Cryptographic Hardware and Software

CICC’17 Panel on
Hardware and Software Security; Gaps and Synergies

Patrick Schaumont
Bradley Department of Electrical and Computer Engineering, Virginia Tech
Cryptography is about Bits you can Trust

Virtual

Internet

Real

Social
Stats
Alert
Real time

Cloud
Mobile
Gateway
Medical IWMD

Bits Trust
Information Security
Physics Truth
Information Security Services

Four essential security services
• Access Authorization
• Key Exchange
• Data Confidentiality
• Data Authentication
Building Secure Crypto for Things

“Standard” Crypto
AES-128
SHA2, SHA3
ECC, RSA, ECDH, DH

“Things” Crypto

Brute Force Security
Computational Security
Implementation Security

Must satisfy all of these at the same time
Implementation Security

Internet

\[\downarrow\] \[\uparrow\]

I/O

Task

Secure Task

OS

Hardware

Connected Platform

I/O Attacker Model

Brute Force Security
Computational Security
Implementation Security

Better Software
Implementation Security

- Internet
- I/O
- Task
- Secure Task
- OS
- Hardware

I/O Attacker Model
Machine Code Attacker Model

Better Software
Secure Architecture Isolation
Implementation Security

- Internet
- I/O Attacker Model
- Machine Code Attacker Model
- Hardware Attacker Model

- I/O
- Secure Task
- OS
- Hardware

- Connected Platform

Brute Force Security
Computational Security
Implementation Security

Better Software
Secure Architecture Isolation
Composable Countermeasures

Faults, EM, Side-channels, Timing, Tamper, Resilience, debug, decap, ...
Example – Side-channels

Software

Secret $S$ is used in
- Memory Lookup
- Control Flow Decision
- Computation
Example – Side-channels

Secret S is used in
- Memory Lookup
- Control Flow Decision
- Computation

Secret S may cause
- Cache Timing
- Instruction Timing
- I/O Timing
Example – Side-channels

**Software**
- Secret S is used in:
  - Memory Lookup
  - Control Flow Decision
  - Computation

**Architecture**
- Secret S may cause:
  - Cache Timing
  - Instruction Timing
  - I/O Timing

**Circuit**
- Secret S may cause:
  - EM Side-channel
  - Power Side-channel
  - Fault-based Side-Channel