1. PRESENTATION

2. CYBER-PHYSICAL SYSTEMS
   2.1 Presentation
   2.2 Networked control systems
   2.3 Cyber-physical attacks

3. PIETC-WD
   3.1 Presentation
   3.2 Normal functioning
   3.3 First sensor alarm
   3.4 Second sensor alarm
   3.5 Validation

4. CONCLUSION
PRESENTATION
Master’s Degree
Telecom SudParis
Cybersecurity specialization

Cybersecurity engineer
Thales C&S
Integration & risk analysis

2016
2017
2018

Senior Internship
University of Malaga
Trust metrics for the IoT

Research associate
(Ingénieure de recherche)
Telecom SudParis
CPS resilience

- Cryptography
- Network security (IP protocols)
- Darknets study (senior project)
- Risk analysis : EBIOS 2010

- Industrial control systems (ICS)
- SCADA systems & protocols
- Human threats in CPS : HCI, etc.
Cyber-Physical System (CPS): Systems that integrate Computation, Communication and Control-Physical processes


Moreover…

Systems with integrated computational and physical capabilities that can interact with humans through many new modalities

Cyber-physical systems have today the following features:

- **Large scale** – large number of physically distributed subsystems
- **Complex** – large number of variables, non-linear & uncertainty
- **Human in the loop** – human beings & feedback control systems

Examples:

- **Industrial control systems**
- **Intelligent transportation systems**
- **Smart cities**
- **E-health**
## Difference between ICT and ICS

<table>
<thead>
<tr>
<th></th>
<th>ICT</th>
<th>ICS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Aim</strong></td>
<td>Information protection</td>
<td>Safety of services and people</td>
</tr>
<tr>
<td><strong>Lifetime</strong></td>
<td>&lt;5 years</td>
<td>&gt;10 years</td>
</tr>
<tr>
<td><strong>Security properties priorities</strong></td>
<td>Confidentiality, Integrity, Availability</td>
<td>Availability, Integrity, Confidentiality</td>
</tr>
<tr>
<td><strong>Network</strong></td>
<td>TCP/IP</td>
<td>SCADA (and TCP/IP)</td>
</tr>
<tr>
<td><strong>Connectivity</strong></td>
<td>Connected to Internet</td>
<td>Isolated (or strong restrictions)</td>
</tr>
</tbody>
</table>
Cyber-physical resilience

- Offer **critical functionalities** (e.g. safety functions) under the presence of failures and attacks

A resilient control systems should*:

- **Identify** threats
- **Minimize** their impact
- **Mitigate** them, or recover to a normal operation in a reasonable time

*Queiroz (2012). A holistic approach for measuring the survivability of SCADA systems. PhD, RMIT University.
**Networked control system**: Control system whose control loops are connected through a communication network.

- **Modeling of CPS using feedback control theory**
- **Controller** commands the system using corrective feedback, based on the distance between a reference signal and the system output.
A **cyber-physical attack** exploits vulnerabilities, to harm the physical processes through the network.

False-data injection attack

**How:** Modification of sensors reading by physical interferences, by the communication channel or individual meters to generate wrong control decisions

**Attack capabilities:** Limited knowledge of the physical system required

**Countermeasure:** Comparison of sensor measurements and system dynamics

Replay attack

► **How**: Replay previous sensor measurements and modification of control inputs
► **Attack capabilities**: No knowledge of the physical system required
► **Countermeasure**: Add some protection on input control signals

Replay attack

► **How**: Replay previous sensor measurements and modification of control inputs

► **Attack capabilities**: No knowledge of the physical system required

► **Countermeasure**: Add some protection on input control signals

---

Replay attack

- **How**: Replay previous sensor measurements and modification of control inputs
- **Attack capabilities**: No knowledge of the physical system required
- **Countermeasure**: Add some protection on input control signals

Covert attack

- **How**: Modification of control inputs and sensor measurements
- **Attack capabilities**: Knowledge of the physical system required
- **Countermeasure**: Undetectable from the regular system operation

2 CYBER-PHYSICAL SYSTEMS
2.3 CYBER-PHYSICAL ATTACKS

DoS attack
► How: Disrupt the communication on a channel to isolate the monitor process

Zero dynamic attack
► How: Disrupt the unobservable part of the system
► Countermeasure: Verify if all the states are observable

Command injection attack
► How: Exploit protocols and devices vulnerabilities to inject false commands
► Countermeasure: Signature-based IDS

1. PRESENTATION

2. CYBER-PHYSICAL SYSTEMS
   2.1 Presentation
   2.2 Networked control systems
   2.3 Cyber-physical attacks

3. PIETC-WD
   3.1 Presentation
   3.2 Normal functioning
   3.3 First sensor alarm
   3.4 Second sensor alarm
   3.5 Validation

4. CONCLUSION
Periodic and intermittent event-triggered control watermark detector

► **System specifications:**
- Discrete linear time-invariant LTI system
- Linear Quadratic Gaussian LQG controller

► **Strategy:**
- **Challenge-response** authentication scheme
- **Non-stationary watermark-based** (noise) to verify the integrity of the control loop

► **Countermeasure** against adversaries that have partial or full knowledge of the system dynamics

► **Penalty:** performance loss

The system model is given by:

\[ x_{t+1} = Ax_t + Bu_t + w_t \]

with \( A \in \mathbb{R}^{p \times p} \) state matrix

\( B \in \mathbb{R}^{p \times m} \) input matrix

\( w_t \sim N(0, Q) \) noise

\[ y_t =Cx_t + v_t \]

with \( C \in \mathbb{R}^{n \times p} \) output matrix

\( v_t \sim N(0, R) \) noise
$u_t = u_t^* (+\Delta u_t)$

Sensor measures & non-stationary watermarks (periodic)

$r_{ct} + \Delta y_{ct}$

$(r_{ct} = y_t - B\hat{x}_{t-1})$

$g(t) = \sum_{i=t-w+1}^{t} r_i^T P^{-1} r_i$
Cyber-physical adversary

**Aim:** Use identification methods to gain knowledge about the system parameters, from the network, to influence the physical behavior.
3 PIETC-WD
3.3 FIRST SENSOR ALARM

\[ u_t = u_t^* + \Delta u_t \]

**Network**

- **Actuators**
- **Plant**
- **Sensor 1**
  - Local controller 1
- **Sensor N**
  - Local controller N

**Detector**

- **LQG controller**
- **Watermark**

**ALARM**
- \( y_{1t} \) sent immediately

**Raw data** \( y_t \)

**Suspicious behavior**

\( g(t) \)

\( t \)

\( w \)

\( \tau \)
ALARM 2

$y_{1t+1}$ sent immediately

Raw data $y_{t+1}$

IF raiseAlarm() DO
falseAlarm()
ELSE
attackDetected()
SCADA Testbed

- LEGO Mindstorm EV3 & Raspberry Pi
- Closed-loop system with wired and wireless communications
Sensor detectors without intermittent policy

Sensor detectors with intermittent policy

Central detector without intermittent policy

Central detector with intermittent policy
CONTENTS

1. PRESENTATION

2. CYBER-PHYSICAL SYSTEMS
   2.1 Presentation
   2.2 Networked control systems
   2.3 Cyber-physical attacks

3. PIETC-WD
   3.1 Presentation
   3.2 Normal functioning
   3.3 First sensor alarm
   3.4 Second sensor alarm
   3.5 Validation

4. CONCLUSION
- **PIETC-WD**
  - Decentralized detection mechanism with non-stationary watermark
  - Detection of integrity cyber-physical attacks
  - Impacts:
    - Performance
    - Detection time

- **Future Work: Resilient CPSs**
  - More thorough analysis of PIETC-WD
  - Mitigation of cyber-physical attacks
    - Programmable networking
References


► Queiroz (2012). A holistic approach for measuring the survivability of SCADA systems. PhD, RMIT University.


ANNEXES
5 ANNEXES
5.1 SCADA TESTBEDS

1 / Bridge and toll testbed

2 / Industrial chain testbed

3 / Railway control testbed

4 / Autonomous industrial agents testbed

http://j.mp/TSPScada
Local controllers architecture

\[ x_t \rightarrow \text{Sensor 1} \rightarrow y_t^1 \rightarrow \text{Detector} \]

\[ \vdots \]

\[ \text{Sensor N} \rightarrow y_t^N \rightarrow \text{Detector} \]

\[ \Delta y_{t-1} \rightarrow \text{Kalman Filter} \rightarrow \Delta y_t^N \rightarrow \text{Watermark} \]

\[ g_N(t) \]

\[ t \]

\[ \tau \]

\[ w \]
Performance loss

► **LQG controller performance loss:** quadratic cost $J$

$$J = \lim_{n \to \infty} E \left[ \frac{1}{n} \sum_{i=0}^{n-1} \left( x_i^T \Gamma x_i + u_i^T \Omega u_i \right) \right] \quad \text{with}$$

- $u_t \in \mathbb{R}^m$ control input
- $x_t \in \mathbb{R}^p$ state vector
- $\Gamma \in \mathbb{R}^{p \times p}$ positive definite cost matrix
- $\Omega \in \mathbb{R}^{m \times m}$ positive definite cost matrix

► **Non-stationary performance loss:** quadratic cost $\Delta J_s$

$$J = J^* + \Delta J_s$$

$$\beta = E[\Delta s^{(i)}] + Var[\Delta s^{(i)}]$$
SCADA Components

Supervisory Control And Data Acquisition (SCADA): A technology to monitor industrial environments

► Programmable Logic Controller (PLC): Microprocessors-based devices to control and acquire inputs/outputs

► Intelligent Electronic Device (IED): Small microprocessors with limited capabilities in power systems

► Remote Terminal Unit (RTU): Stand-alone data acquisition and control units on a remote site via telemetry

► Master Terminal Unit (MTU): Control center of the system to collect, store and control data from RTUs and PLCs

► Human-Machine Interface (HMI): Displays real-time operation information about the processes to the operators to coordinate and control the system
ISA 95

Definition of the different levels of SCADA Systems

► Level 0 – Field level: Physical plant
► Level 1 – Direct control: Measurement and manipulation of the plant
► Level 2 – Plant Supervisory: Control and supervision systems of the plant
► Level 3 – Production control: Work flow to produce the desired end products and optimization of the system
► Level 4 – Production scheduling: Establishment of the basic plant schedule (production, delivery, inventory, etc.)
5 ANNEXES
5.3 SCADA & PROTOCOLS

Level 0 – Field level
Level 1 – Direct control
Level 2 – Plant Supervisory
Level 3 – Production control
Level 4 – Production scheduling

Enterprise resource planning
Manufacturing execution system

Corporate ICT network
SCADA system

Programming station
HMI
Data historian

PLC
I/O module
MTU

SITE A

RTU SITE B
Sensor
Actuator

RTU SITE C
Sensor
Actuator
IED
### SCADA protocols

- Modbus
- PROFINET
- PROFIBUS
- DNP3
- IEC-60870-5-104
- EtherNet/IP
- Ethernet Powerlink
- AGA-12, etc.

<table>
<thead>
<tr>
<th>OSI Level</th>
<th>Industrial protocols</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>Modbus/TCP</td>
</tr>
<tr>
<td></td>
<td>DNP3-SA</td>
</tr>
<tr>
<td></td>
<td>PROFINET IO</td>
</tr>
<tr>
<td></td>
<td>IEC-60870-5-104</td>
</tr>
<tr>
<td></td>
<td>EtherNet/IP</td>
</tr>
<tr>
<td>6</td>
<td>PowerLink</td>
</tr>
<tr>
<td>5</td>
<td>TCP/UDP</td>
</tr>
<tr>
<td>4</td>
<td>IP</td>
</tr>
<tr>
<td>3</td>
<td>Ethernet</td>
</tr>
<tr>
<td>2</td>
<td>Ethernet PowerLink</td>
</tr>
<tr>
<td>1</td>
<td>Physical</td>
</tr>
<tr>
<td></td>
<td>Modbus ASCII/RTU</td>
</tr>
<tr>
<td></td>
<td>PROFIBUS</td>
</tr>
<tr>
<td></td>
<td>DNP3</td>
</tr>
<tr>
<td></td>
<td>AGA-12</td>
</tr>
<tr>
<td></td>
<td>IEC-60870-5-101</td>
</tr>
</tbody>
</table>

:\!

*Designed for safety and not security* :\!