From Hardware to Software to System: Trusted embedded Nodes in IoT

APOSTOLOS P. FOURNARIS, PHD

POSTDOCTORAL RESEARCH FELLOW, UNIVERSITY OF PATRAS, GREECE

ADJUNCT FACULTY MEMBER, TECHNOLOGICAL EDUCATIONAL INSTITUTE OF WESTERN GREECE
Presentation outline

- Research motivation
- Exploring alternative number systems for Cryptography algorithm leakage attacks resistance
- Exploring overhead of public key arithmetic building blocks
- Building trusted IoT devices
- The sense-city smart city concept
- Introducing blockchain contracts in the smart city concept
IoT devices cannot be trusted

- IoT devices are left without surveillance
- End nodes to broad IoT ecosystem
- Can be an attack vector for the whole IoT ecosystem
- Extracting though leakage traces the IoT sensitive information is not hard....
  - Side channel Analysis Attacks,
  - Fault Injection Analysis Attacks
  - Due to resources restriction many end node device are not well protected against leakage attacks

• Which solutions can be applicable to the embedded system world?
• Are all countermeasures applicable in IoT embedded system devices?

Current Focus point: Use of alternative number systems as public key leakage attack countermeasures
RNS as leakage attack countermeasure

RNS not only for parallelism, performance enhancement

RNS being a non-positional system and capable of redundancy and fault tolerance can be used for fault attack resistance

RNS Montgomery Multiplication (Base Extension) key fault detection mechanism

X: Binary Number

\[ X \in \text{RNS} \]

Set of independent elements \( x_i \) on a given Base \( B_n = \{m_1, m_2, \ldots, m_n\} \)

**Pool of 2n RNS Base moduli**

\[
\begin{align*}
    b_1 & \quad b_2 & \quad b_3 & \quad b_4 & \quad \ldots & \quad b_{2n-3} & \quad b_{2n-2} & \quad b_{2n-1} & \quad b_{2n} \\
    m_1 & \quad m_2 & \quad \ldots & \quad m_{n-1} & \quad m_n \\
    b_1 & \quad b_3 & \quad \ldots & \quad b_{2n-3} & \quad b_{2n} \\
    m_1 & \quad m_2 & \quad \ldots & \quad m_{n-1} & \quad m_n \\
    b_{2n-2} & \quad b_2 & \quad \ldots & \quad b_4 & \quad b_{2n-1} \\
    m_{n+1} & \quad m_{n+2} & \quad \ldots & \quad m_{2n-1} & \quad m_{2n} \\
    b_{2n-1} & \quad b_{2n} \\
    m_{n+1} & \quad m_{2n-1} & \quad m_{2n} 
\end{align*}
\]

Random placement (permutation) of \( n \) moduli as \( B_n \) and the remaining \( n \) moduli as \( B'_n \)

Leak Resistant Arithmetic technique (LRA) (2004, J.C. Bajard et al)

Used in RNS Montgomery Modular multiplication (needs 2 RNS bases)

**Mod Exponentiation**

(eg. RSA)

Once per round

Rerandomize bases

**Scalar multiplication**

(ECC)

Once per round

Rerandomize bases
Towards a Trusted IoT end device

- Includes strong security features
  (AES + ECC → authentication, key agreement, secure storage)
  (Distributed certification schemes, homomorphic encryption schemes)
- Leakage attack resistant design (hardware + software)
- Secure code design (use of GlobalPlatform Trusted Execution Environment, ARM TrustZone and/or TPM)
- Hardware virtualization approach....(VirISA environment concept)
- Support for Application level security protocols (secure CoAP with TLS/DTLS)
VirISA: Recruiting Virtualization and Reconfigurable Processor ISA for Malicious Code Injection Protection

- run-time execution environment with limited capabilities by explicitly and intentionally reducing the processor ISA
- In this environment, host programs have instructions of the limited ISA subset.
- An attacker can’t know the exact employed limited ISA.
- malicious injected code will have instructions that are not part of the ISA and won’t be executable
- We end up with a low-level protection scheme that cannot be bypassed

Example:
1. **Stop support of indirect memory addressing modes** (used to implement pointer-like operations)
2. **host process code re-written** (either by the programmer or by employing dynamic binary rewriting techniques) → does not rely on pointer indirections.
3. In a typical malicious code, its operation is heavily relied on pointer-based indirections in order to alter and migrate the dynamic execution.
4. So, the malicious code **not runnable** in this environment.
VirISA code injection Protection

Trusted VirISA VM 1
- VirISA VM 1 Dedicated ISA, executable
- Host Process Y
- Malicious code Injection attack on Y
- VirISA driver

Trusted VirISA VM n
- VirISA VM n Dedicated ISA, executable
- Host Process Y
- Malicious code Injection attack on Y
- VirISA driver

UnTrusted VirISA VM
- VirISA VM Full ISA Compiled
- Non Critical PROGRAM A
- ...
- VirISA VM Full ISA Compiled
- Non Critical PROGRAM A
- VirISA VM Full ISA Compiled
- Operating System
- VirISA driver

VirISA virtualization Environment

Computer System Hardware/Processor

Full Instruction Set Architecture
The sense.city Platform

What’s happening in the city
Citizens are the city sensors! Using own communication devices, through the sense.city mobile application they update their fellow citizens and the municipality of problems and incidents that occur every moment.

Urban participation
Actively participate in the processes and solve problems concerning your life in the city. Help in urban development and better relationship between citizens and administration services of the city.

Co-creativity
The sense.city platform provides the tools to enable citizens, and calls for collective thinking and actions both citizens and administration services.
http://sense.city
http://patras.sense.city
http://athens.sense.city

http://api.sense.city:3000 (node.js)
mongoDB

Backend RESTful sense.city API

Mobile app

Intel® XDK

Develop, test & deploy your mobile apps & games to all platforms

Get it on Google Play
Available on the App Store

CloudVille
(Network Architecture Management (NAM) Group)

3rd party apps and IoT smart devices

Trusted end node Devices
(Secure Sensor data collection and processing)

LoRA Gateways

Trusted gateways- arbiters
(Intermediate Trusted entities nodes)
Open Hardware – Open Software ecosystem for Security and Trust

- Introducing reward mechanism through blockchain technology in the sense.city platform
- 3rd party Microcommunities having access to the sense.city infrastructure (sensor data collection and sharing) in a secure, authorized way preserving privacy.
- Blockchain based Contracts
- A research platform for testing security and trust potentials
Thank you!

END OF PRESENTATION