Smart (health) systems need smart security

Dave Singelée
ESAT COSIC
KU Leuven - iMinds

Smart Systems Industry Summit
October 14, 2014
Outline of the talk

• Who are we?
• Smart medical devices: security risks
• Cryptographic solutions
• Key generation
• Privacy
• Conclusion
Outline of the talk

• Who are we?
  • Smart medical devices: security risks
  • Cryptographic solutions
  • Key generation
• Privacy
• Conclusion
iMinds security department

ICRI
Legal Engineering

COSIC
Cryptographic Engineering

DistriNet
Secure Software Engineering
COSIC: CCOMputer Security and Industrial Cryptography
Founded in 1978
COSIC - Research

Efficient and secure implementations

Cryptographic protocols: design and cryptanalysis

Cryptographic algorithms: design and cryptanalysis

Fundamental research in discrete mathematics

- software: block ciphers, point counting algorithms
- hardware: FPGA and ASIC
- side-channel attacks: power, timing, and electromagnetic analysis, fault attacks

entity authentication, credentials, oblivious transfer,

block ciphers, stream ciphers, hash functions, MAC algorithms, (hyper)-elliptic curve cryptography
e.g.: AES, RIPEMD-160, HAMSI

number theoretic algorithms, Boolean functions, secure multi-party computation, secret sharing
COSIC - Applications

Creating electronic equivalent of the real world:
- confidentiality, digital signature, anonymity, payments, digital right managements, elections

- Technologies:
  - key management: ad hoc networks
  - anonymous communications and services
  - software tamper resistance and obfuscation
  - trusted platforms
  - multimedia security

- Applications:
  - electronic payments and commerce
  - e-government: electronic ID card, e-voting
  - car-to-car communications
  - ehealth
Implementations in embedded systems

**Protocol:** low power authentication protocol design

**Algorithm:** public key, secret key, hash algorithms

**Architecture:** Co-design, HW/SW, SOC

**Micro-Architecture:** co-processor design

**Circuit:** Circuit techniques to combat side channel analysis
Outline of the talk

• Who are we?
• Smart medical devices: security risks
• Cryptographic solutions
• Key generation
• Privacy
• Conclusion
Implantable medical devices

• Remote reprogramming / monitoring
• Software updates
Wireless Body Area Networks

- WBAN: Sensor network on/in the patient
- Remote monitoring / reprogramming
(Ultra) low power medical devices
Wireless communication link

• **Wireless communication** omnipresent
  – MICS band / Bluetooth / ZigBee / ...
  – More convenient
  – Extract medical telemetry
  – Remote commands
  – (Re)configuring device

• Wireless sensors
• Medical implants
• Internet of Things
Wireless communication link vulnerable to attacks

Cyber crime: First online murder will happen by end of year, warns US firm

The rapidly evolving Internet of Everything will leave us more vulnerable to cyber criminals, according to a worried Europol.
Security and privacy risks

• Passive attacks
  – Eavesdropping

• Active attacks
  – Man-in-the-middle attacks
  – Replay attacks
  – Unauthorized commands
  – Denial-of-Service attacks
  – ....
Intercepting wireless communication
Software Defined Radio: setup
Software Defined Radio: setup
Software Defined Radio attacks
Software Defined Radio attacks
Outline of the talk

- Who are we?
- Smart medical devices: security risks
- Cryptographic solutions
- Key generation
- Privacy
- Conclusion
Secure wireless communication

• End-to-end security
• Cryptographic algorithms needed
• Technological challenges
  – Low-cost hardware resources
  – Ultra low-power budget
  – Limited memory
  – Long lifetime
  – …
• Lightweight cryptography
Lightweight cryptographic primitives

• Lightweight, compact cryptographic algorithms
  – KATAN (802 GE)
  – Present (1075 GE)
  – Trivium (2599 GE)

• Lightweight cryptographic protocols
  – Wireless authentication protocols
  – Broadcast authentication
  – Key agreement protocols
Embedded crypto implementations

- Efficient lightweight implementations
  - Within power, area, speed, ... budgets
  - E.g., ECC processor (0.13µm - 14,566 GE - 7.3µW)
Embedded crypto implementations

- Efficient lightweight implementations
  - Within power, area, speed, ... budgets
  - E.g., ECC processor (0.13µm - 14,566 GE - 7.3µW)

- Trustworthy implementations
  - Resistant to side-channel and fault injection attacks

=> BOTH are needed
Crypto: long lifetime

• Large key size
• Key updates -> cryptographic protocols needed
• Post-quantum cryptography
  – Multivariate Quadratic (MQ)
  – Lattice-based cryptography
Outline of the talk

• Who are we?
• Smart medical devices: security risks
• Cryptographic solutions
• Key generation
• Privacy
• Conclusion
Key management

• Pre-installed
• Using out-of-band channel
  – Location-based
  – Physical contact
  – User input
  – Biometrics
  – ...
• Physical Unclonable Functions (PUFs)
• Key distribution schemes
• PKI infrastructure
PKI Infrastructure

CA₁

Vendor₁

Vendor₂

Implant₁

Implant₂

CA₂

Hospital₁

Hospital₂

Server₁

…
PUF: concept (I)

- Physically Unclonable Functions

PUFs represent a paradigm shift in physical security:

1. Explicitly programmed digital identity → Intrinsic physical identity

2. Unclonable because of physical protection of digital data
   → Unclonable because of uncontrollable physics
PUF: concept (II)

Single PUF instance

Multiple “identically manufactured” PUF instances

Basic PUF property: $\mu_{\text{inter}} >> \mu_{\text{intra}}$
PUF: concept (III)

- Non-silicon
- Silicon
- Intrinsic
  1. Randomness = *intrinsic* manufacturing variability
     - no manufacturing overhead
     - i.c. CMOS process variations
  2. Integrated measurement
     - no external equipment
     - i.c. PUF response on-chip

\[ (V_T, L_{eff}, R_{SD}, \ldots) \]
Outline of the talk

• Who are we?
• Smart medical devices: security risks
• Cryptographic solutions
• Key generation
• Privacy
• Conclusion
Privacy challenges

Mr. Jones in 2020

Brain Implant

Implantable Cardiac Device

Glucose Monitoring

Replacement hip
Location privacy
Data minimization

- Homomorphic encryption
- Oblivious transfer

- A does not learn which item B has chosen;
- B does not learn the value of the item that he did not choose
Outline of the talk

• Who are we?
• Smart medical devices: security risks
• Cryptographic solutions
• Key generation
• Privacy
• Conclusion
Conclusion

• **Smart security solutions are needed**
• **Lightweight cryptography**
• **Security architecture**
  – Key generation / agreement
  – Key update/revocation mechanisms
• **Very long lifetime of cryptographic primitives** (> 30 years)
• **Privacy is also important**
• **Active area of research**
Questions
Contact information

ESAT / COSIC

• Dave.Singelee@esat.kuleuven.be

• http://www.esat.kuleuven.be/cosic/

• K.U.Leuven, ESAT / COSIC
  Kasteelpark Arenberg 10, bus 2452
  B-3001 Leuven-Heverlee