
# Modern Cryptography Algorithms in Embedded Systems

28.04.2010 | Antti Hakkala

Faculty of Mathematics and Natural Sciences
Department of Information Technology
Turku Center for Computer Science

# Motivation and research challenges/interests

- Amount of sensitive data processed and stored in embedded devices is growing.
  - What is sensitive data?
- Human element of embedded system security
  - How people use (and lose) their PDAs, cellphones etc.
- Laws and regulations evolve
  - ...often behind the SOTA, and can be excessive or poorly defined

# Modern cryptography

- Algorithms of interest
  - Symmetric ciphers
    - AES
  - Public key ciphers
    - RSA
    - ECC
  - Hash functions

# Embedded systems

- Limited processing capabilities make effective cryptography implementations interesting
- Specialized, fast but rigid hardware vs. Flexible but slow software implementations
- Or something in between?
  - ASIP solutions?

# Why encryption...

- ...in sensor networks?
- ...in embedded networks?
- ...within device modules?
- ...between different devices?
- ...between software applications?
- ...altogether?

# Sensor networks

- Several interconnected sensors or devices which communicate with each other and possibly with a master device
- Several possible and existing applications which require secure communication between nodes.

# Implantable Medical Devices (IMD)

- Remotely accessible devices have considerable advantages
  - No surgery required for maintenance/upgrade/fault analysis
- Faults are literally lethal
  - The same applies for insecure remote access connections
- Interconnected implants?
  - Via wire? Wireless connection?

TURUN YLIOPISTO
UNIVERSITY OF TURKU

# Embedded networks

- If network-like architectures are used in embedded systems for interconnection of modules, should these connections be secure?

# Secure embedded systems

- Security must be one of the design parameters in all layers of design
  - As it is the case elsewhere, there is no ”add-on” security that works.
    - Design flaws in different layers provide attack points in other layers
- Always not enough
  - ”If the enemy has physical access to your system, you have lost the battle”

# Future work

- What can exactly be done with embedded networks? What requirements would they impose on cryptography applications?
- Define optimization criteria of crypto requirements for different applications
  - Throughput, area, power consumption
  - Tamper resistance
  - Flexibility

# Future work (cont.)

- Methods and systems for protection of information processed on embedded systems
  - Against internal and external attacks
- Flexible, adaptive solutions
  - Acceleration of common cryptography primitives that support a broad base of algorithms

# Thank you