Systematic generation of attack scenarios against industrial systems

Maxime Puys, Marie-Laure Potet and Jean-Louis Roch

VERIMAG, University of Grenoble Alpes / Grenoble-INP, France
Firstname.Name@imag.fr

June 8, 2016

AFADL 2016

Industrial Systems (SCADA)

Hot topic

- Increasing number of attacks showed in the medias since Stuxnet.
- Becoming a priority for government agencies.
  - Laws to ensure the security of OIVs *(Loi de Programmation Militaire, Livre blanc sur la défense et la sécurité nationale, 2013)*.
  - Publications from ANSSI *(Managing Cybersecurity for ICS, Protection Profiles, 2012-now)*.

Disambiguation

Security concepts

- Safety = Protection against identified/natural difficulties.
  - Historic industrial concern.
- Cybersecurity = Protection against malicious adversaries.
  - Often called Security.

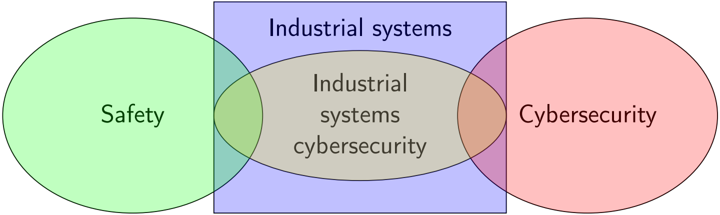

Figure : Relations among security concepts

- Ludovic Pietre-Cambacedes' thesis: On the relationships between safety and security, Telecom ParisTech and EDF, 2010.

Differences between Industrial and Business IT

- Really long-term installations, hard to patch, lot of legacy hosts.
- Security objectives are different from traditional systems:
  - Availability, integrity, authentication and non-repudiation.
- Messages are READ/WRITE commands to PLCs.
  - Sometimes SUBSCRIPTIONS, RPCs or grouped commands.
  - Industrial protocols: MODBUS, OPC-UA.
- Attack examples: change the value of a WRITE request to change a temperature, change a READ response to mislead opperators.

Approach

- Objectives:
  - From modeling, automatically produce high-level attack scenarios exploiting protocols weaknesses.
  - Convert them to real network packets with using infrastructure's context to verify and quantify their plausibility.
  - Possible interest: Generate behavioral attack scenarios (i.e.: close to nominal behavior) to avoid IDS.

- High-level attack scenarios:
  - On the network.
  - Rely on the content of commands.

- Take into account the safety **but not redo it**.

Approach

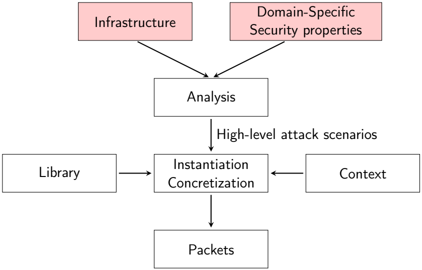

Figure : Our global approach

- Infrastructure representation:
  - Devices behaviors.
  - Communication channels.
  - Communication protocols.

- Safety properties an attacker would violate using security weaknesses.
- Security properties of:
  - Devices.
  - Communication protocols.
- Attacker models:
  - Position(s).
  - Capacities.

Approach

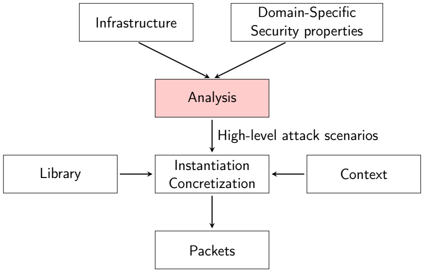

Figure : Our global approach

Currently two analyses:

- Identification of attack vectors:
  - How an attacker can reach his objectives exploiting protocol weaknesses.
- Produce attacks on safety properties:
  - Model-checking between clients, servers and attackers.

Approach

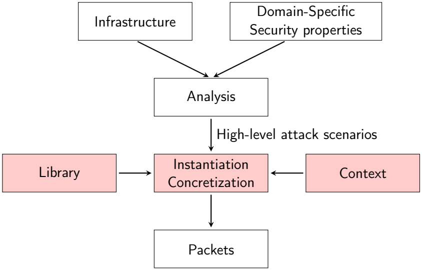

Figure : Our global approach

- Vulnerability library database for ICS
  - Similar to Metasploit
  - E.g.: How to modify an OPC-UA packet, how to change permission of a MODBUS variable?

- What should be put in the packets:
  - IP addresses of peers
  - Values of the variables

Identification of Attack Vectors

- Part of the "Analysis" box:
  - Global analysis of attacker's objectives and communication protocols to reduce the number of possible scenarios

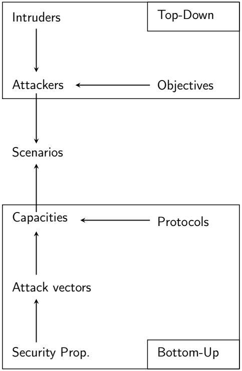

Figure : Attack vector analysis

- Top-down step:
  - Identify attacker's position and objectives
  - Similar to risk analysis methods
- Bottom-Up step:
  - Identify attacker's capacities given protocols counter-measure (encryption, signatures, etc)
- Combine both to obtain possible attack vectors

Top-Down Example

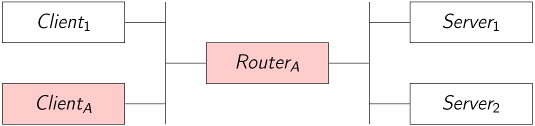

Figure : Infrastructure example

Possible security objectives:

- $IdTh$ = Identity theft,
- $AuthBP$ = Authentication by-pass,

$\mathcal{R}_{Obj}$	$IdTh$	$AuthBP$
$Client_A$		✓
$Router_A$	✓	

Table : Objectives for each attacker

Bottom-Up Example

Possible realisation of objectives:

- $Real(IdTh) = \{\{Spy\}\}$
- $Real(AuthBP) = \{\{Usurp\}, \{Replay\}\}$

$Atk.vectors$	Spy	$Usurp$	$Replay$
FTP_{Auth}	✓		✓
$\text{OPC-UA}_{SignEnc}$			

Table : Atk. vectors for each protocol

Results:

- $\mathcal{S}_{Client_A,\text{FTP}_{Auth}} = \{(AuthBP, Replay)\}$
- $\mathcal{S}_{Client_A,\text{OPC-UA}_{SignEnc}} = \emptyset$
- $\mathcal{S}_{Router_A,\text{FTP}_{Auth}} = \{(IdTh, Spy)\}$
- $\mathcal{S}_{Router_A,\text{OPC-UA}_{SignEnc}} = \emptyset$

Conclusion

Some other approaches/tools:

- Conchon et al. [CC15] *Expression des besoins et identification des objectifs de résilience*, 2015. ⇒ Very complete but also complex.
- Kriaa et al. [KBL15] *A Model Based Approach For SCADA Safety And Security Joint Modelling: S-Cube*, 2015. ⇒ Tool not available.

Risk analysis on SCADA infrastrucutre: easy automation, reusable.

- Developed and instanciated in an industrial context

Limits: protocol encapsulation, clearer separation between security objectives and safety objectives.

Conclusion

- A global approach to assess SCADA's security
- Attack vector analysis to reduce the number of possible scenarios
- Interest in formal verification of industrial protocol (OPC-UA):
  - Formal Analysis of Security Properties on the OPC-UA SCADA Protocol, *SAFECOMP'16*

- Perspectives:
  - Continue to build the approach (library, more protocols, link pieces together)
  - POC of safety properties analysis using CSP and FDR3.

Thanks for your attention!

Safety and Security 2/2

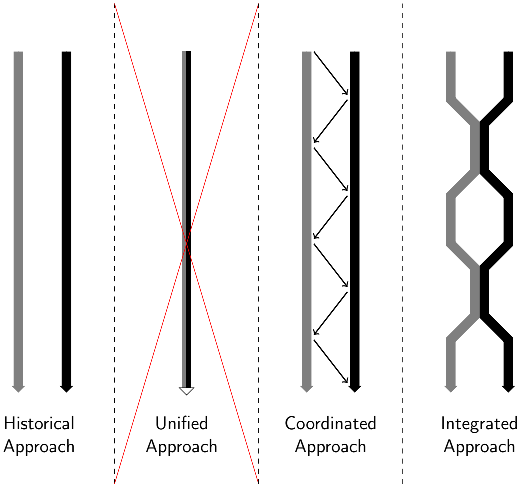

Figure : How to link safety and security [PC10]

Purdue Model

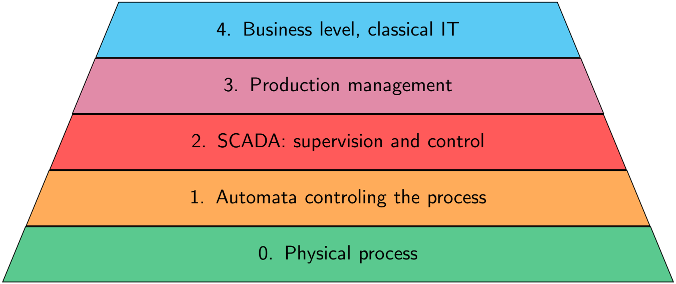

Figure : Purdue model [Wil91]

Cryptographic Protocols Verification

Needham-Schroeder

1. A $\rightarrow$ B : $\{A, N_A\}_{KB}$
2. B $\rightarrow$ A : $\{N_A, N_B\}_{KA}$
3. A $\rightarrow$ B : $\{N_B\}_{KB}$

Designed and **proved** in 1978.
Broken in 1996 (17 years after).

Man-In-The-Middle attack

1. A $\rightarrow$ I : $\{A, N_A\}_{KI}$

1. I $\rightarrow$ B : $\{A, N_A\}_{KB}$
2. B $\rightarrow$ I : $\{N_A, N_B\}_{KA}$

2. I $\rightarrow$ A : $\{N_A, N_B\}_{KA}$
3. A $\rightarrow$ I : $\{N_B\}_{KI}$

3. I $\rightarrow$ B : $\{N_B\}_{KB}$

- Way too much possible combinations.
  - Need of automation using tools.

References I

- Sylvain Conchon and Jean Caire, *Expression des besoins et identification des objectifs de résilience*, C&esar'15 (2015).
- S Kriaa, M Bouissou, and Y Laarouchi, *A model based approach for SCADA safety and security joint modelling: S-Cube*, IET System Safety and Cyber Security, IET Digital Library, 2015.
- Ludovic Piètre-Cambacédès, *The relationships between safety and security*, Theses, Télécom ParisTech, November 2010.
- Theodore J Williams, *A reference model for computer integrated manufacturing (cim): A description from the viewpoint of industrial automation: Prepared by cim reference model committee international purdue workshop on industrial computer systems*, Instrument Society of America, 1991.