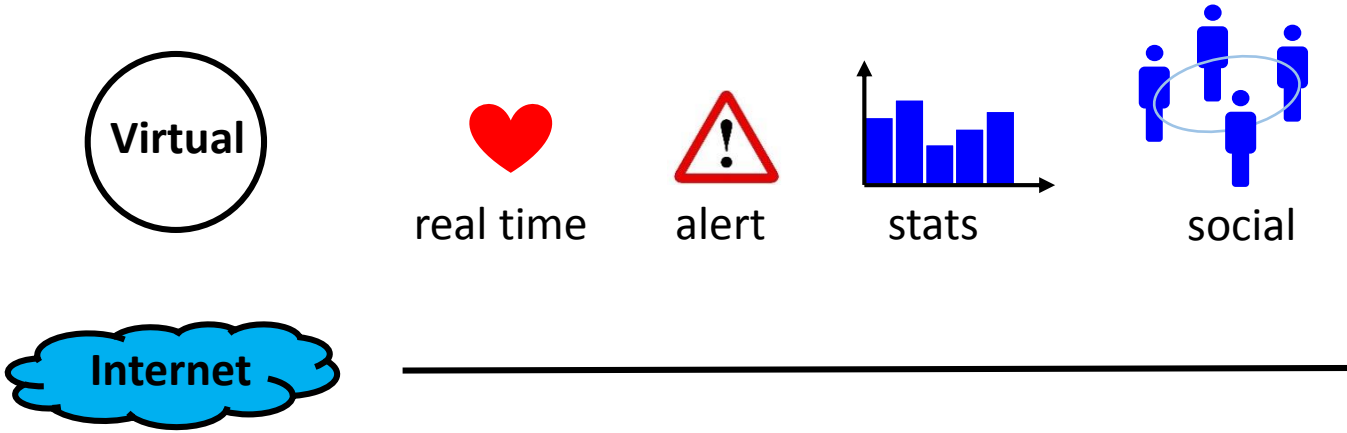
DATE 17
DESIGN, AUTOMATION & TEST IN EUROPE
27 – 31 March, 2017 · STCC · Lausanne · Switzerland
The European Event for Electronic
System Design & Test

Security in the Internet of Things: A Challenge of Scale

Patrick Schaumont
Bradley Department of Electrical and Computer Engineering

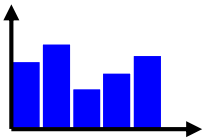
Internet of Things



Internet of Things

real time

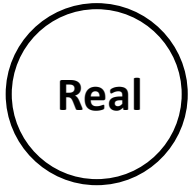
alert



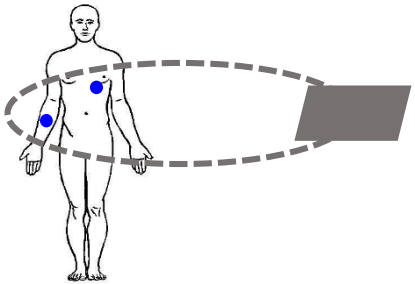
stats

social

Bits
Trust



Medical IWMD



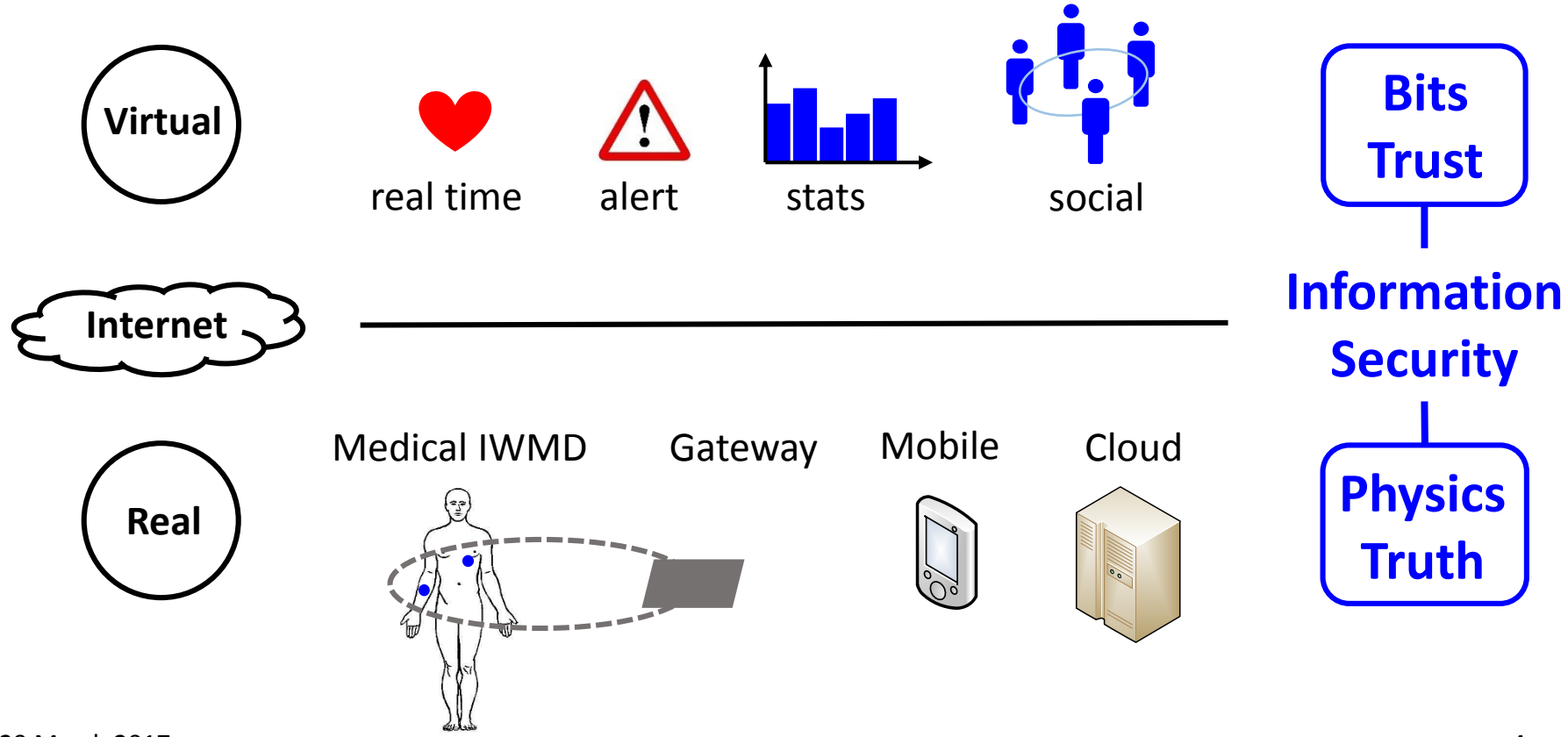
Gateway

Mobile

Cloud

Physics
Truth

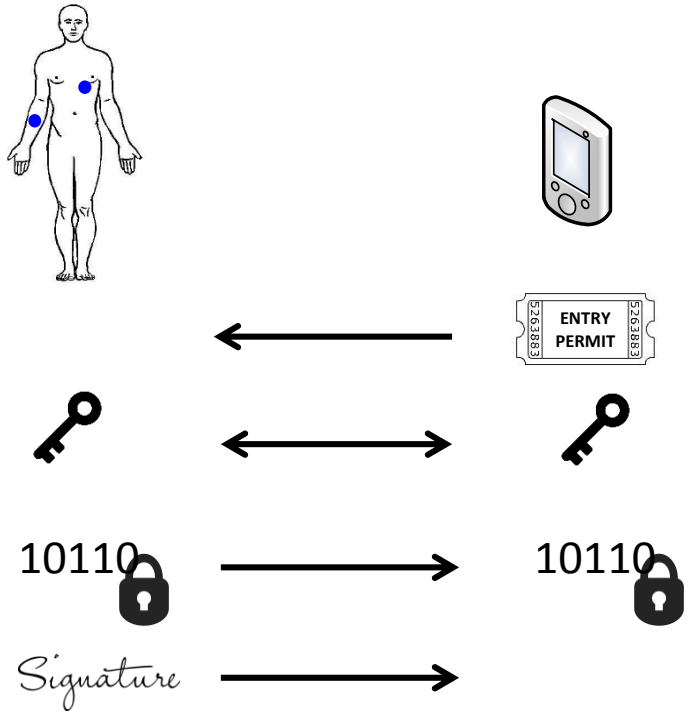
Internet of Things



Security Services

Four essential security services

- **Access Authorization**
- **Key Exchange**
- **Data Confidentiality**
- **Data Authentication**

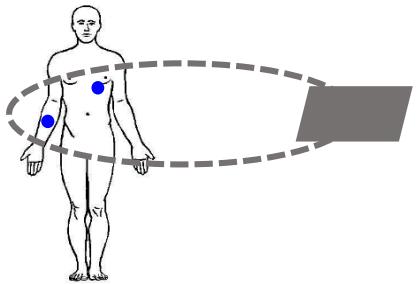


Standard Crypto Algorithms

	Symmetric Key		*Public Key*	
	Symmetric Encryption	**Message Authentication**	**Signatures**	**Diffie Hellman**
Confidentiality	✓			
Authentication		✓	✓	
Key Exchange	✓ (PSK)			✓
Standard Crypto	**AES-128**	**SHA2, SHA3**	**ECC, RSA**	**ECDH, DH**

How to build Crypto for *Things*?

Medical IWMD Gateway Mobile Cloud



“Things” Crypto

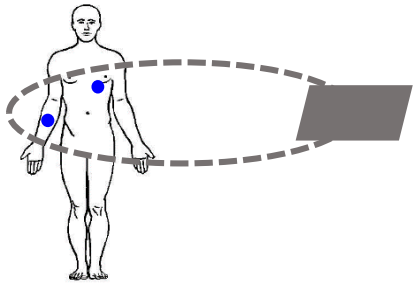
?

“Standard” Crypto

AES-128
SHA2, SHA3
ECC, RSA,
ECDH, DH

How to build Crypto for *Things*?

Medical IWMD Gateway Mobile Cloud



Long Lifetime

Low Footprint

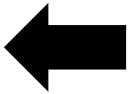
Low Latency

Low Energy

New Attack Models

“Things” Crypto

?



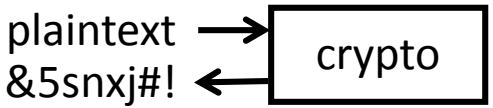
“Standard” Crypto

AES-128
SHA2, SHA3
ECC, RSA,
ECDH, DH

What is *secure* Information Security?

- **Brute Force Security**

- **Computational Security**



- **Implementation Security**

Brute Force Security

Brute Force Security implied through key-length under Von Neumann computing

Primitive	Symmetric Encryption	Message Authentication	Signatures	Diffie Hellman
Algorithm	AES-128	SHA2, SHA3	ECC, RSA	ECDH, DH

Brute Force Security

Brute Force Security implied through key-length under Von Neumann computing

Primitive	Symmetric Encryption	Message Authentication	Signatures	Diffie Hellman
Algorithm	AES-128	SHA2, SHA3	ECC, RSA	ECDH, DH

However ..

Increased Computational Cost

Post Quantum	AES-256	SHA-512 SHA3-512

Brute Force Security

Brute Force Security implied through key-length under Von Neumann computing

Primitive	Symmetric Encryption	Message Authentication	Signatures	Diffie Hellman
Algorithm	AES-128	SHA2, SHA3	ECC, RSA	ECDH, DH

However ..

	Increased Computational Cost		New Algorithm	
Post Quantum	AES-256	SHA-512 SHA3-512	Lattice Based Hash Based Code Based	Lattice Based

Computational Security

Current algorithms trusted, but IoT constraints require innovation

Primitive	Symmetric Encryption	Message Authentication	Signatures	Diffie Hellman
Algorithm	AES-128	SHA2, SHA3	ECC, RSA	ECDH, DH

Lightweight Cryptography: Jointly Optimize {Security, Performance, Area}

Computational Security

Current algorithms trusted, but IoT constraints require innovation

Primitive	Symmetric Encryption	Message Authentication	Signatures	Diffie Hellman
Algorithm	AES-128	SHA2, SHA3	ECC, RSA	ECDH, DH

Published Proposals since 2005

Lightweight Cryptography	21 Block 4 Stream	8 Hash 5 Auth Enc

Computational Security

Current algorithms trusted, but IoT constraints require innovation

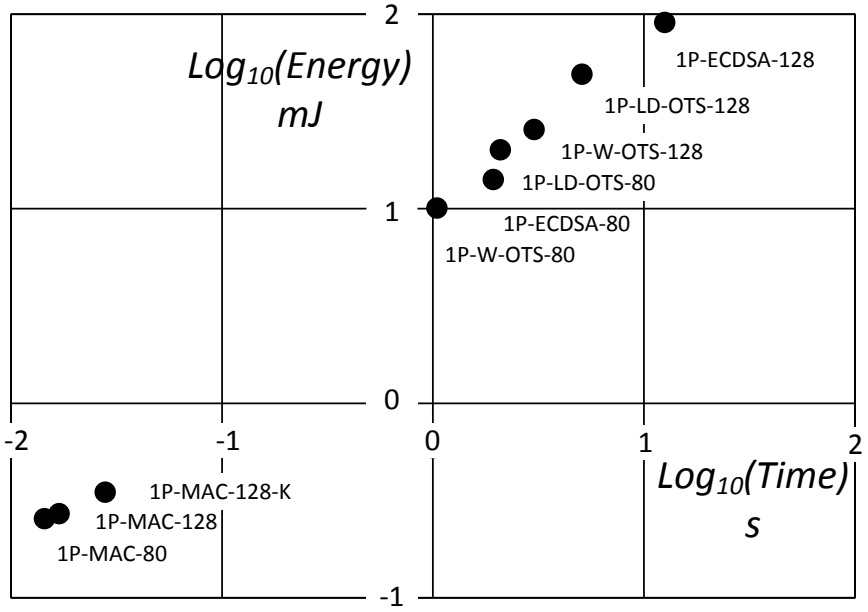
Primitive	Symmetric Encryption	Message Authentication	Signatures	Diffie Hellman
Algorithm	AES-128	SHA2, SHA3	ECC, RSA	ECDH, DH

	Published Proposals since 2005		Hardly any choice ?	
Lightweight Cryptography	21 Block 4 Stream	8 Hash 5 Auth Enc	?	?

Public-Key Crypto in Constrained Environment

Authentication Protocol

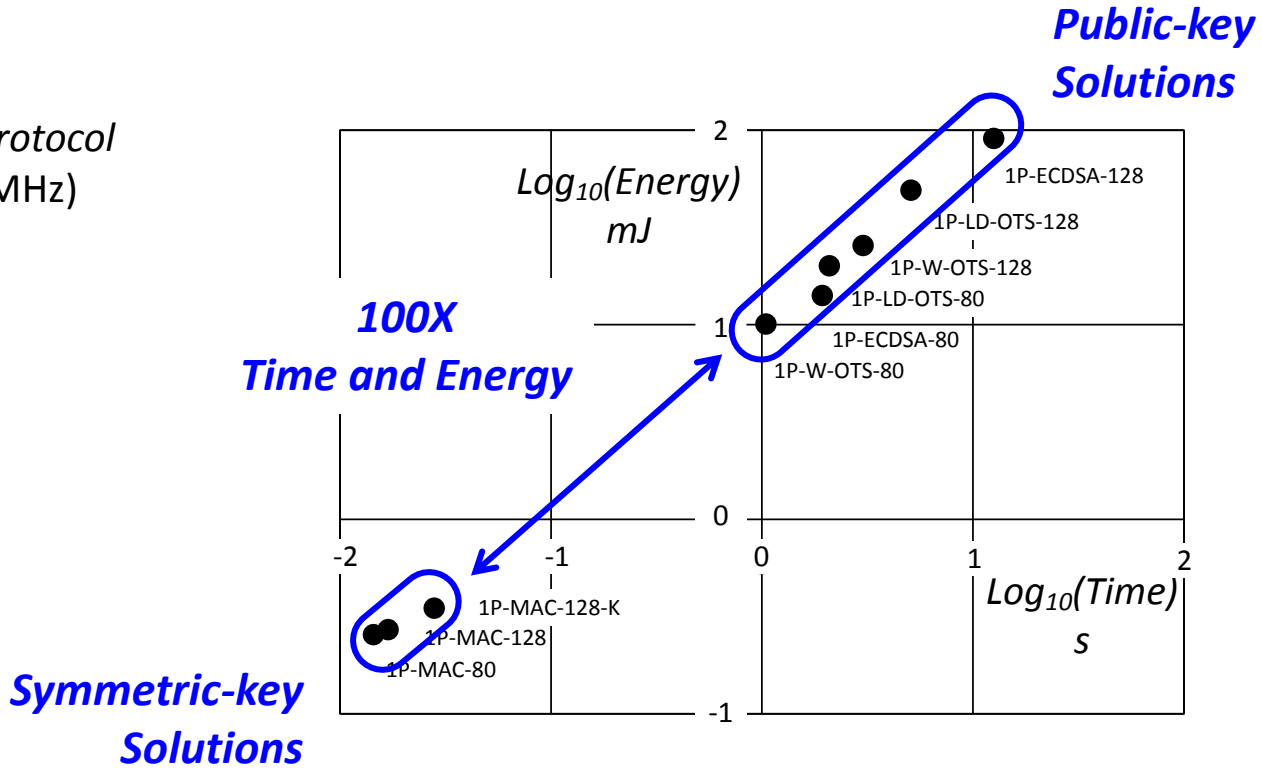
- MSP430 (10 MHz)
- CC2500 RF



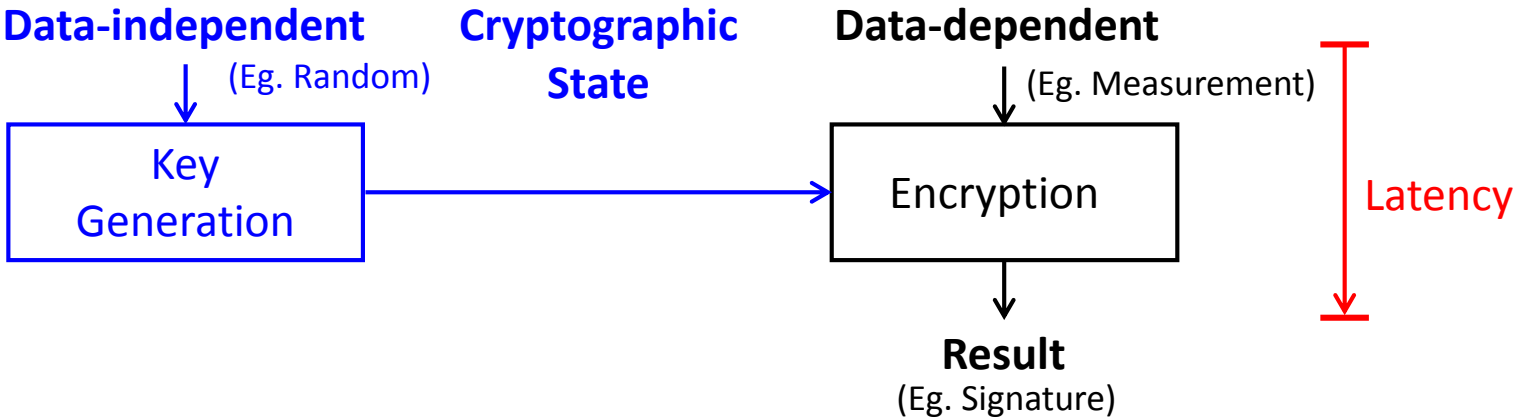
Public-Key Crypto in Constrained Environment

Authentication Protocol

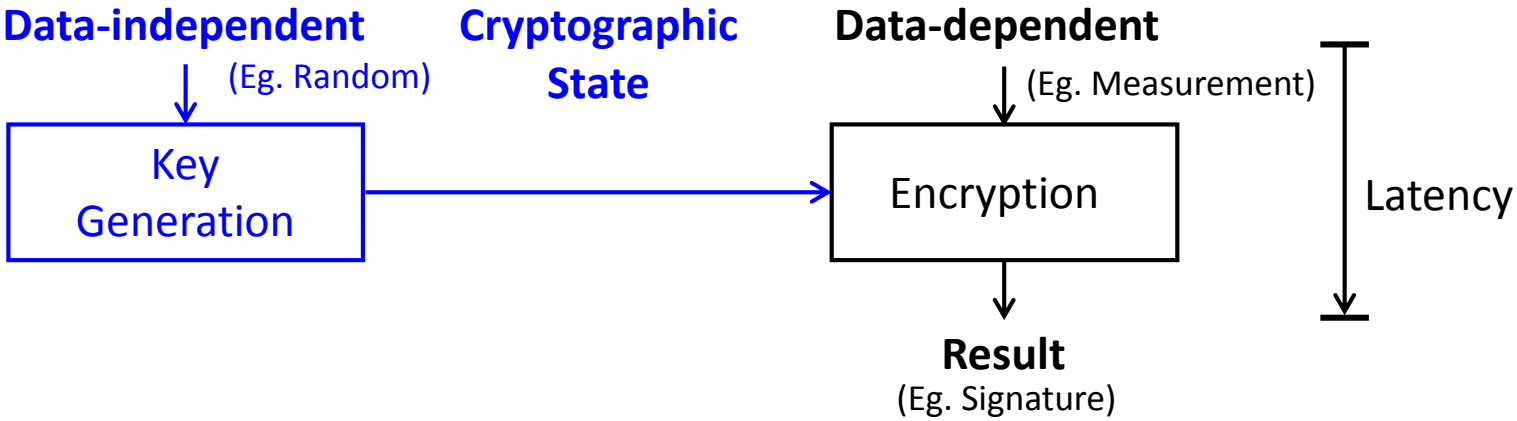
- MSP430 (10 MHz)
- CC2500 RF



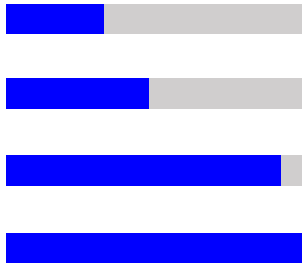
Precomputed Security



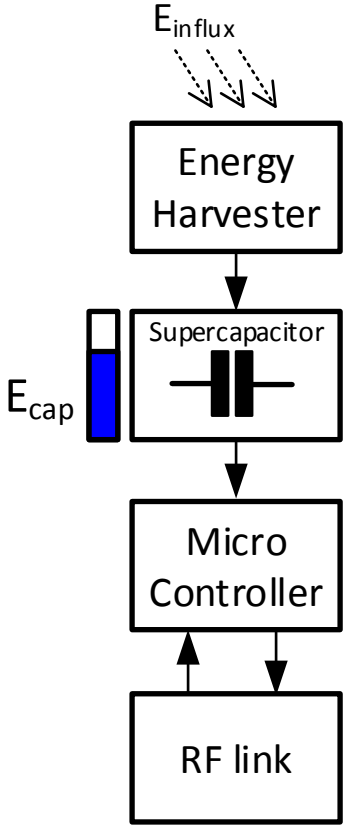
Precomputed Security

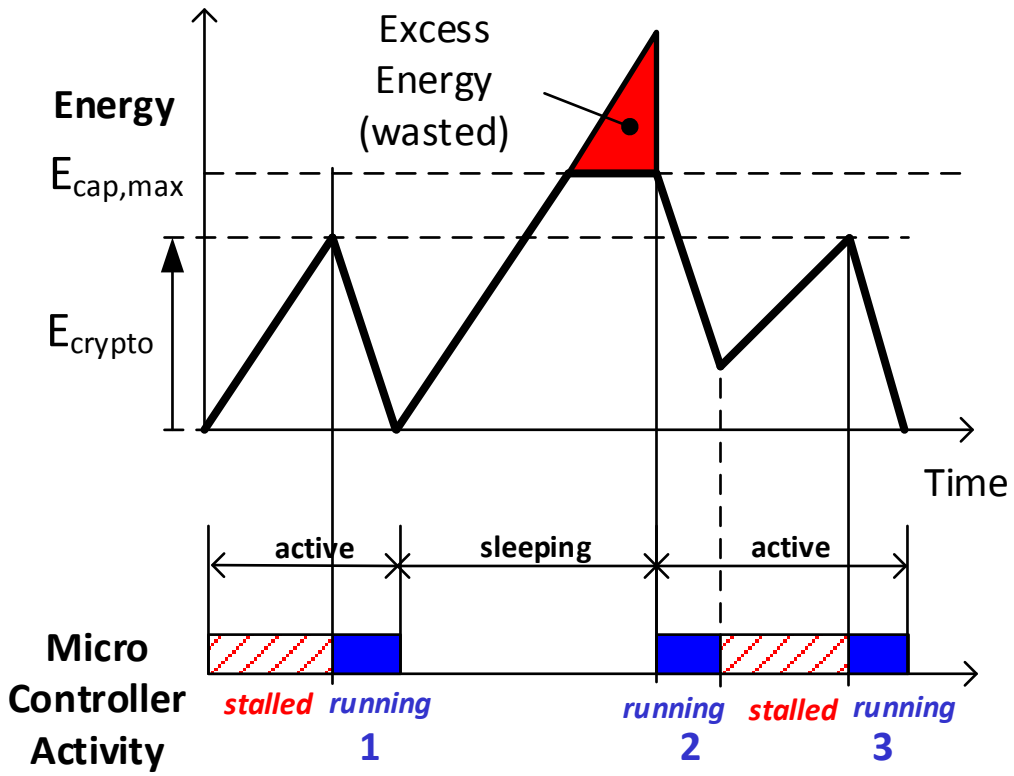


AES	Roundkey Exp	Encryption
DTLS	½ DH Key Exchange	½ DH Key Exchange
ECDSA	Point Mult	Mod Mul
TRNG	Entropy Harvesting	

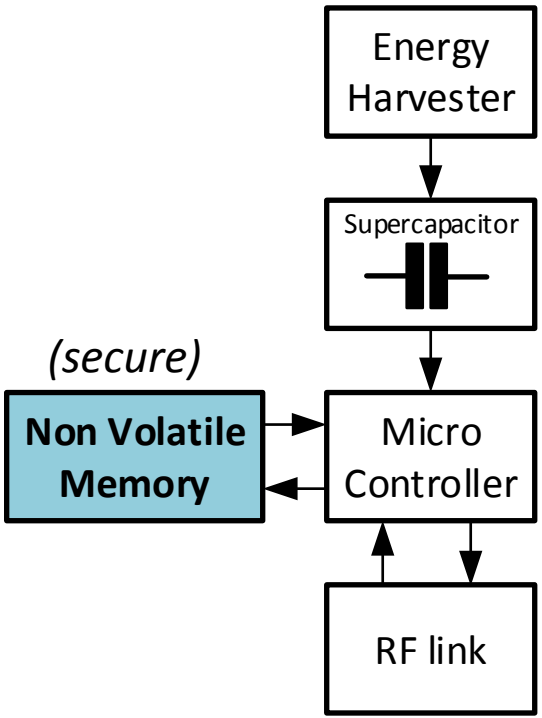


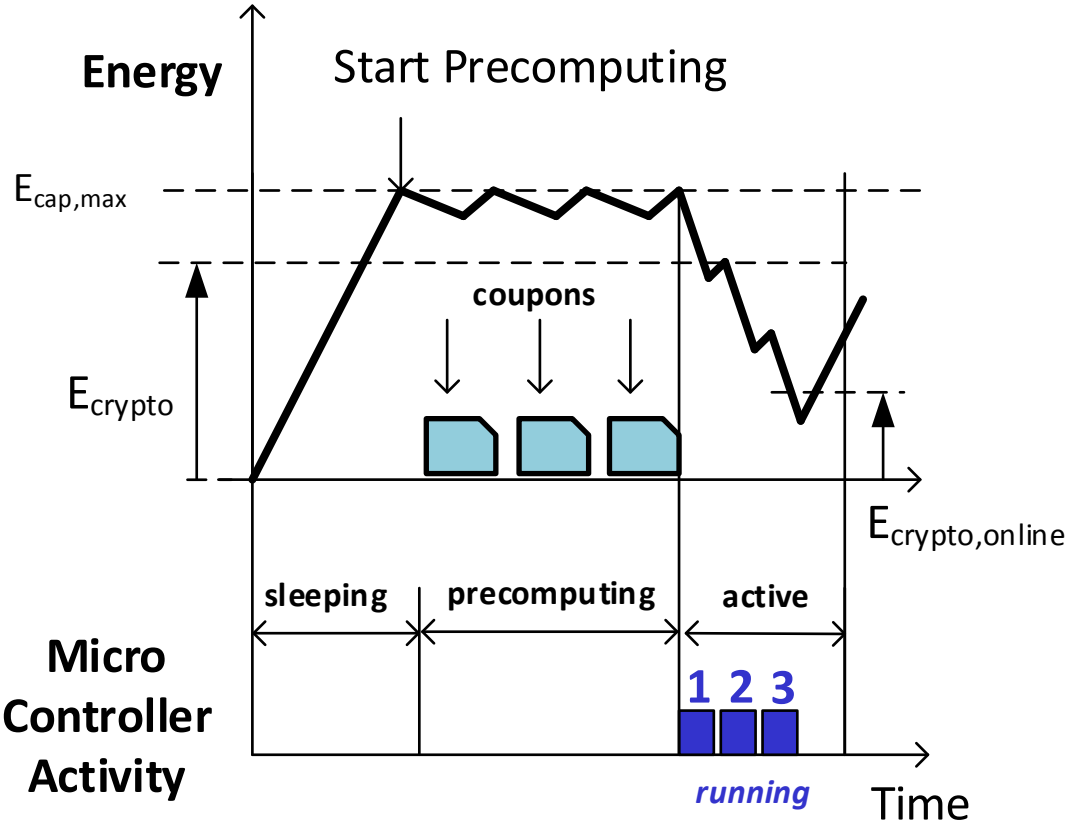
EH Operation *without* precomputing





EH Operation *with* precomputing

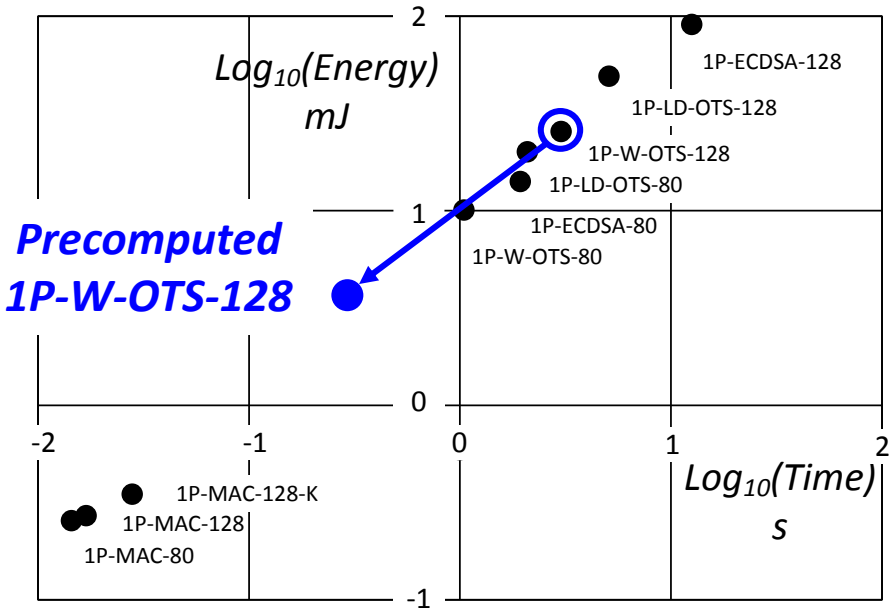




Energy-Driven Computing

Authentication Protocol

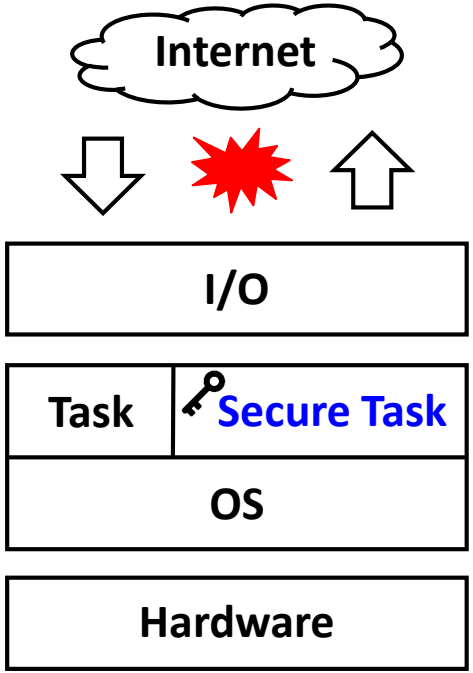
- MSP430 (10 MHz)
- CC2500 RF



Energy Reduction: 11.8X

Latency Improvement: 10.1X

Implementation Security

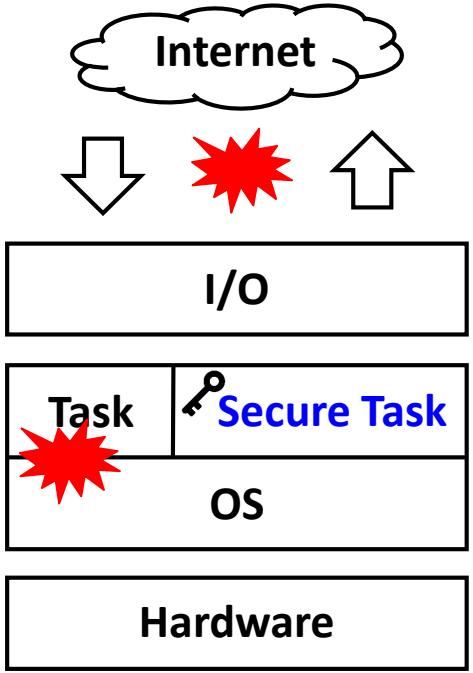


Connected Platform

I/O Attacker Model

Better Software

Implementation Security



Connected Platform

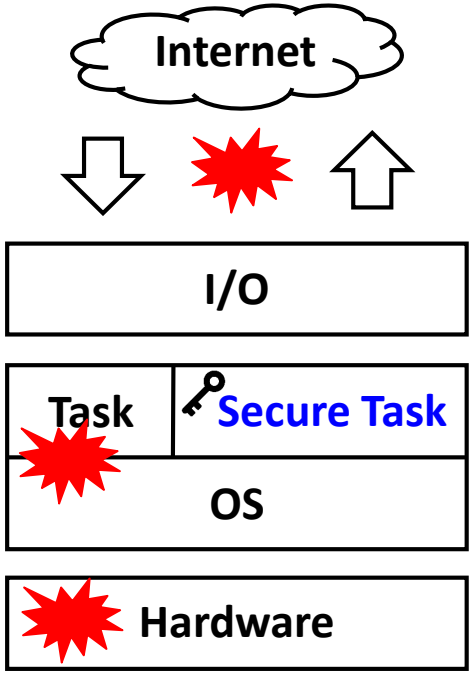
I/O Attacker Model

Machine Code Attacker Model

Better Software

Secure Architecture Isolation

Implementation Security



Connected Platform

I/O Attacker Model

Machine Code Attacker Model

Hardware Attacker Model

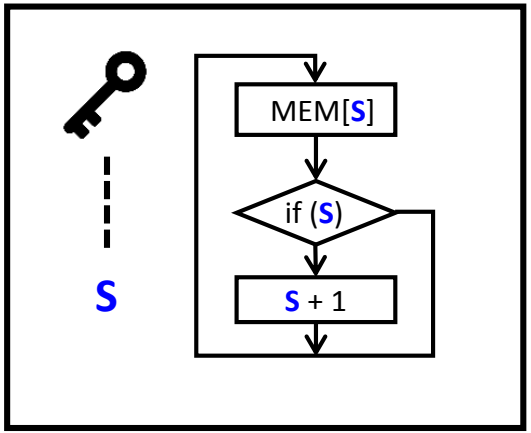
Better Software

Secure Architecture
Isolation

? Composable ?
Countermeasures

Example – Side-channels

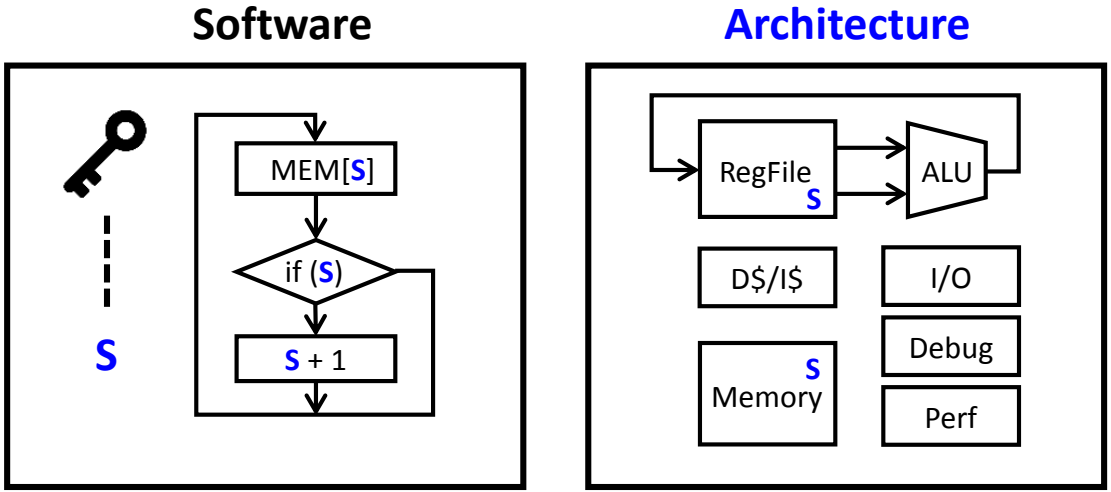
Software



Secret S is used in

- Memory Lookup
- Control Flow Decision
- Computation

Example – Side-channels



Secret S is used in

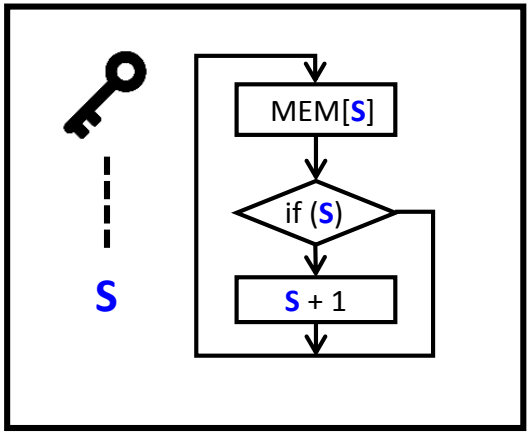
- Memory Lookup
- Control Flow Decision
- Computation

Secret S may cause

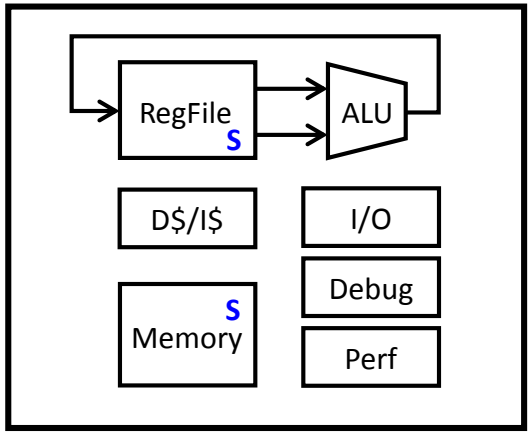
- Cache Timing
- Instruction Timing
- I/O Timing

Example – Side-channels

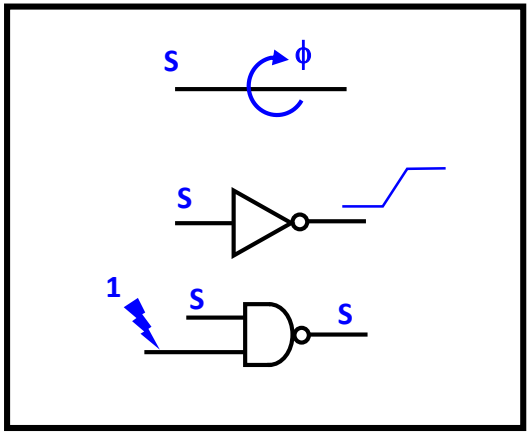
Software



Architecture



Circuit



Secret S is used in

- Memory Lookup
- Control Flow Decision
- Computation

Secret S may cause

- Cache Timing
- Instruction Timing
- I/O Timing

Secret S may cause

- EM Side-channel
- Power Side-channel
- Fault-based Side-Channel

Conclusions

- **IoT Security builds on comprehensive solutions for**
  - **Brute-force Security**
  - **Computational Security**
  - **Implementation Security**
- **Plenty of *hard* problems remain**
  - **Public-key cryptography in Energy/resource-constrained context**
  - **Composable Countermeasures (Timing, Power, Faults, ..)**
  - **Design Correctness, Implementation Correctness, Operation Correctness**

Thank you for your attention!

Patrick Schaumont
schaum@vt.edu