

CPDY: Extending the Dolev-Yao Attacker with Physical-Layer Interactions

MARCO ROCCHETTO and Nils Ole Tippenhauer

University of Luxembourg

Singapore University of Technology and Design

CPS

- systems that consist of networked embedded systems, which are used to **sense, actuate**, and **control physical processes**
- Examples: industrial water treatment facilities, electrical power plants, public transportation infrastructure, or even smart cars



- Security of CPS is a major concern: Stuxnet
- CPS are complex systems (with 100+ communicating components, physics of the system)
- Mostly analyzed from an engineering point of view (fault detection) with no attacker model
- (formal) Security analysis of **any** system relies on **attacker** and system models
- Information security \Rightarrow Dolev-Yao attacker model
- CPS security \Rightarrow ???

- 1 Discuss general **limitations** of the DY attacker model for analysis of CPS, and physical layer interactions between the attacker and the attacked system
- 2 Propose a number of **rule extensions** to analyze CPS using the DY model
- 3 Implement these rule extensions in the ASLan++ formal language (not in this talk)
- 4 Present **use case examples** (water treatment plant)

- 1 The DY model **can** be used for the security analysis of CPS
- 2 The standard DY is **not enough**
- 3 The **Cyber-Physical Dolev-Yao model**

Attacker Model

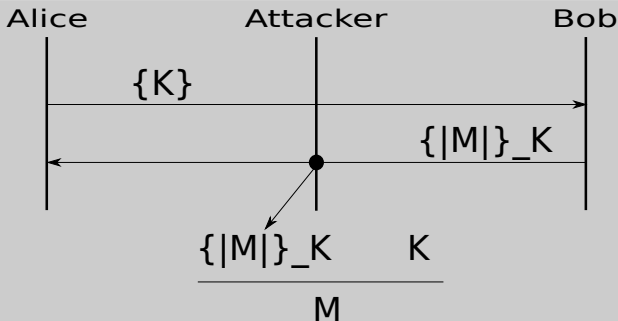
- 1 define **constraints for the attacker** (e.g. finite computational resources, no access to shared keys)
- 2 fully characterize the possible **interactions** between the attacker and the system under attack
- 3 Assumptions: perfect cryptography & attacker = network

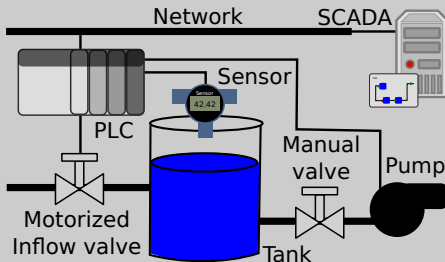
$$\begin{array}{c}
 \frac{M_1 \in M}{M_1 \in DY} G_{\text{axiom}} \quad \frac{M_1 \in DY \quad M_2 \in DY}{[M_1, M_2] \in DY} G_{\text{pair}} \quad \frac{M_1 \in DY \quad M_2 \in DY}{\{M_1\}_{M_2} \in DY} G_{\text{crypt}} \\
 \frac{M_1 \in DY \quad M_2 \in DY}{\{\{M_1\}\}_{M_2} \in DY} G_{\text{sCrypt}} \quad \frac{[M_1, M_2] \in DY}{M_i \in DY} A_{\text{pair}_i} \quad \frac{\{\{M_1\}\}_{M_2} \in DY \quad M_2 \in DY}{M_1 \in DY} A_{\text{sCrypt}} \\
 \frac{\{M_1\}_{M_2} \in DY \quad \text{inv}(M_2) \in DY}{M_1 \in DY} A_{\text{crypt}} \quad \frac{\{M_1\}_{\text{inv}(M_2)} \in DY \quad M_2 \in DY}{M_1 \in DY} A_{\text{crypt}}^{-1}
 \end{array}$$

Fig. 2: The system of rules of the Dolev-Yao attacker

Attacker Model

- 1 define **constraints for the attacker** (e.g. finite computational resources, no access to shared keys)
- 2 fully characterize the possible **interactions** between the attacker and the system under attack
- 3 Assumptions: perfect cryptography & attacker = network



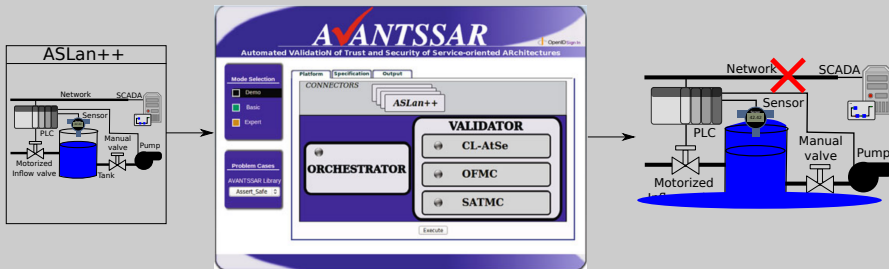


- **SCADA**: logic of the CPS
- **PLC**: analog/digital conversion
- **Valve/Pumps**: mechanics of the system
- **Initial state**: valves opened, pump closed

Goal of the attacker (LTL)

Water spillage or (tank burst) in the **tank**

Formal security analysis (AVANTSSAR)

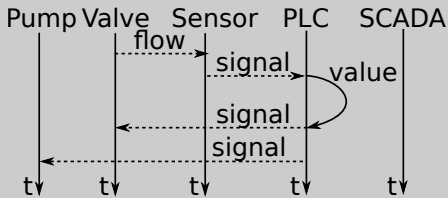
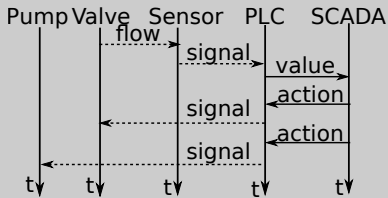


ASLan++ formal specification

- Behavior of each entity
- Communication between entities
- No fluid dynamics is involved in the model of the system
- Initial state: valves opened, pump closed

- ✓ The DY model **can** be used for the security analysis of CPS
 - 1 The standard DY is **not enough**
 - 2 (intuition) The **Cyber-Physical Dolev-Yao model**

The Dolev-Yao model is not enough



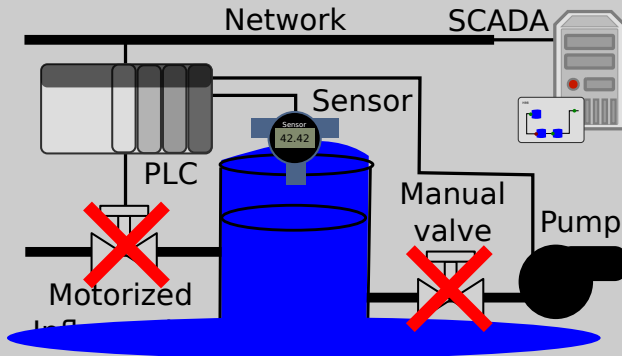
Logic integrated into the PLC

- No communication between the PLC and the SCADA therefore
- The DY cannot see any message between the valve/PLC and the SCADA
- The AVANTSSAR platform reports **no attack found**

Really secure?

Obviously **NOT**. A physically present attacker can find an attack

Physically present attacker



Physical properties

There are some properties (not in DY e.g., distance) that can be exploited by an attacker to perform some actions that might lead to an attack

- ✓ The DY model **can** be used for the security analysis of CPS
- ✓ The standard DY is **not enough**
 - 1 (intuition) The **Cyber-Physical Dolev-Yao model**

Abstraction of physical processes

- no differential equations (no dynamics)
- abstract away the details of the physics (similar to perfect cryptography)

CPS: system rules

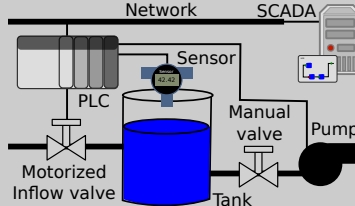
$$\frac{\text{Tank}(\text{level}, \text{value}) \in \text{Sys} \quad \text{Pump}(\text{status}, \text{off}) \quad \text{InflowValve}(\text{status}, \text{open}) \in \text{Sys}}{\text{Tank}(\text{level}, \text{value}') \in \text{Sys} \wedge (\text{value}' > \text{value})} \text{raise}_1(\text{Tank})$$

$$\frac{\text{Tank}(\text{level}, \text{value}) \in \text{Sys} \quad \text{ManualValve}(\text{status}, \text{close}) \in \text{Sys} \quad \text{InflowValve}(\text{status}, \text{open}) \in \text{Sys}}{\text{Tank}(\text{level}, \text{value}') \in \text{Sys} \wedge (\text{value}' > \text{value})} \text{raise}_2(\text{Tank})$$

$$\frac{C(\text{status}, \text{damaged}) \in \text{Sys} \quad C(\text{contains}, \text{water}) \in \text{Sys} \quad C(\text{level}, \text{value}) \in \text{Sys}}{C(\text{level}, \text{value}') \in \text{Sys} \wedge (\text{value}' < \text{value})} \text{damaged}(C)$$

$$\frac{C(\text{operate}, \text{manual}) \in \text{Sys} \quad C(\text{status}, \text{open}) \vee C(\text{status}, \text{close}) \in \text{Sys}}{C(\text{status}, \text{close}) \in \text{Sys}} \text{close}(C)$$

$$\frac{C(\text{operate}, \text{manual}) \in \text{Sys} \quad C(\text{status}, \text{open}) \vee C(\text{status}, \text{close}) \in \text{Sys}}{C(\text{status}, \text{open}) \in \text{Sys}} \text{open}(C)$$



CPS: system rules

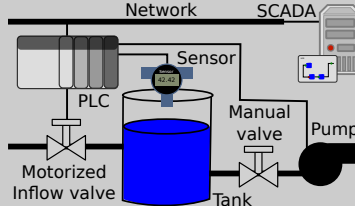
$$\frac{\text{Tank}(\text{level}, \text{value}) \in \text{Sys} \quad \text{Pump}(\text{status}, \text{off}) \quad \text{InflowValve}(\text{status}, \text{open}) \in \text{Sys}}{\text{Tank}(\text{level}, \text{value}') \in \text{Sys} \wedge (\text{value}' > \text{value})} \text{raise}_1(\text{Tank})$$

$$\frac{\text{Tank}(\text{level}, \text{value}) \in \text{Sys} \quad \text{ManualValve}(\text{status}, \text{close}) \in \text{Sys} \quad \text{InflowValve}(\text{status}, \text{open}) \in \text{Sys}}{\text{Tank}(\text{level}, \text{value}') \in \text{Sys} \wedge (\text{value}' > \text{value})} \text{raise}_2(\text{Tank})$$

$$\frac{C(\text{status}, \text{damaged}) \in \text{Sys} \quad C(\text{contains}, \text{water}) \in \text{Sys} \quad C(\text{level}, \text{value}) \in \text{Sys}}{C(\text{level}, \text{value}') \in \text{Sys} \wedge (\text{value}' < \text{value})} \text{damaged}(C)$$

$$\frac{C(\text{operate}, \text{manual}) \in \text{Sys} \quad C(\text{status}, \text{open}) \vee C(\text{status}, \text{close}) \in \text{Sys}}{C(\text{status}, \text{close}) \in \text{Sys}} \text{close}(C)$$

$$\frac{C(\text{operate}, \text{manual}) \in \text{Sys} \quad C(\text{status}, \text{open}) \vee C(\text{status}, \text{close}) \in \text{Sys}}{C(\text{status}, \text{open}) \in \text{Sys}} \text{open}(C)$$

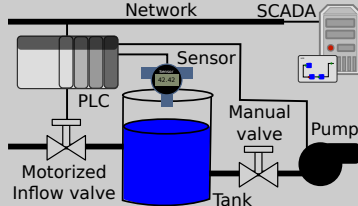


CPDY: attacker rules

$$\frac{DYProp(distance, physical_access) \quad DYProp(tool, damage)}{C(status, damaged) \in Sys} \quad damage_{DY}$$

$$\frac{DYProp(distance, physical_access) \quad C(operate, manual) \in Sys \quad C(status, open) \in Sys}{C(status, close) \in Sys} \quad manualClose_{DY}$$

$$\frac{DYProp(distance, physical_access) \quad C(operate, manual) \in Sys \quad C(status, close) \in Sys}{C(status, open) \in Sys} \quad manualOpen_{DY}$$



CPDY: attacker rules

$$\frac{\text{attacker_property} \quad \text{system_property}}{\text{result of action}} \quad \text{action}$$

- we cannot (easily) modify the internal behavior of the validators
- we have used Horn Clauses (HC) to add extra rules to the DY attacker model
- we have used databases (shared memories) to store the state of the components the system, e.g., the level of the water of a tank.

- ✓ The DY model **can** be used for the security analysis of CPS
- ✓ The standard DY is **not enough**
- ✓ (intuition) The **Cyber-Physical Dolev-Yao model**

	attack found		timing	
	DY	CPDY	analysis	total
Network	✓	✓	220ms	1.7s
Manual		✓	8ms	1.3s
Heating		✓	4ms	1.0s

- Network: Logic in the SCADA
- Manual: Logic in the PLC
- Heating: The attacker can heat a component (i.e., a tank)

Goal (Network and Manual)

$$\Box(\text{inflowValve}(\text{status}, \text{open}) \in \text{Sys} \Rightarrow \text{manualValve}(\text{status}, \text{open}) \in \text{Sys} \wedge (\text{tank}(\text{status}, \text{underT}) \in \text{Sys} \vee \text{pump}(\text{status}, \text{on}) \in \text{Sys}))$$

Case study: Heating

	attack found		timing	
	DY	CPDY	analysis	total
Network	✓	✓	220ms	1.7s
Manual		✓	8ms	1.3s
Heating		✓	4ms	1.0s

Attacker heating rule

$$\frac{DYProp(Distance, physical_access) \quad DYProp(Tool, heating)}{C(status, heating) \in Sys} \quad heat_{DY}$$

Goal

$$\Box(Tank(pressure, overT) \notin Sys)$$

Case study: Heating

	attack found		timing	
	DY	CPDY	analysis	total
Network	✓	✓	220ms	1.7s
Manual		✓	8ms	1.3s
Heating		✓	4ms	1.0s

System rules (linear proportionality of heating and pressure)

$$\frac{C(\text{status}, \text{heating}) \in \text{Sys} \quad C(\text{contains}, \text{water}) \in \text{Sys} \quad C(\text{temperature}, \text{Level}) \in \text{Sys}}{C(\text{temperature}, \text{Level}') \in \text{Sys} \wedge \text{Level}' > \text{Level}} \text{heat}_1(C)$$

$$\frac{C(\text{status}, \text{heating}) \in \text{Sys} \quad C(\text{contains}, \text{water}) \in \text{Sys} \quad C(\text{pressure}, \text{Level}) \in \text{Sys}}{C(\text{pressure}, \text{Level}') \in \text{Sys} \wedge \text{Level}' > \text{Level}} \text{heat}_2(C)$$

$$\frac{C(\text{status}, \text{heating}) \in \text{Sys} \quad C(\text{contains}, \text{water}) \in \text{Sys} \quad C(\text{temperature}, \text{TLevel}) \in \text{Sys} \quad C(\text{pressure}, \text{PLevel}) \in \text{Sys}}{C(\text{temperature}, \text{TLevel}') \in \text{Sys} \wedge C(\text{pressure}, \text{PLevel}') \in \text{Sys} \wedge (\text{PLevel}' > \text{PLevel}) \wedge (\text{TLevel}' > \text{TLevel})} \text{heat}_3(C)$$

Goal

$$\Box(\text{Tank}(\text{pressure}, \text{overT}) \notin \text{Sys})$$

- 1 ESORICS 2016, and dimensions of the attacker model
- 2 ICFEM 2016, formal modeling CPDY
 - 1 The DY model **can** be used for the security analysis of CPS
 - 2 The standard DY is **not enough**
 - 3 (intuition) The **Cyber-Physical Dolev-Yao model**
- 3 EUMAS 2016, theoretical analysis of all possible attack states
- 4 FUTURE WORK: full security analysis of SWaT

	attack found		timing	
	DY	CPDY	analysis	total
Network	✓	✓	220ms	1.7s
Manual		✓	8ms	1.3s
Heating		✓	4ms	1.0s