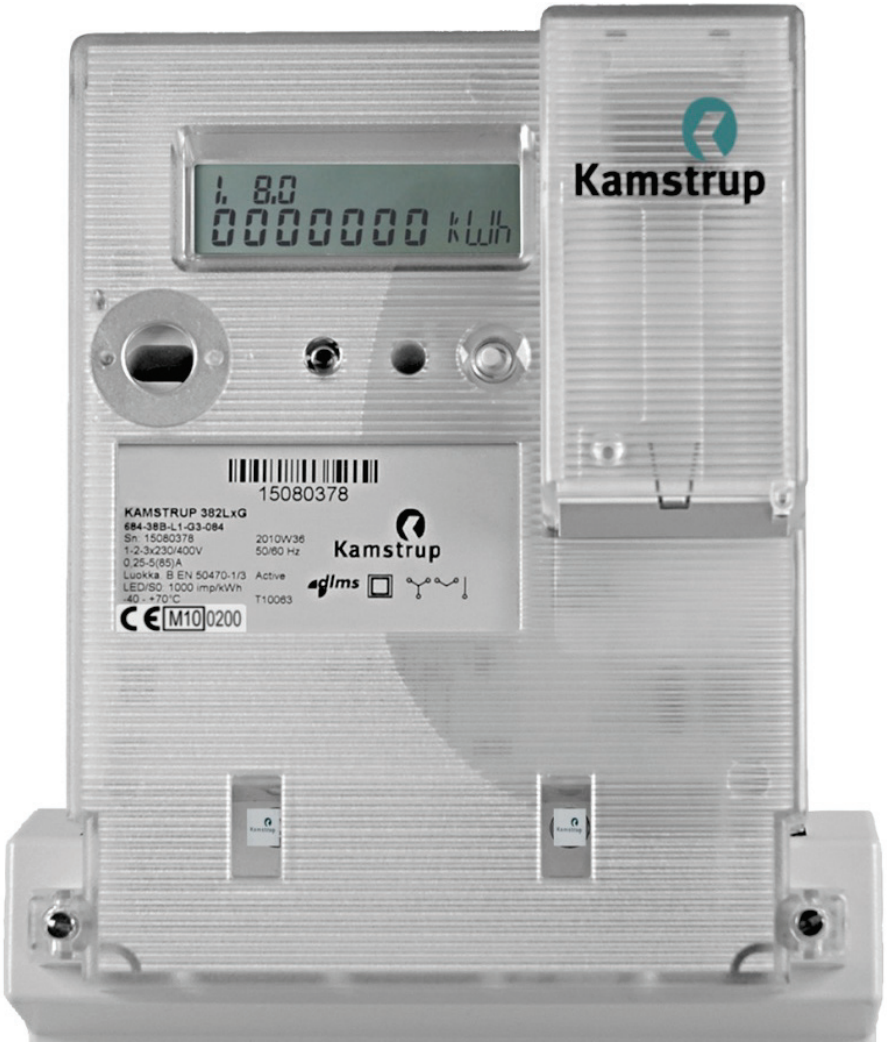
- Various Vendors
- Kamstrup is just an example

Interfaces

- Optical
- Wired Interfaces
- GPRS
- ZigBee
- Wireless M-Bus

Functionality

- Meter reading
- Pre-payment
- Tariffs
- Disconnect



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 wireless 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

Protocol Stack

European 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 frequency 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

Physical Layer

- Frequency Spectrums
  - 868 MHz
  - 434 MHz
  - 169 MHz
- Distance
  - Up to 5 miles (LoS)
- Line coding (depends on communication mode)
  - 3 of 6 code (constant-weight code)
  - Manchester coding
  - NRZ coding

Protocol Overview – Data Link Layer

Data Link Layer

- Frames (typical)

  - CRCs
  - Device addressing
  - Specification of data (application layer)
    - Response
    - Command
    - Alerts and Errors...
- Extended Link Layer
  - CRCs
  - Provides encryption at link layer

Protocol Overview - Data Link Layer

First Block (Frame Header)

Example Capture (Sent by meter, CRCs removed)

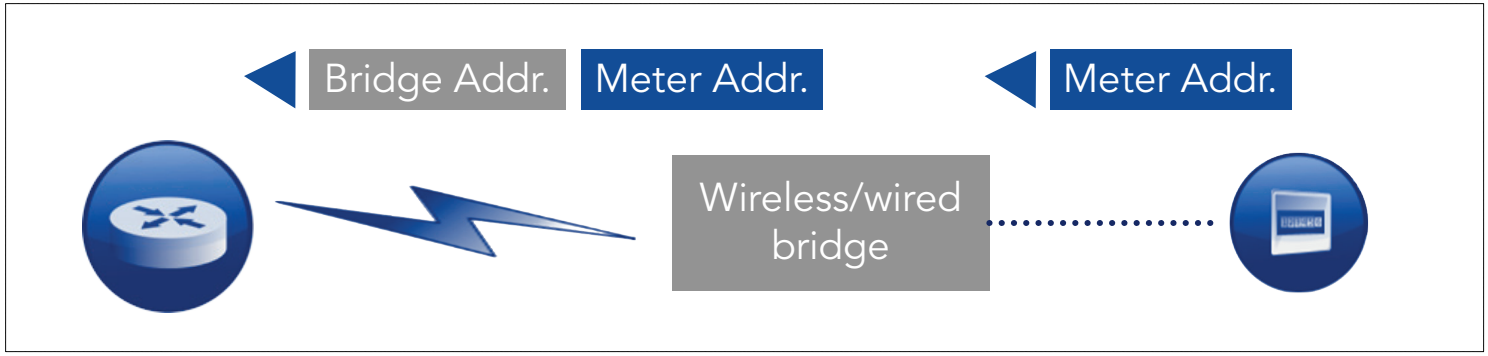
1E 44 2D 2C 07 71 94 15 01 02 7A B3 00 10 85 BF
5C 93 72 04 76 59 50 24 16 93 27 D3 03 58 C8

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) Device Type: 02 (electricity meter) Version: 01

Data Header Types

Frame Header | **Data Header** | Data Records

- No header
- Short header
  - Indicates access number
  - Signals errors and alerts
  - Indicates encryption mode
- Long header
  - Additionally signals addresses behind bridges or virtual devices



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 number	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)

Data Records

- Structured using data information fields (DIF) and value information fields (VIF) incl. relevant 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

Wireless M-Bus Sniffer

Protocol sniffers 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"

cbrunsch@tortuga: ~/Dev/scambus

```
cbrunsch@tortuga:~/Dev/scambus$ ./scanner.py -vv -i /dev/ttyUSB3
Aug 01 19:24:03 AMB 57 00 00 44 SND-NR Records: 2
--
CI Detail:      72 (EN 13757-3 Application Layer with long Transport Layer, SND-
header:         long header
has errors:     False
access:         No access
config word:    05 30
mode:           5 (AES encryption with CBC; IV is not zero)
iv:             A2 05 44 00 00 57 0C 37 58 58 58 58 58 58 58 58
key:            CA FE BA BE 12 34 56 78 9A BC DE F0 CA FE BA BE
--
DIFs:   0E (Instantaneous value, 12 digit BCD)
VIFs:   13 (Volume l)
Value:  00 00 00 00 21 36
--
DIFs:   0D (Instantaneous value, variable length)
VIFs:   FD 11 (Second extension of VIF-codes)
Value:  41 4D 42 45 52 20 77 69 72 65 6C 65 73 73 20 54 65 73 74 6D 6F 64 75 6C
```

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

Encryption Modes

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

Extended Link Layer (ELL) Encryption Modes

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

Are we safe with AES?

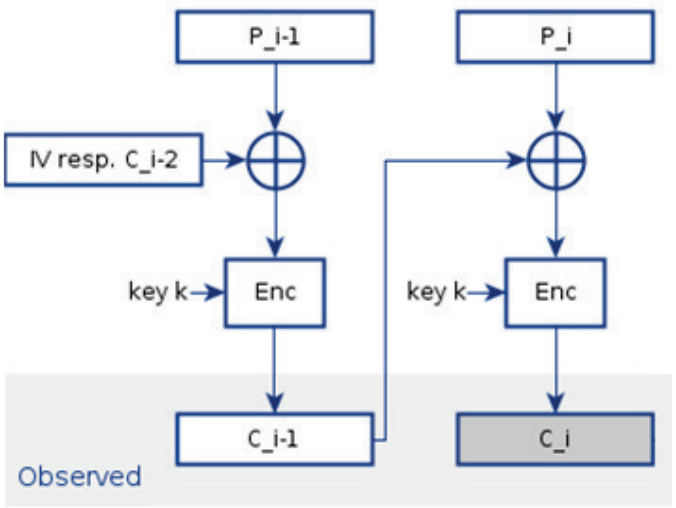
Compass Security AG
Werkstrasse 20
P.O. Box 2038
CH-8645 Jona

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

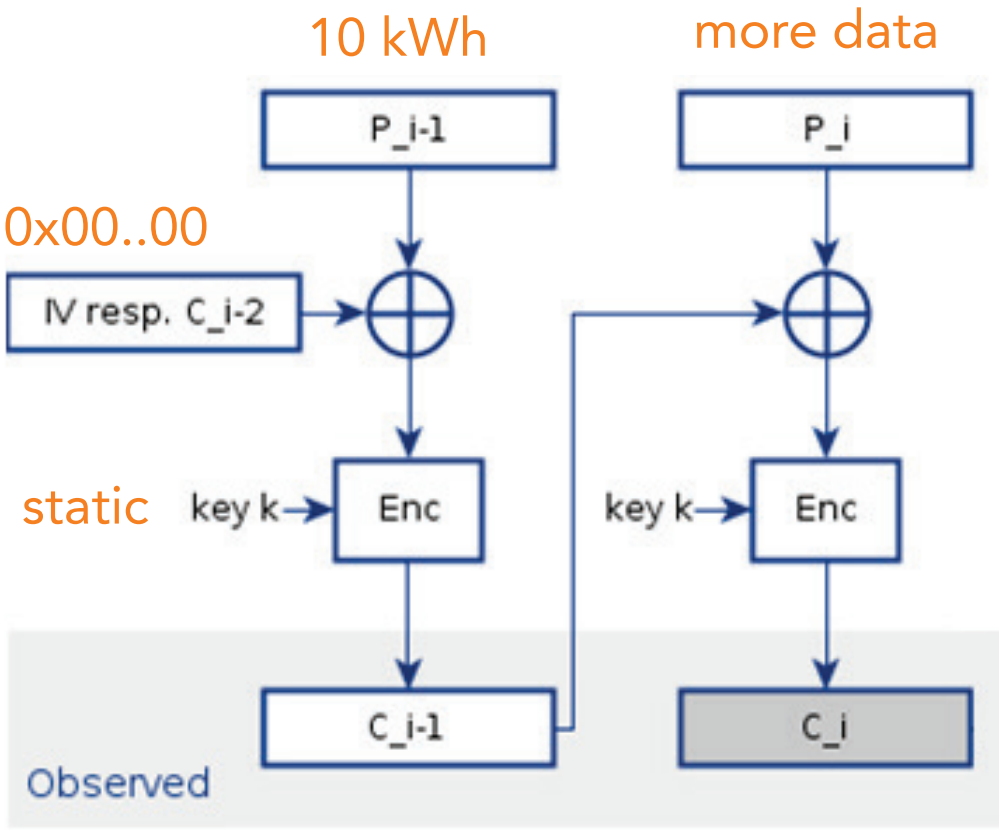
Are we safe with AES?

Encryption Mode 4 (DAL)

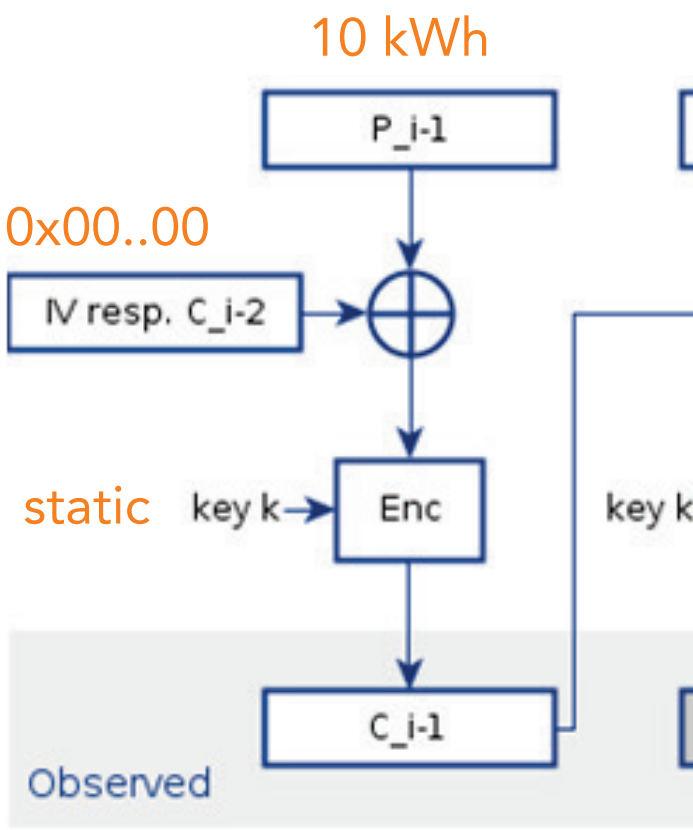
- AES-128 in CBC mode
- All-zero IV
- Uses static key k
- $C_1 = Enc_k(P_1 \oplus IV)$
  $= Enc_k(P_1 \oplus 00\ 00\ \ldots\ 00\ 00)$
  $= Enc_k(P_1)$
- Equal PT result in same CT



Are we safe with AES?



Cipher Text Block

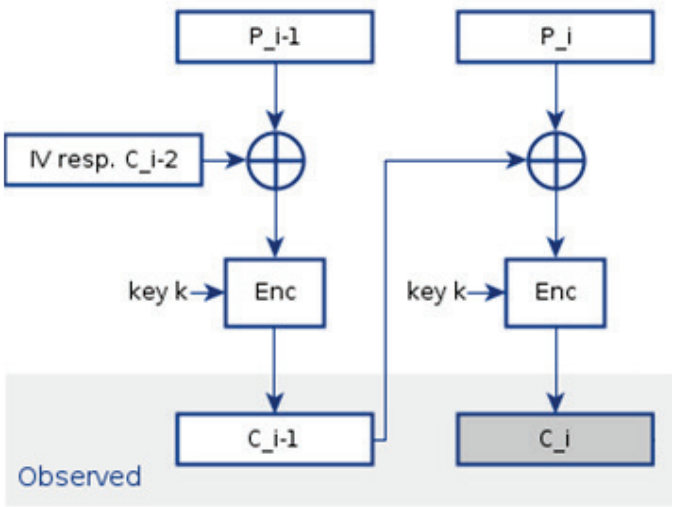


Cipher Text Block

Are we safe with AES?

Encryption Mode 4 (DAL)

- 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 PT result in same CT



Standard workaround

- Standard mandates to prefix value with date and time record
- Date and time (record type F) maximum granularity is minutes

Side note

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

Is encryption mode 5 our friend?

Encryption Mode 5 (DAL)

- 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)

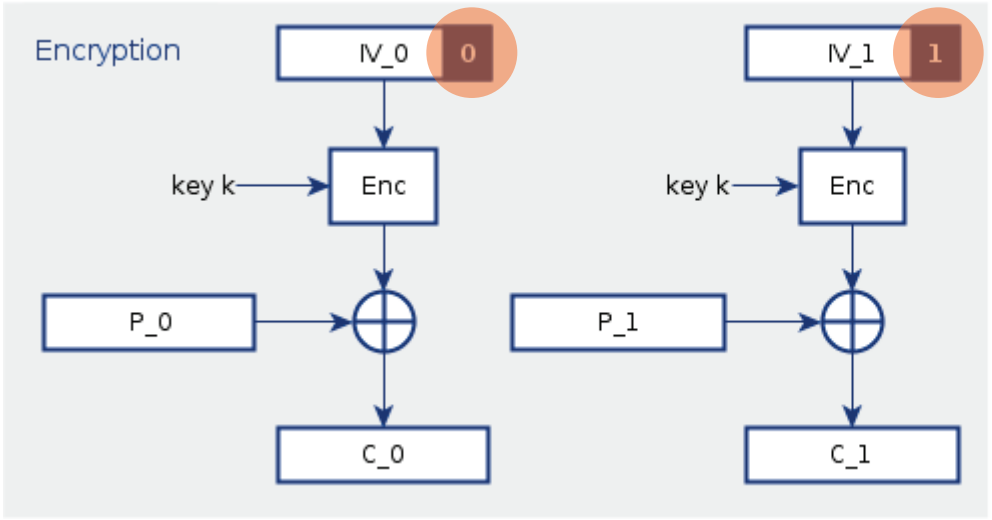
1E 44 **2D 2C 07 71 94 15 01 02** 7A **B3** 00 10 85 BF
5C 93 72 04 76 59 50 24 16 93 27 D3 03 58 C8

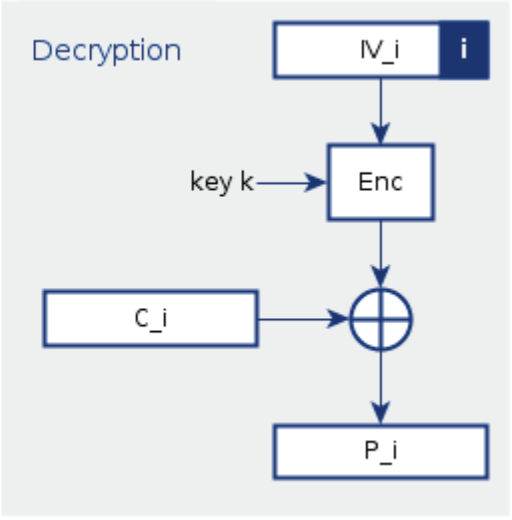
Initialization Vector (IV)															
Manuf.		Address						Padding with Access Number							
2D	2C	07	71	94	15	01	02	B3	B3	B3	B3	B3	B3	B3	B3

How about Counter Mode?

Encryption Mode 1 (ELL)

- AES-128 in CTR mode





How about Counter Mode?

Keystream repetition in CTR mode

$$C_a = Enc_k(IV) \oplus P_a$$
$$C_b = Enc_k(IV) \oplus P_b$$

Apply Mathemagic

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

Example of Keystream Repetition

```
Pa =          04 83 3B 08 34 05 00 2F...  (341'000 Wh)
Pb =          04 83 3B 14 34 05 00 2F...  (341'012 Wh)

Pa ⊕ Pb = 00 00 00 1C 00 00 00 00...
Ca ⊕ Cb = 00 00 00 1C 00 00 00 00...
```

How about Counter Mode?

We observed a difference of 0x1C. So what?

Think about the construction of 0x1C out of two values

```
Max. difference:   1 1100 = 28
                  -0 0000 =  0
                          = 28 Wh
Min. difference:   1 0000 = 16
                  -0 1100 = 12
                          =  4 Wh
```

Consumption must have changed between 4 and 28 Wh

How about Counter Mode?

IV in encryption mode 1

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

- CC Signal communication direction, prioritise frames ...
- SN Encryption mode, time field, session counter (4 bits)
- FN Frame number
- BC Block counter

- Predictable IVs result in 85-bits security due to TMTO

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

Can we adjust the device time?

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

Issues with message integrity?

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

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

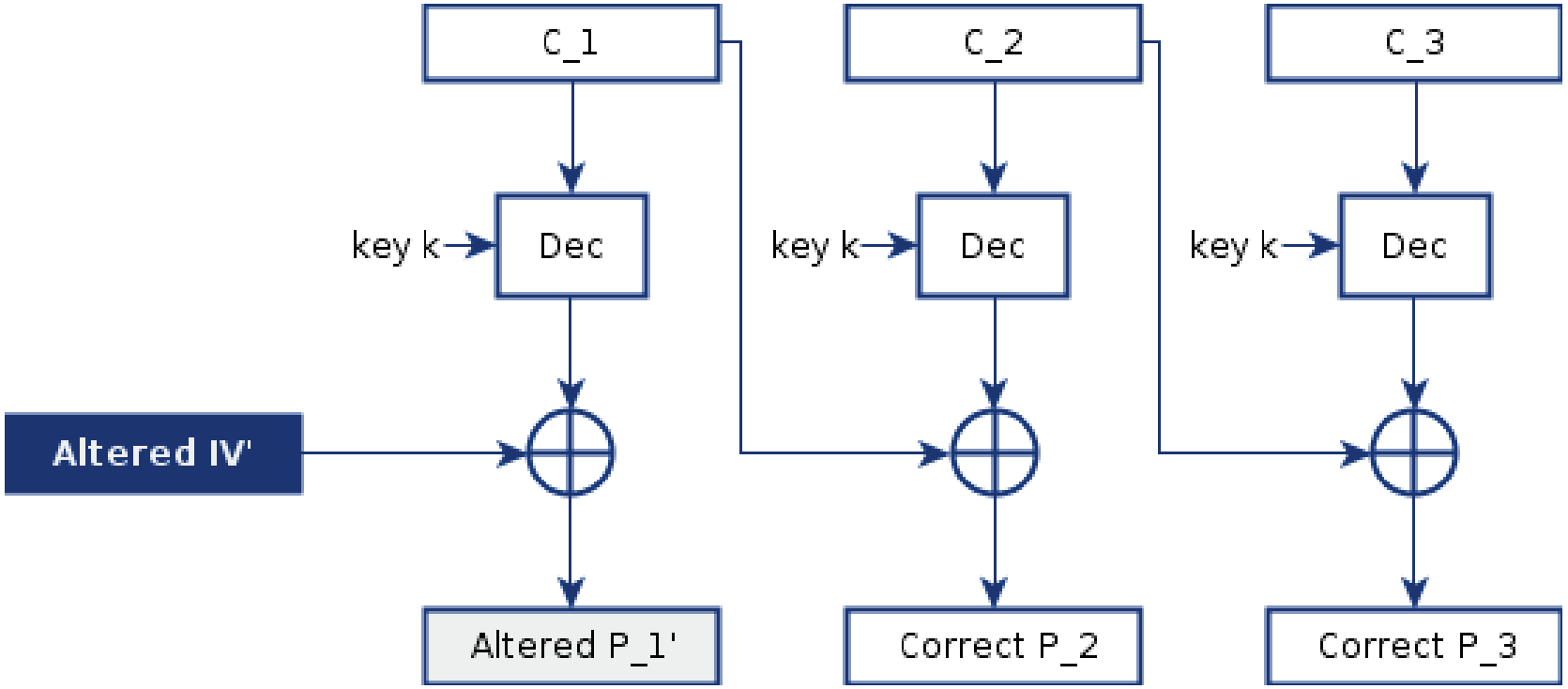
- CRCs
  - There are CRCs at the frame level
  - CRCs are not considered integrity protection
- Signatures
  - Encryption mode 5 and 6 can signal digitally signed billing data
  - Not widely used => due to meter display has priority
- MACs
  - Not available

Manipulation of Ciphertexts or IVs

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

IV Manipulation in CBC

CBC Mode of Decryption



IV Manipulation in CBC

Feasibility of IV 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?

IV Manipulation Example

Example of Consumption Value Manipulation

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

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

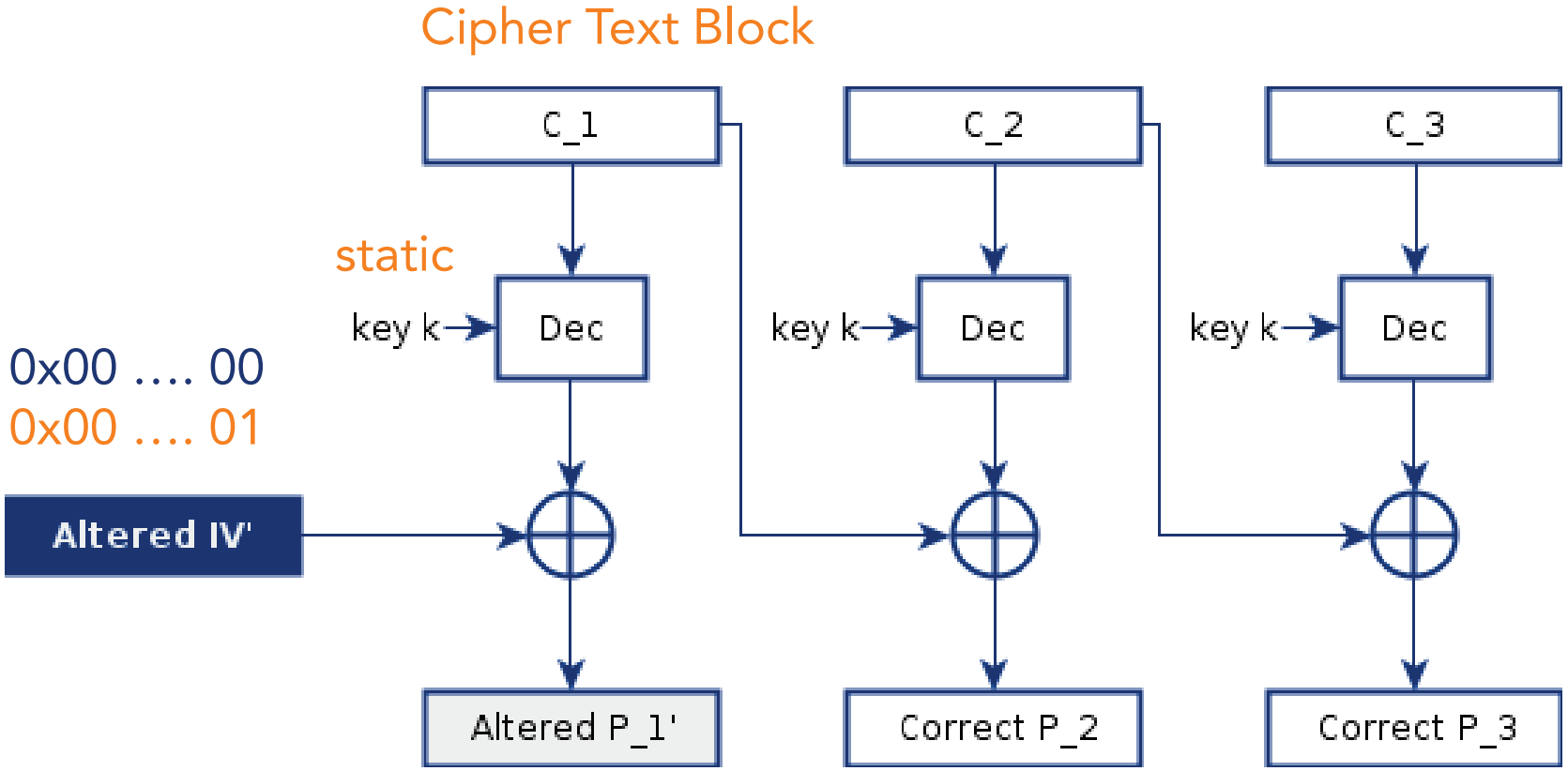
Precondition

- Original value read from meter display 341 kWh (**08 34 05 00**)

Calculate Plaintext P_1'

P_1	2F	2F	04	83	3B	**08**	**34**	**05**	**00**	2F	2F	2F	2F	2F	2F	2F
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

IV Manipulation - Receiver Side



XOR causes plaintext bits
to flip as altered in IV'

IV Manipulation Example

Example of Consumption Value Manipulation

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

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

Precondition

- Original value read from meter display 341 kWh (**08 34 05 00**)

Calculate Plaintext P_1'

P_1	2F	2F	04	83	3B	**08**	**34**	**05**	**00**	2F	2F	2F	2F	2F	2F	2F
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

Result

- P1’ 144'392 Wh (08 34 02 00)

Partial Encryption in wM-Bus

Partial Encryption

- Dedicated Application Layer allows for partial encryption
- How does the receiver handle doubled data records?

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
```

Manipulation of the ELL

ELL Integrity Protection

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

ELL CRC calculation

Frame Header	ELL Header	Encrypted Data

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

How to easily calculate the CRC

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
```

....

```
Copyright (C) 2010, 2011, 2012, 2013  Gregory Cook
This is free software; see the source for copying conditions.  There
warranty; not even for MERCHANTABILITY or FITNESS FOR A PARTICULAR PU
Version 1.1.0                                  <http://reveng.sourceforge.
$
$ ./reveng -D | grep 13757
width=16  poly=0x3d65  init=0x0000  refin=false  refout=false  xorout
=0xc2b7  name="CRC-16/EN-13757"
$
$ ./reveng -m CRC-16/EN-13757 -c 01FD1F01
cc22
$ ./reveng -m CRC-16/EN-13757 -c 01FD1F00
f147
$
```

ELL Manipulation Example

C_a = E7 8E 1B 7B 9D 86 (Intercepted Ciphertext)

P_a = CC 22 01 FD 1F 01 (On Command)

P_b = F1 47 01 FD 1F 00 (Off Command)

$C_b = C_a \oplus P_a \oplus P_b$

C_b = E7 8E 1B 7B 9D 86 ⊕

CC 22 01 FD 1F 01 ⊕

F1 47 01 FD 1F 00

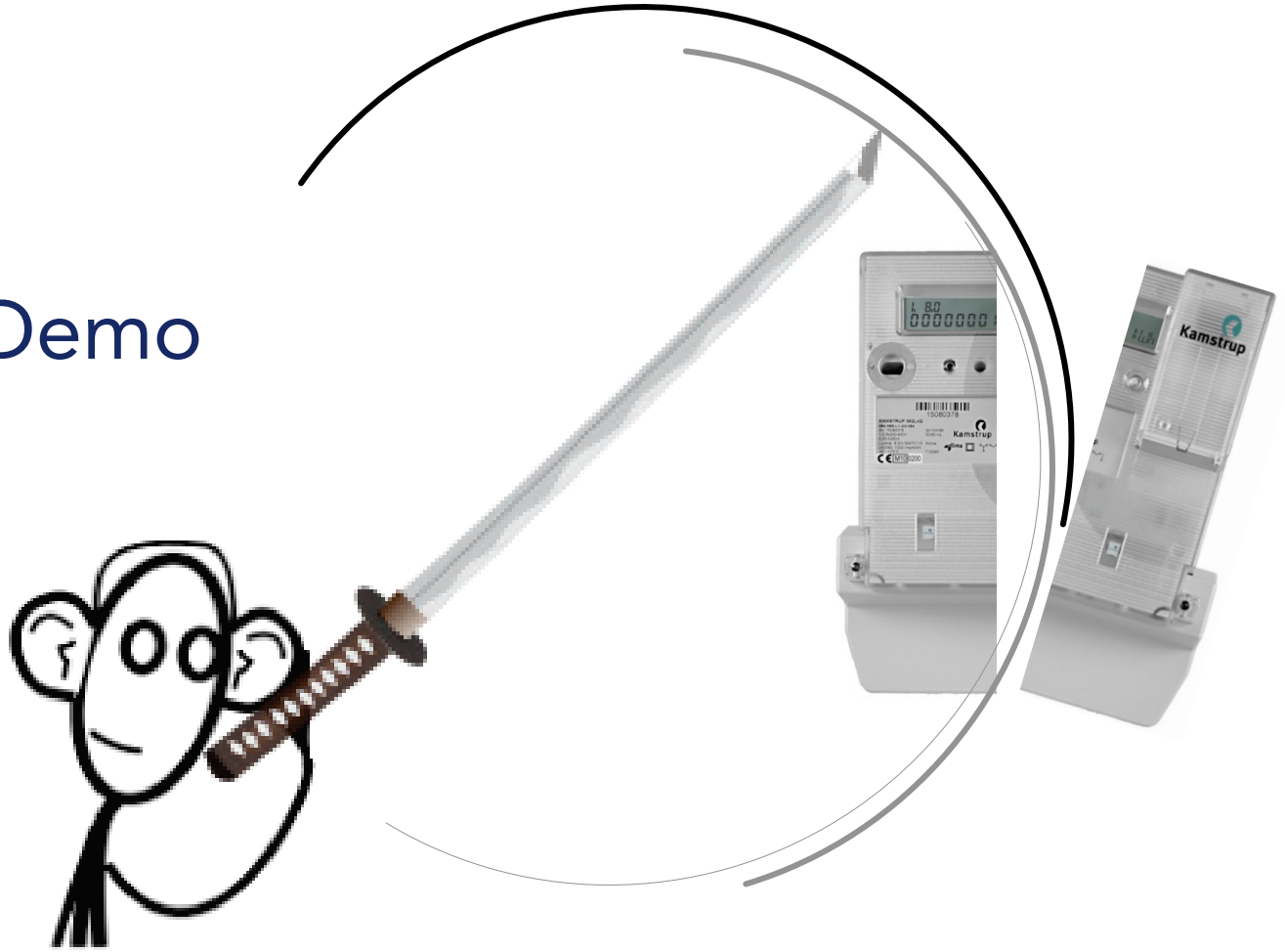
C_b = DA EB 1B 7B 9D 87 (Manipulated Ciphertext)

Which messages are affected?

Integrity with Special Protocols

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

Demo

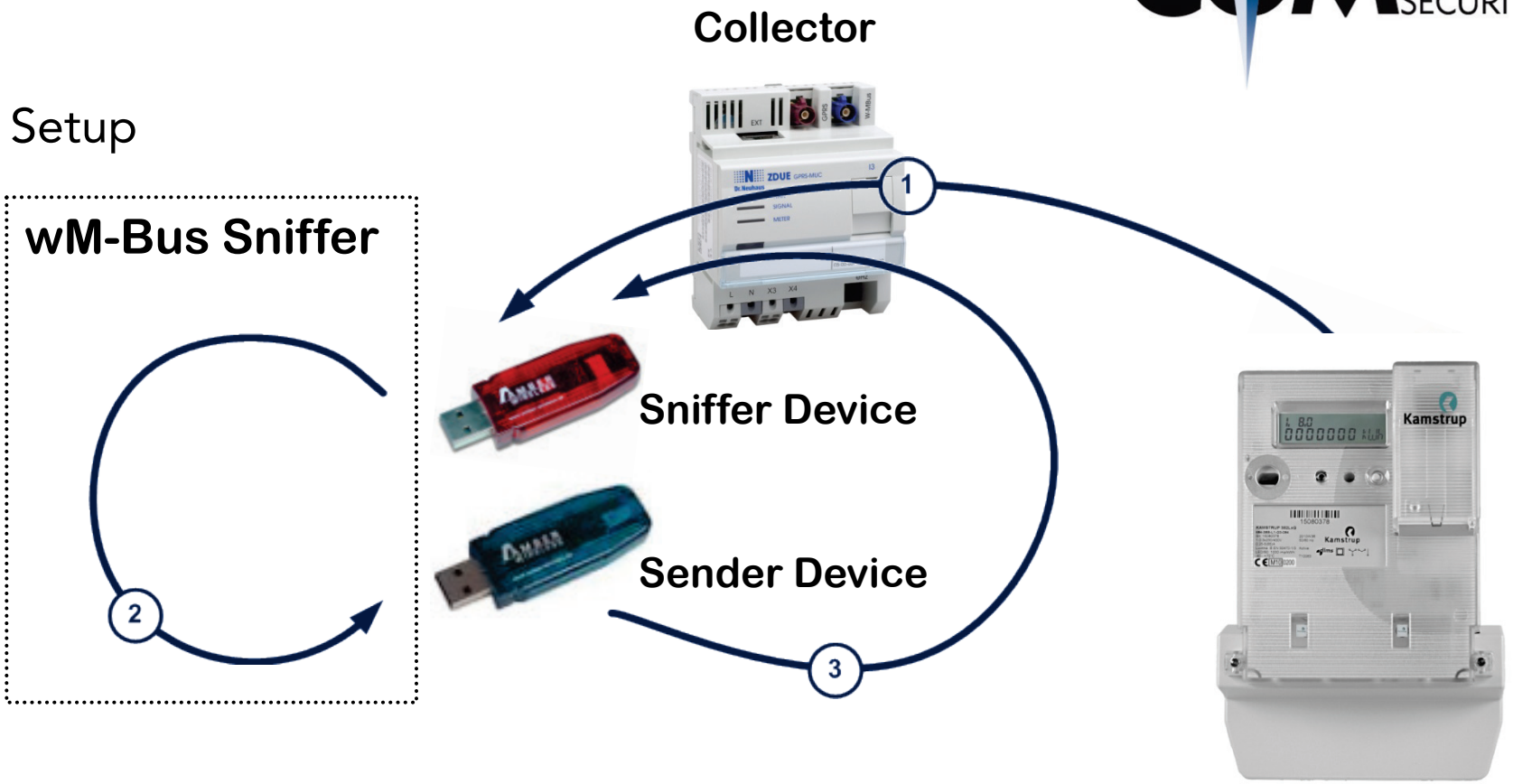


Compass Security AG
Werkstrasse 20
P.O. Box 2038
CH-8645 Jona

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

Energy Fraud Demo

Setup

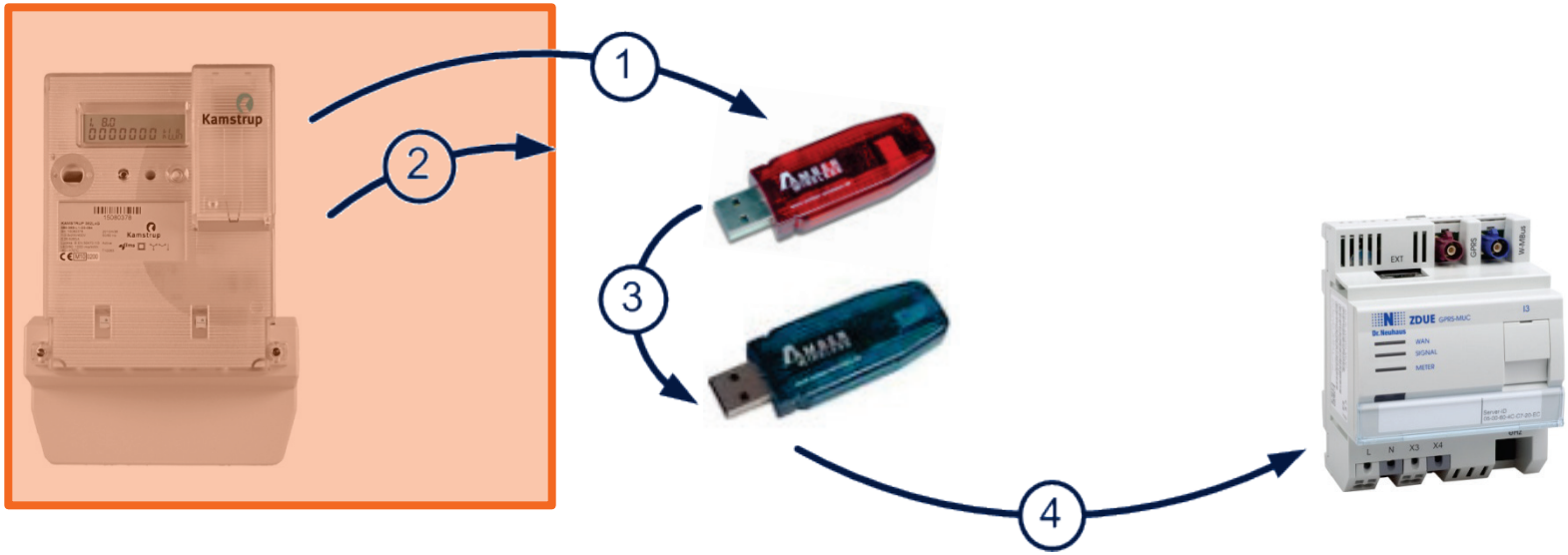


Hardware

- Amber Sticks http://amber-wireless.de/406-1-AMB8465-M.html
- TI Transceiver http://www.ti.com/lit/ds/symlink/cc1101.pdf
- TI App Note http://www.ti.com/lit/an/swra234a/swra234a.pdf

Issues with Packet Replay

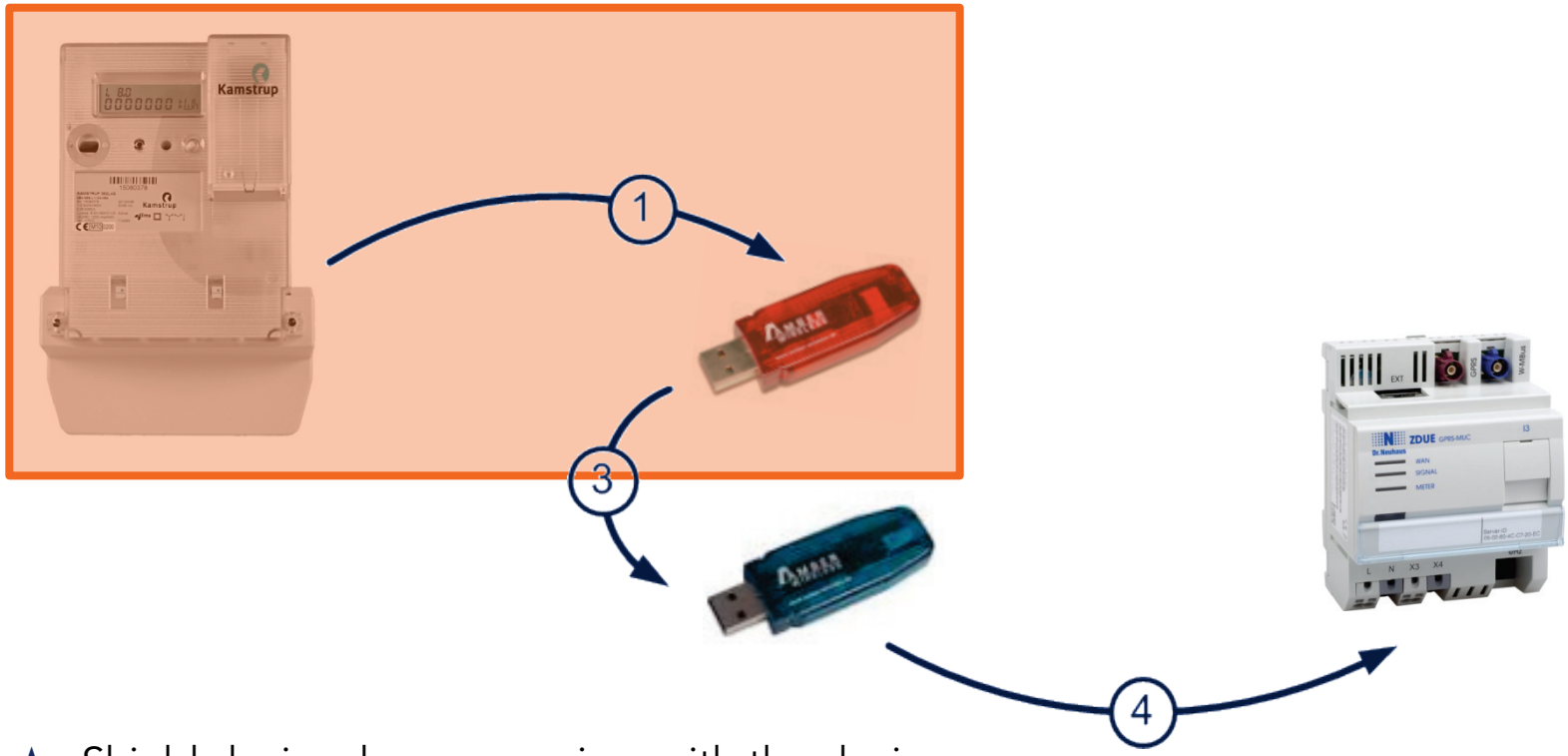
Shield and Replay I



- Capture messages from original device
- Shield device and replay messages

Issues with Packet Replay

Shield and Replay II

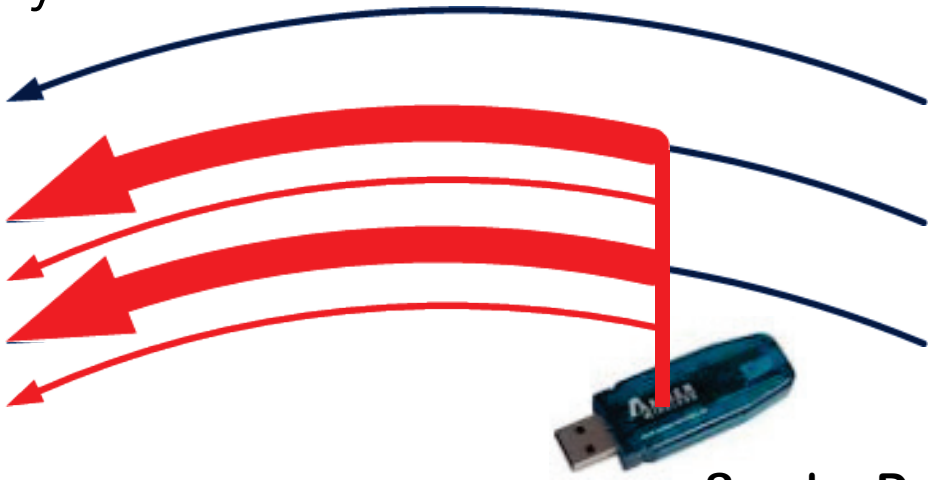


- Shield device, have a receiver with the device
- Submit messages to collector at maybe lower pace

Issues with Packet Replay

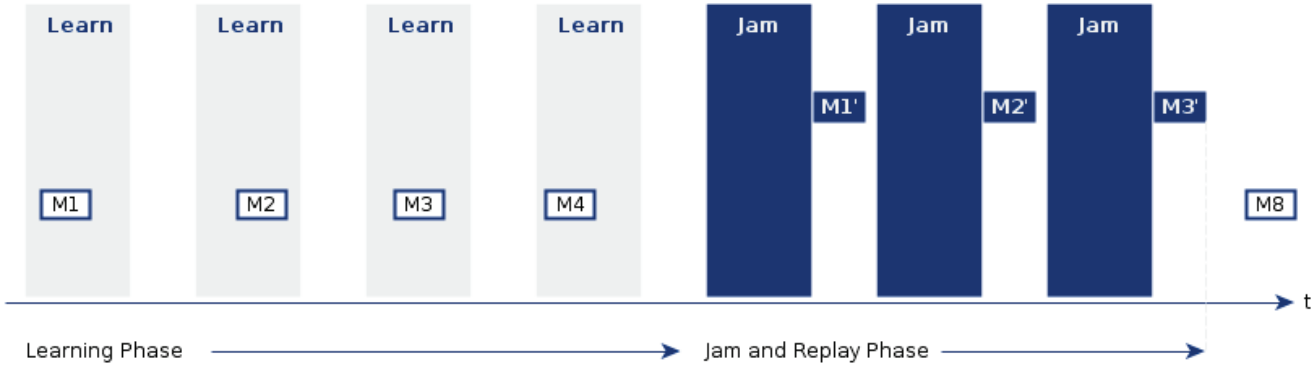
Jam and Replay

Collector



Sender Device

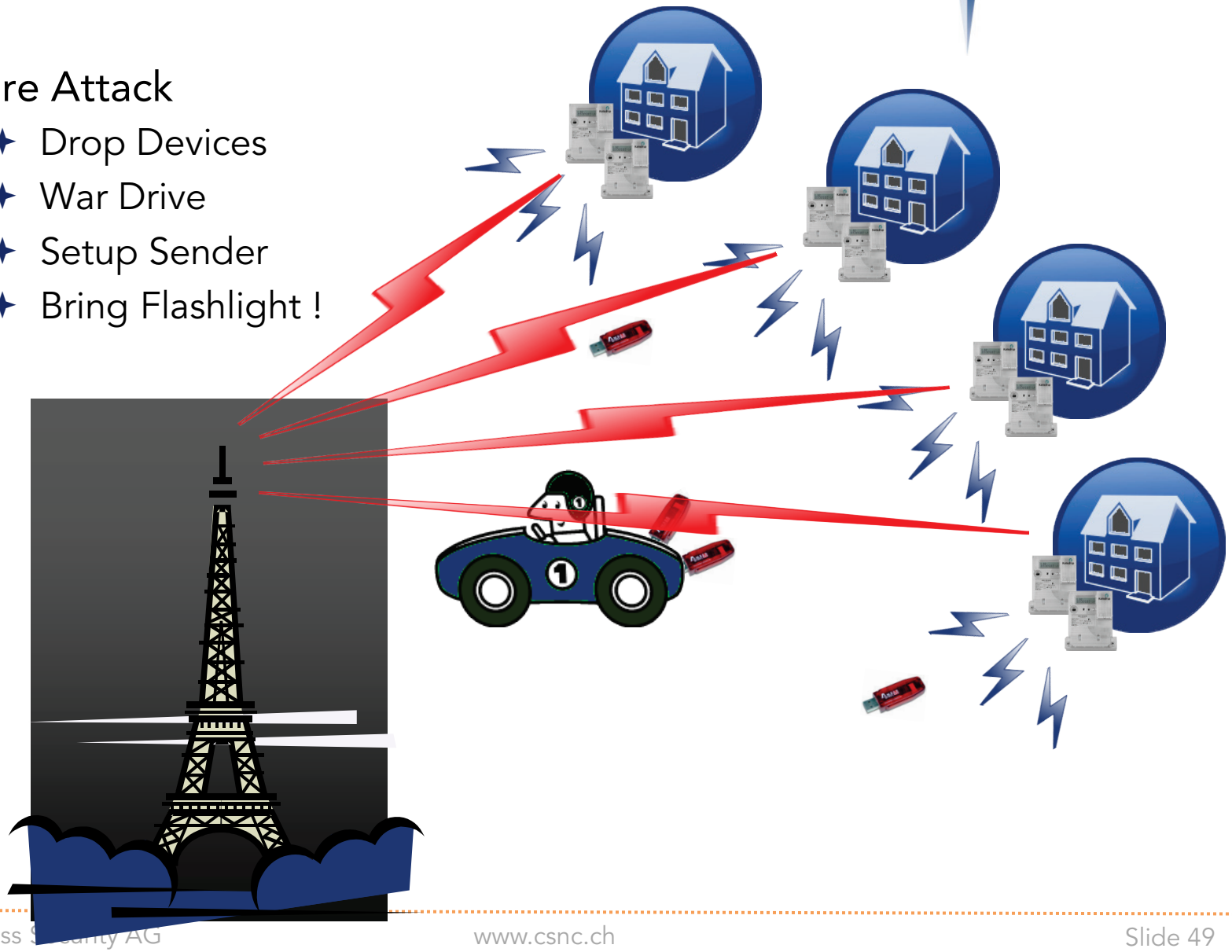
Meter



Orchestrated Blackouts

Prepare Attack

- Drop Devices
- War Drive
- Setup Sender
- Bring Flashlight !



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

General Issues

- Key size 64 bits
- Zero consumption detection
- Disclosure of consumption values
- Plaintext errors and alarms
- Information Disclosure
- Man-in-the-middle in routed environments
- Key disclosure

Energy Fraud

- Manipulation of consumption value

Orchestrated Blackouts

- Manipulation of valve and breaker open/close commands

Outlook

Counter Measures

- Latest Standard "OMS Specification Vol. 2 Primary Comm. Issue 4.0.2"
  - Released on January 27th 2014
  - Allows for modes 0, 5, **7, 13**
    - Mode 7: Additional encryption mode relying on AES-128 in CBC mode using dynamic keys, requires integrity-preserving authentication and fragmentation layer (AFL) to derive keys from
    - Mode 13: TLS 1.2 support for wM-Bus