KU LEUVEN

On the feasibility of cryptography for a wireless insulin pump system

EDUARD MARIN, BOHAN YANG, DAVE SINGELÉE, INGRID VERBAUWHEDE AND BART PRENEEL

KU LEUVEN, ESAT-COSIC AND IMINDS

CODASPY 2016
March 9-11, New Orleans, US

Outline

- Insulin pump system
- Black-box approach
  - Wireless communication parameters
  - Reverse engineering
  - Obtain serial number
  - Software radio-based attacks
- AES-based security solution
- Conclusions

Insulin pump system

Remote control

Glucose meter

Insulin pump

USB stick

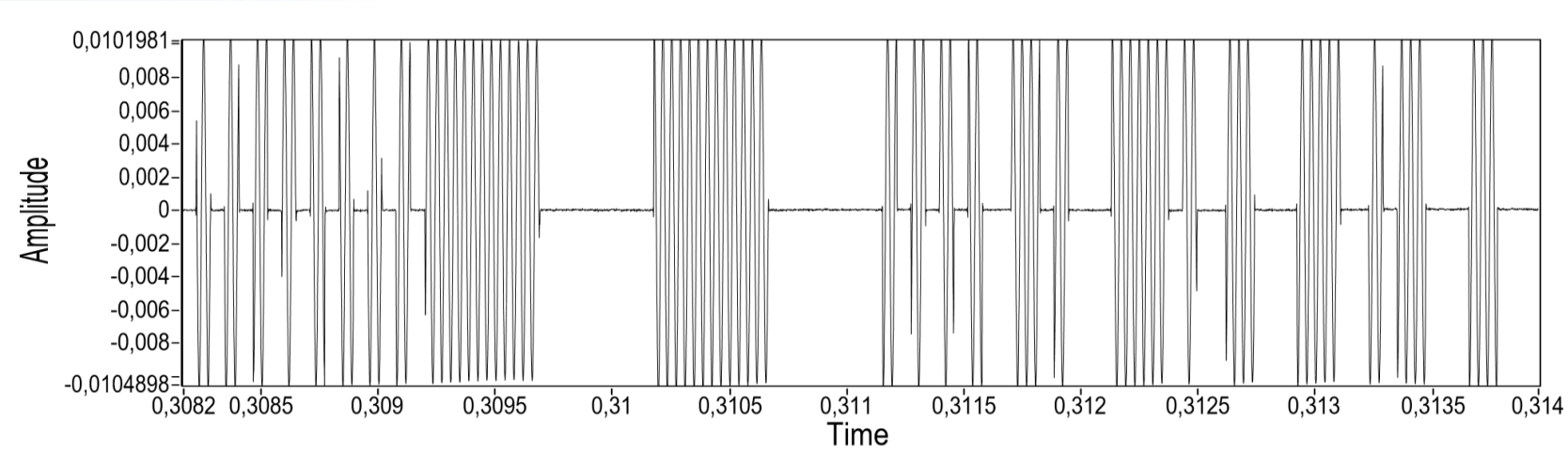
Glucose sensor

Black-box approach

- 1. Find wireless communication parameters
- 2. Reverse engineering the protocol
- 3. Obtain the serial number
- 4. Carry out software radio-based attacks

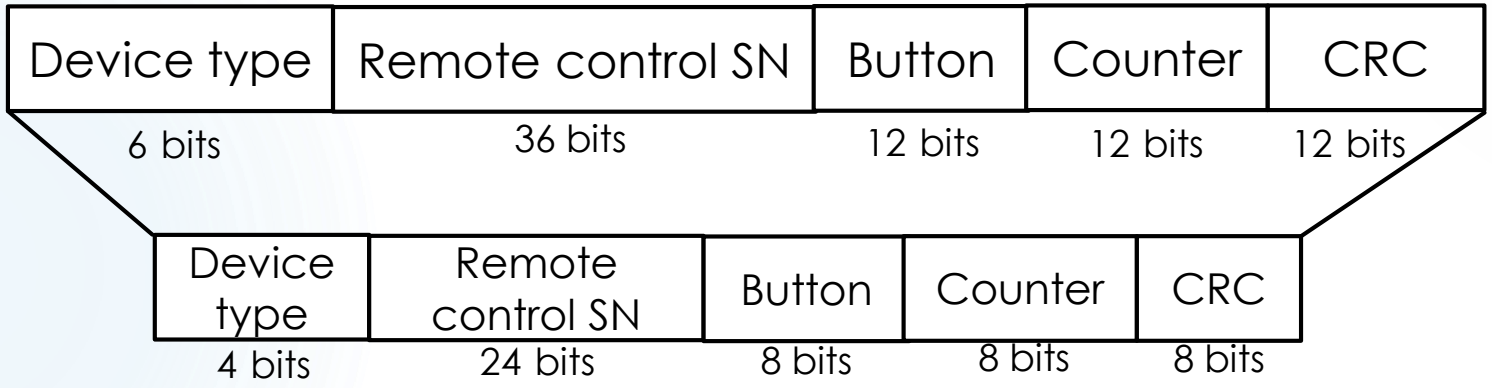
Wireless communication parameters

- 868.35 MHz
- On-Off Keying (OOK)
- Symbol rate



Reverse engineering

- Mapping sequence
- CRC-8-WCDMA



Obtain serial number

- Eavesdrop the wireless channel once
- Brute-force (24 bits SN)
- Peek at the back of the device itself
- Get it through an insider working in the hospital

Software radio-based attacks

- Replay attacks (weak anti-replay mechanism)
- Message injection attacks
- Privacy attacks
  - Type of device and serial number
  - Glucose value
  - …

AES-based solution

- Data confidentiality
- Authentication
- Freshness

- New message format
  - Remove mapping sequence and CRC
  - 16-bit counter
  - Serial number optimization

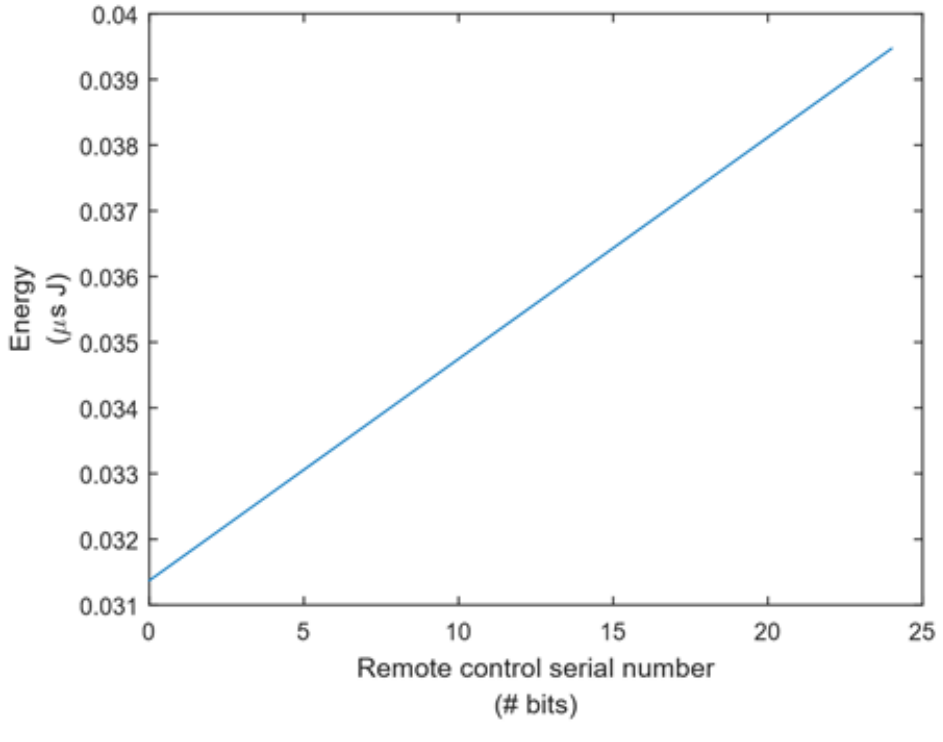
Energy cost

- Communication cost: 2.25 µJ/bit (TX) & 0.75 µJ/bit (RX)
- Computational cost: AES-128 CTR mode & AES-128 MAC

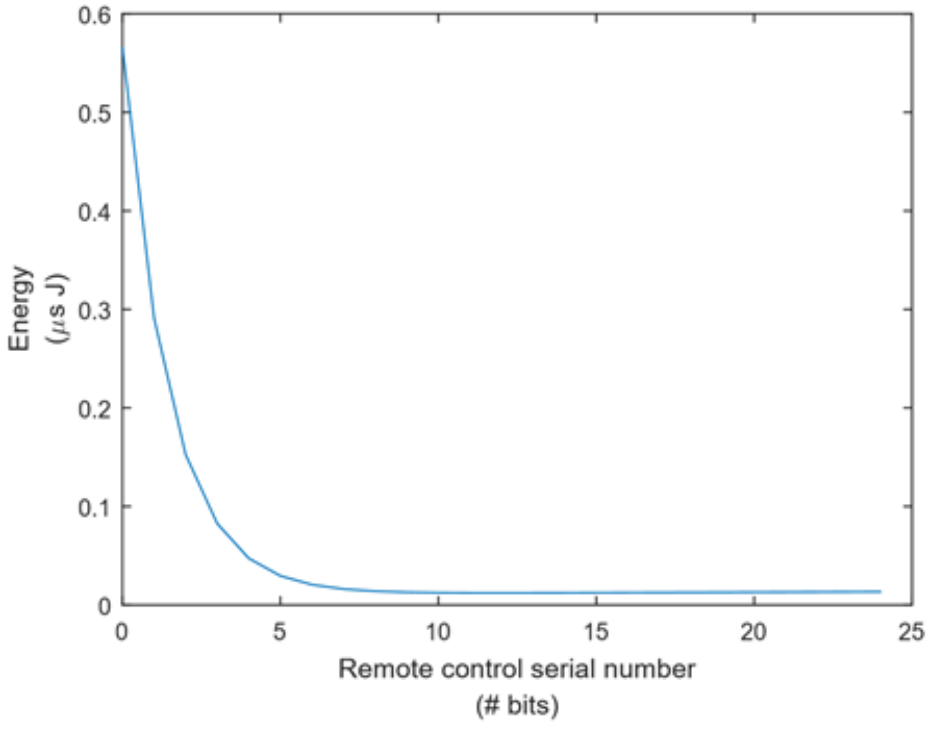
Operation	ROM (Byte)	Cycles	Time (μs)	Energy (μJ)
MAC generation	2684	9430	590	2.14
MAC verification	2760	9561	598	2.16
Encryption/Decryption	2664	9404	588	2.13
Encryption + MAC generation	2879	18865	1180	4.27
Decryption + MAC verification	2847	18964	1186	4.30

*MSP430 @16 MHz, 1.8V on a Spartan-6 FPGA

Serial number optimization

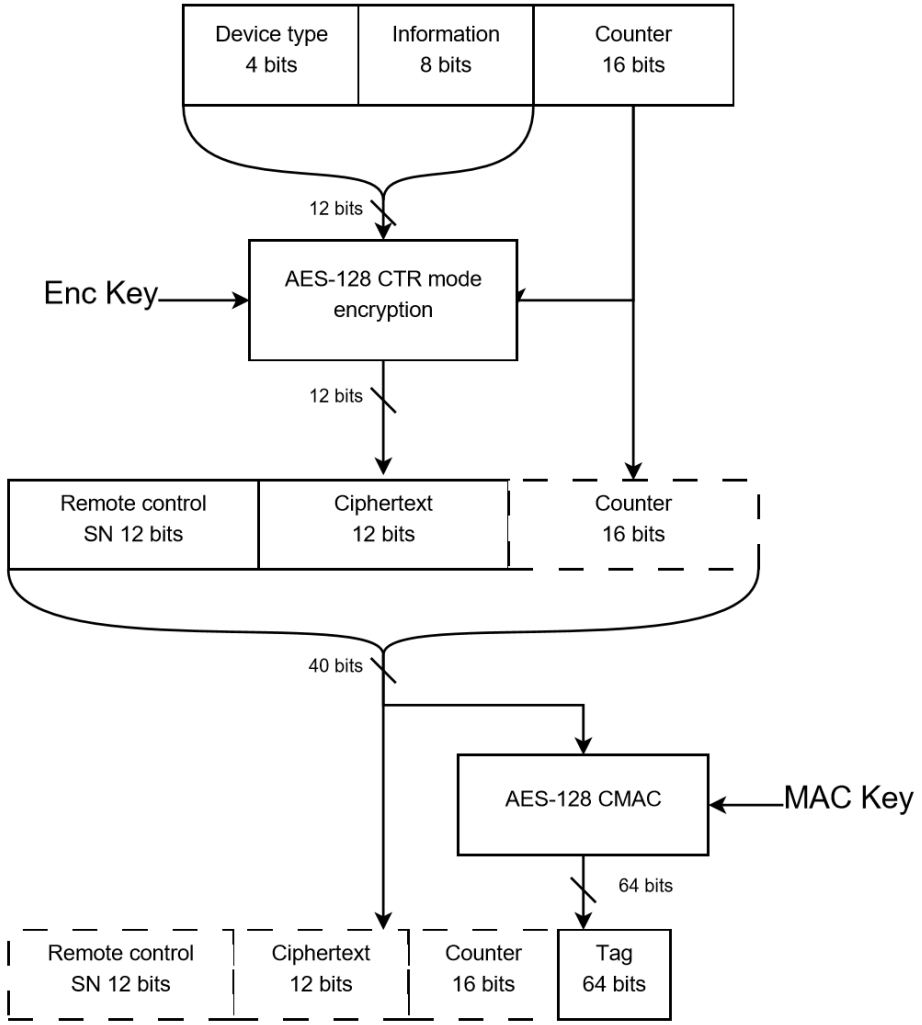


Energy consumption vs remote control SN length (Remote control)



Energy consumption vs remote control SN length (Insulin pump)

MAC + optimized SN + encryption



Energy cost per solution

Energy cost (per day) of each solution in the remote control

Solution	Confidentiality	Authentication	Computation cost	Communication cost	Total cost	Cost increase
No security (old message format)	✗	✗	0 mJ	26.32 mJ	26.32 mJ	-
No security (new message format[a])	✗	✗	0 mJ	18.9 mJ	18.9 mJ	-28.19%
MAC + opt SN encryption	✓	✓	0.64 mJ	35.10 mJ	35.74 mJ	+35.79%
Encryption	✓	✗	0.32 mJ	20.25 mJ	20.57 mJ	-21.84%
MAC	✗	✓	0.32 mJ	39.15 mJ	39.47 mJ	+50%

Energy cost (per day) of each solution in the insulin pump

Solution	Confidentiality	Authentication	Computation cost	Communication cost	Total cost	Cost increase
No security (old message format)	✗	✗	0 mJ	8.77 mJ	8.77 mJ	-
No security (new message format[a])	✗	✗	0 mJ	6.30 mJ	6.30 mJ	-28.16%
MAC + opt SN encryption	✓	✓	0.65 mJ	11.86 mJ	12.51 mJ	+42.64%
Encryption	✓	✗	0.32 mJ	6.75 mJ	7.07 mJ	-19.38%
MAC	✗	✓	0.32 mJ	13.05 mJ	13.37 mJ	+52.45%

Discussion

- Computational cost << Communication cost
- How can the energy costs be further reduced?
  - Further optimize message format
  - 32-bit tag
  - MAC over several messages

Conclusions

- Security through obscurity is a dangerous approach
- Insecure protocol
- However.. it is possible to mitigate some of these problems!
- How to protect the message integrity more efficiently?