Security Challenges in Cyber-Physical Systems

Francesco Regazzoni

Contents

1. Cyber-Physical Systems
2. Cyber Security
3. Physical Security
4. Long-Term Security
5. Security of Machine Learning
6. Physical on Physical
7. Cyber on Physical

Cyber-Physical Systems

What is an autonomous system?

- Yet another definition....
- Autonomous Cyber-Physical System

Cyber-

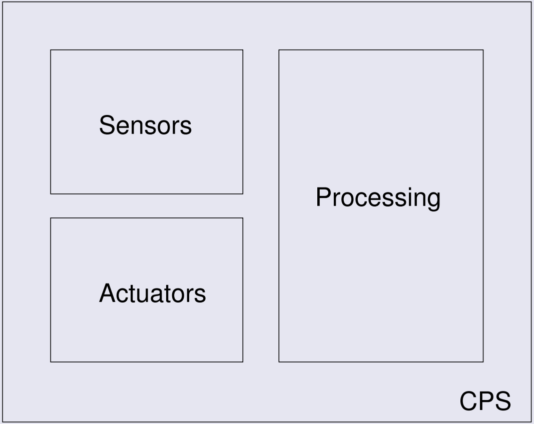
- Computational Element
- Some “intelligence”
- Network Connected

-Physical

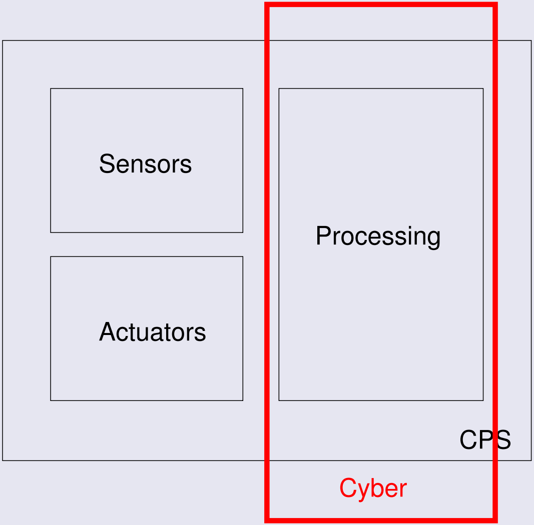
- Sensors
- Actuators

Cyber-Physical Systems

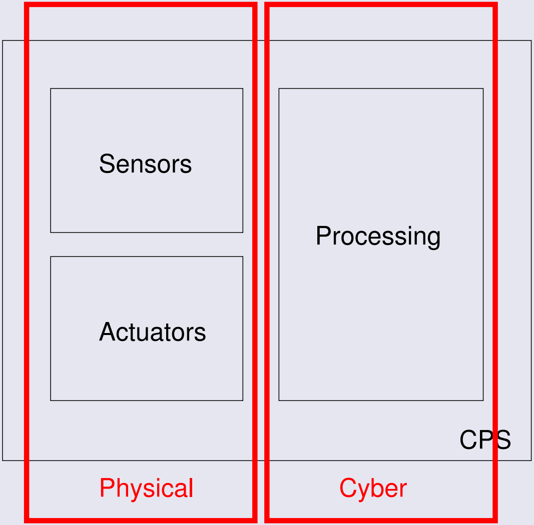
Cyber-Physical Systems Schema



Cyber-Physical Systems Schema



Cyber-Physical Systems



Applications of Autonomous systems

- Medical
- Critical Infrastructure
- You mention...

Contents

1 Cyber-Physical Systems

2 Cyber Security

3 Physical Security

4 Long-Term Security

5 Security of Machine Learning

6 Physical on Physical

7 Cyber on Physical

Confidentiality

Attempt to gain access to **data stored/handled** or to the **IP**

Integrity

It is related to the absence of **undesired malicious modifications**

Authenticity

It is related to the authenticity of **components** and **data**

Security, the big picture

	Cyber	Physical
Cyber		
Physical		

Let’s start from the Cyber-

- Virus-Malware
- Network attacks
- You mention...

Malware

Network Attacks

Hardware Trojans

Contents

1. Cyber-Physical Systems
2. Cyber Security
3. **Physical Security**
4. Long-Term Security
5. Security of Machine Learning
6. Physical on Physical
7. Cyber on Physical

Why Physical Security is so Important Today?

Long Time Ago   Past   Present

Mainframes   Personal Computer   Pervasive

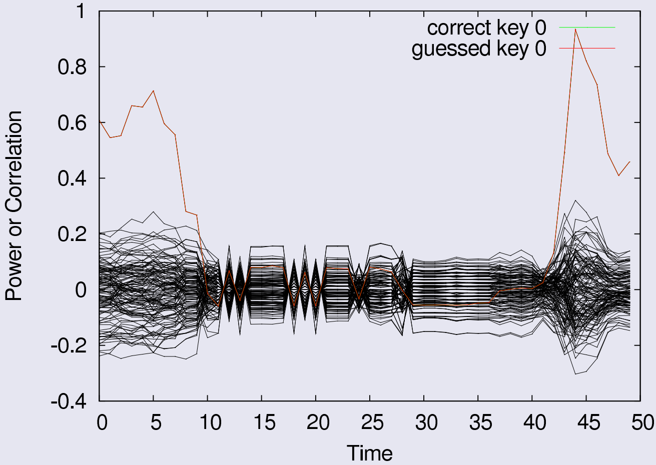
Power Analysis Attacks

Power Analysis Attacks exploit the relation between the power consumed and the processed data.

- Cheap
- Powerful

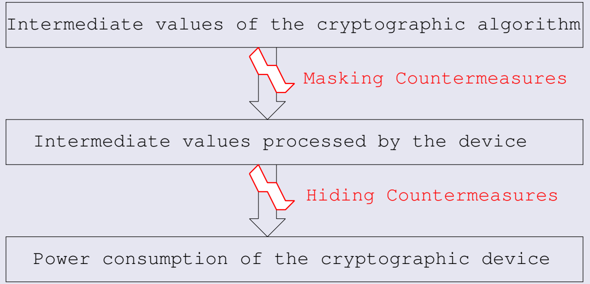
Example of Differential Power Attacks

Simulate whole embedded processor at SPICE



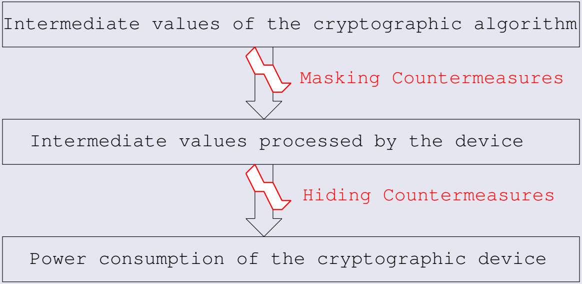
Countermeasures

Power consumption **independent** from processed key dependent data


Intermediate values of the cryptographic algorithm
Masking Countermeasures
Intermediate values processed by the device
Hiding Countermeasures
Power consumption of the cryptographic device

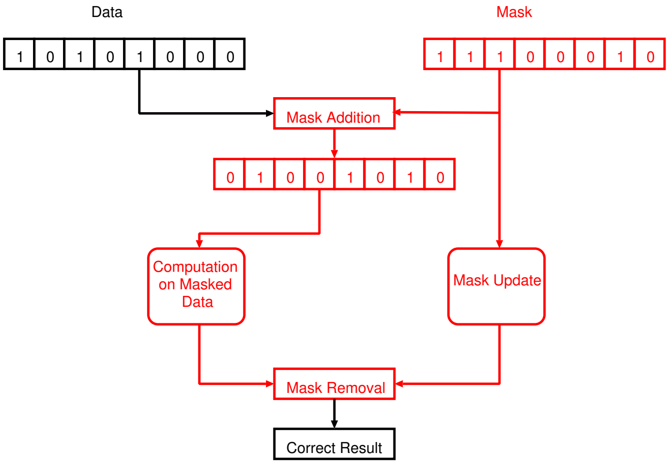
Countermeasures

Power consumption **independent** from processed key dependent data


Intermediate values of the cryptographic algorithm
Masking Countermeasures
Intermediate values processed by the device
Hiding Countermeasures
Power consumption of the cryptographic device

They can be implemented in **Software** or in **Hardware**

More Details on Masking



Data

1 0 1 0 1 0 0 0

Mask

1 1 1 0 0 0 1 0

Mask Addition

0 1 0 0 1 0 1 0

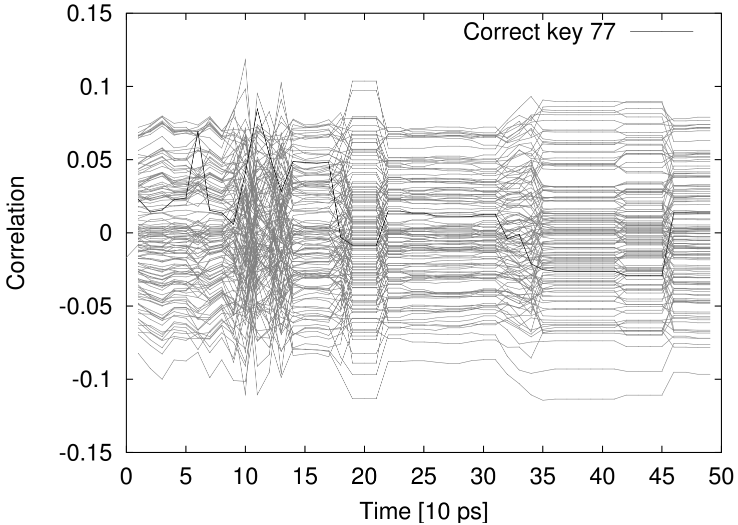
Computation on Masked Data

Mask Update

Mask Removal

Correct Result

More Details on Hiding



Timing Attacks

- **Goals**: The adversary attempt to recovery the secret key exploiting the time difference of of the instructions
- **Requirements**: Knowledge about the algorithm

- Spy process
- Hardware performance registers
- Visual inspection

Countermeasures

- Avoid branches dependent from secret data
- Compute secret data always in constant time

Fault Attacks

- **Goals**: The adversary attempt to recovery the secret key exploiting the relation between a faulty output and the correct one
- **Requirements**: Fault in the right position

- Laser or equivalent
- Control of the power supply

Countermeasures

- Add space redundancy
- Add time redundancy

Contents

1. Cyber-Physical Systems
2. Cyber Security
3. Physical Security
4. **Long-Term Security**
5. Security of Machine Learning
6. Physical on Physical
7. Cyber on Physical

Long-term security

- Autonomous systems have lifetime longer than consumer electronic systems
- Systems are exposed to more powerful attack and to unknown attacks

Post-quantum cryptography

- Quantum computational power would make insecure our current public key network
- Transition towards post-quantum cryptography is under standardization

Crypto-agility

- “Capability to update cryptographic functionality of a system”

- Possible at algorithmic level or at device level (reconfigurable blocks specifically dedicated to cryptography)

Lightweight

Light-

weight?

- Area
- Power
- Energy

Contents

1 Cyber-Physical Systems

2 Cyber Security

3 Physical Security

4 Long-Term Security

5 Security of Machine Learning

6 Physical on Physical

7 Cyber on Physical

Security of Machine learning

Autonomous systems include artificial intelligence

Protecting the IP of AI

- Training AI algorithms is a costly process
- Parameters of AI algorithms needs to be protected

Protecting from adversarial machine learning

- Malicious input data used to mislead machine learning algorithms
- Very relevant case: road signals

Contents

1 Cyber-Physical Systems

2 Cyber Security

3 Physical Security

4 Long-Term Security

5 Security of Machine Learning

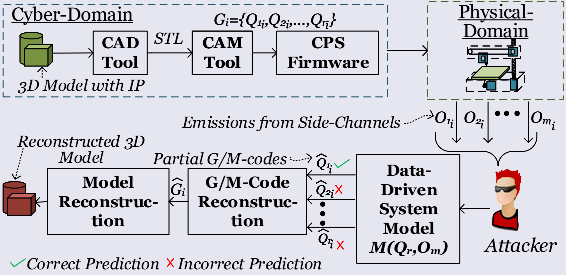
6 **Physical on Physical**

7 Cyber on Physical

Physical on Physical

3D printer

Physical on Physical



Cyber-Domain

3D Model with IP

CAD Tool

STL

CAM Tool

$G_i=\{Q_{1_i},Q_{2_i},\dots,Q_{r_i}\}$

CPS Firmware

Physical-Domain

Emissions from Side-Channels

O_{1_i} O_{2_i} • • • O_{m_i}

Attacker

Data-Driven System Model $M(Q_r,O_m)$

Partial G/M-codes

$\widehat{Q}_{1_i}$ ✓

$\widehat{Q}_{2_i}$ ✗

$\widehat{Q}_{r_i}$ ✗

G/M-Code Reconstruction

$\widehat{G}_i$

Model Reconstruction

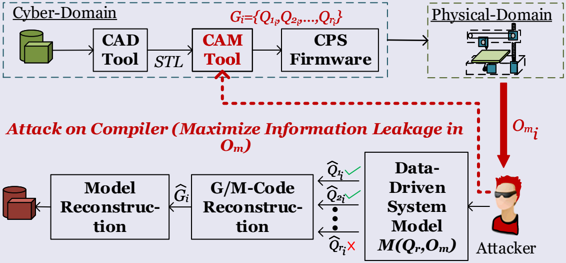
Reconstructed 3D Model

✓ Correct Prediction ✗ Incorrect Prediction

Contents

1. Cyber-Physical Systems
2. Cyber Security
3. Physical Security
4. Long-Term Security
5. Security of Machine Learning
6. Physical on Physical
7. **Cyber on Physical**

Cyber on Physical



Cyber-Domain

CAD Tool

STL

CAM Tool

$G_i=\{Q_{1_i},Q_{2_i},\ldots,Q_{r_i}\}$

CPS Firmware

Physical-Domain

O_{m_i}

Attack on Compiler (Maximize Information Leakage in O_m)

Model Reconstruction

$\widehat{G}_i$

G/M-Code Reconstruction

$\widehat{Q}_{1_i}$ ✓

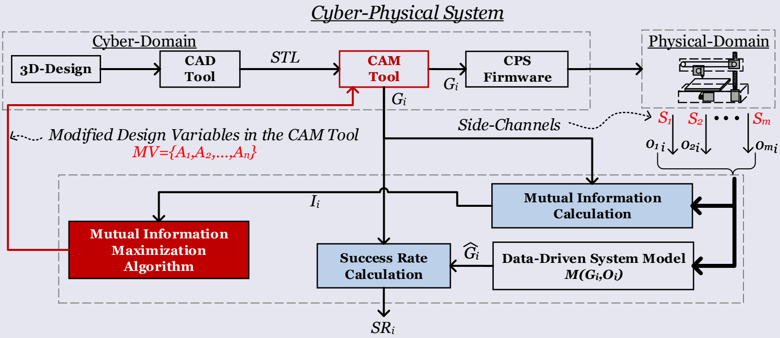
$\widehat{Q}_{2_i}$ ✓

$\widehat{Q}_{r_i}$ ✗

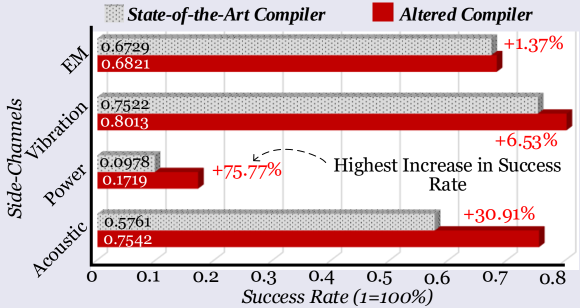
Data-Driven System Model $M(Q_r,O_m)$

Attacker

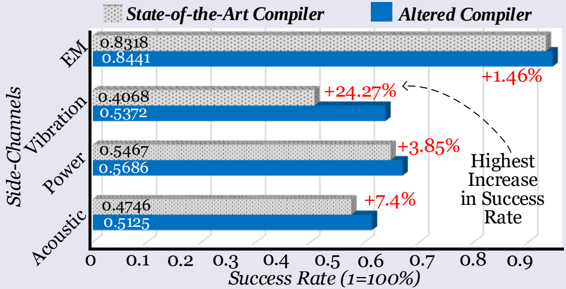
Cyber on Physical



Cyber on Physical



Cyber on Physical



Conclusions

- Security is a crucial extra-functional requirement for cyber-physical systems
- We cover only half of the problem...

Questions?

Thank you for your attention!

mail: regazzoni@alari.ch

Acknowledgment

CERBERO project, EU Commissions H2020 Program, grant agreement N. 732105