Security Aspects in Distributed Embedded Systems and Internet of Things Solutions with Emphasis on Encryption Algorithms

Michał Nowiński, Kazimierz Wiatr

AGH University of Science and Technology

Agenda

- Introduction
- Embedded Systems
- Internet of Things
- Threads and Vulnerabilities
- Security Services
- Encryption Algorithms
- Encryption Overhead
- Low Power MCU:s
- Expected Results
- Future Work
- Conclusion

Introduction

- Huge amount of Data is being processed
- Data must be secured while stored or sent through a bus
- Unauthorized access to Data creates a risk
  - System
  - Users

Embedded Systems

- Single Functioned
- Tightly Constrained
- Reactive and Real Time
- Microprocessors Based
- Memory
- Connected
- HW-SW Systems

Source: EMBEDDED SYSTEMS-BACKBONE OF IOT, Rydhm Beri, Assistant Professor, PG Department of Computer Science, BBK DAV College for Women, Amritsar

Internet of Things

- Connection of the physical world of devices to the Internet
- Enabler for data from devices to be processed
- Every powered on device could be part of an IoT
- The cost of connecting device to the Internet is declining
- Lot of devices is collection data already
- Companies are making their equipment smarter and safer

Threads and Vulnerabilities

Threads

- Denial-of-Service
- Integrity violation
- Information leakage
- Degraded level of protection

Vulnerabilities

- Programming errors
- Web based vulnerability
- Weak access control or authentication
- Improper use of cryptography
- Unknown

Source: Embedded Systems Security: Threats, Vulnerabilities, and Attack Taxonomy. Dorottya Papp, Zhendong Ma, Levente Buttyan

Security Services

1. Confidentiality
    - Information is not disclosed to unauthorized parties
2. Data Integrity
    - Data has not been modified in an unauthorized manner
3. Authentication
    - Identity of the user or system that created information
4. Authorization

▪Providing permission to perform a security function or activity

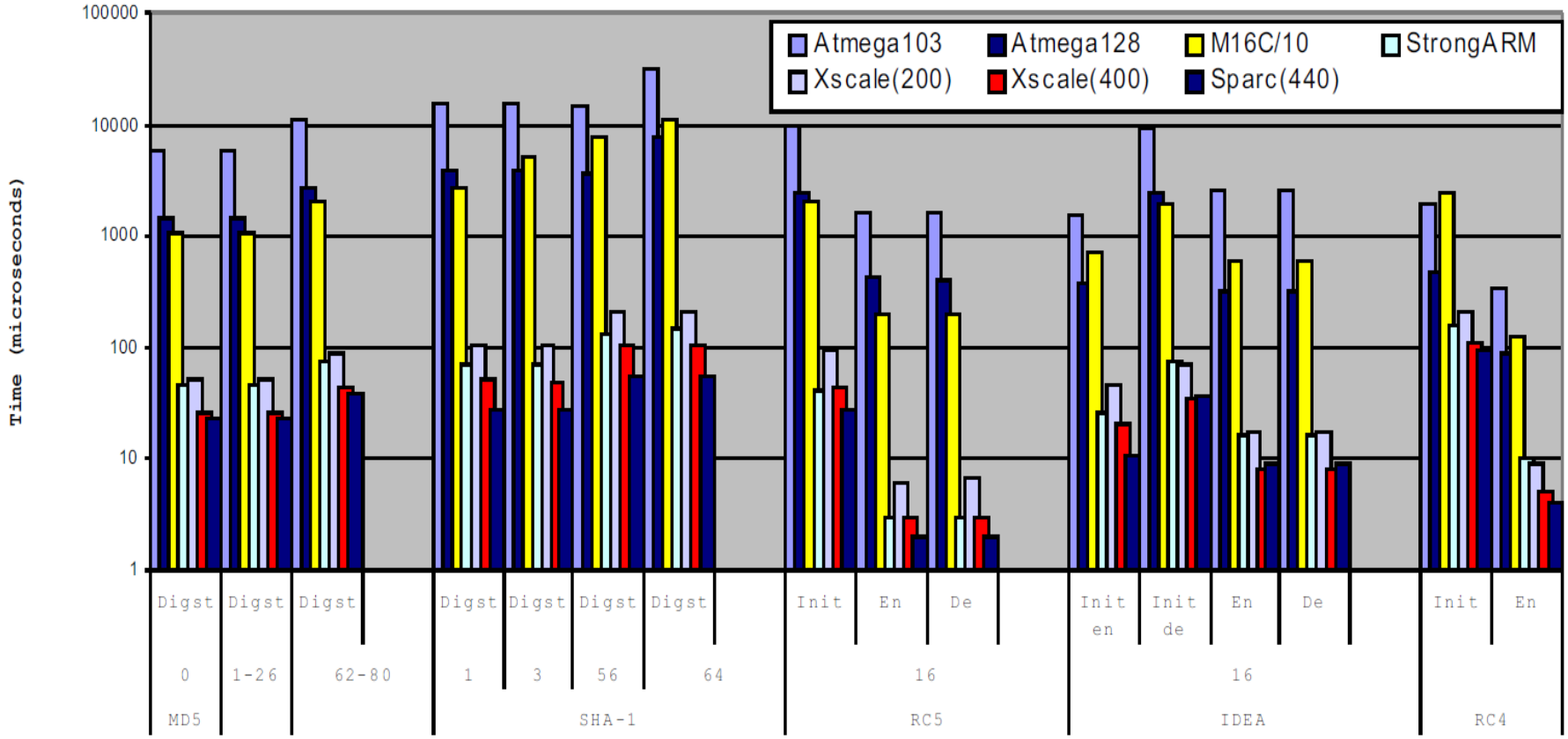
Source: NIST SP 800-57 Pt. 1 Rev. 4

Encryption Algorithms

- Symmetric Encryption (example: AES)
  - One shared secret key
  - Relatively low resources consumption
  - Typical key and block sizes: 128, 192, 256 bits

- Asymmetric Encryption (example: RSA, ECC)
  - Public and private key
  - Very compute-intensive operation
  - Typical key and block sizes: 4096 bits (RSA), 256 bits (ECC)

Encryption Overhead



Source: Alexander G. Dean, Embedded Systems Design, Analysis and Optimization using the Renesas RL78 Microcontroller, Micrium Press, September 2013, ISBN: 978-1-935772-96-5

Low Power MCU:s

Manufacturer	Symbol	Core	Frequency	Flash	RAM
STM	STM32F042x	ARM® 32-bit Cortex®-M0	Up to 48 MHz	16 to 32 kB	6 kB
NXP	LPC122x	ARM® 32-bit Cortex®-M0	Up to 45 MHz	Up to 128 kB	8 kB
NI	MSP430FR6972	16-Bit RISC Architecture	Up to 16 MHz	64 kB	2 kB
Microchip	ATSAM4S2B	ARM® 32-bit Cortex®-M4	Up to 120 MHz	128 kB	64 kB

Expected Results

- Execution Times
- MCU usage
- Memory usage
- Code size
- Overhead

Future Work

- Feasibility of security services
- Computation requirements
- Impact of encryption techniques
- Impact of embedded solution
- Performance requirement for cryptographic tasks
- Computational and memory usage overhead

Conclusion

- Assuring Security is essential
- Cryptography is very expensive on CPU/Memory
  - Based on advance mathematical operations
  - It needs to be efficient

'If you think cryptography is the solution to your problem, then you don't understand your problem'

Roger Michael Needham (9 February 1935 – 1 March 2003)

AGH

Thank You