Diagnosis of failures and of malicious acts in industrial control systems

Edwin Bourget

IMT Atlantique

2nd October 2018

CHAIRE
CYBERCNI
Sécurité des infrastructures critiques

Outline of the presentation

Motivation

Thesis subject

Diagnosis *of* **failures** *and of* **malicious acts** *in industrial control systems*

- Objective: given a set of alerts, corresponding to undesired events, provide an explanation about the incident

On the difficulty to mix safety with security

- ICS[1] safety well studied since the 1960s
- To ensure security: build a wall around your system and hire a guard at the gate
- ICS are now interconnected through the cyberspace and inherit vulnerabilities from the IT world

What is the problem?

We know how to evaluate safety or security individually but have no methods working for both at the same time

[1] Industrial Control Systems

Defining diagnosis

- For safety, three tasks:
  - Fault detection: discovering the fault
  - Fault isolation: finding which component is at fault
  - Fault identification: nature and scope of the fault
- For security, diagnosis is often a synonym for intrusion detection
- Everyone has their own definitions for diagnosis: models look very differently

The definition of diagnosis we consider

Diagnosis aims at providing relevant and intelligible information to a decision taker when a problem occurs.

Thesis subject

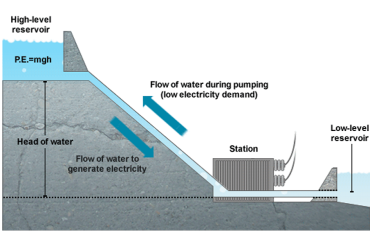
What is meant by diagnosis?

- Identify the origin of the incident
- Identify the objective/undesired event
- Calculate the impact of the incident on the system
- Calculate the risks of the incident on the system

The thesis is about **analysing alerts** (**not raising them**) corresponding to either **safety or security** events, in order to perform the diagnosis.

Tackling real and serious threats

The Taum Sauk power station

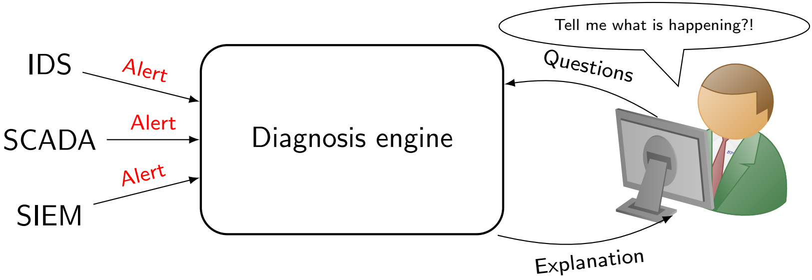


http://www.bbc.co.uk/bitesize/standard/physics/energy_matters/generation_of_electricity/revision/3/
http://damfailures.org/case-study/taum-sauk-dam-missouri-2005/
https://en.wikipedia.org/wiki/Taum_Sauk_Hydroelectric_Power_Station

Diagnosing security and safety events

A diagnosis engine

- Input: set of alerts
- Output: meaningful explanation about the problem



Objectives for a diagnosis model

The diagnosis engine should

- Process, sort, correlate alerts
- Identify the origin of the incident
- Identify the objective/undesired event
- Compute the likelihood of occurrence of an event
- Compute MTTS/MTTF
- Estimate the risk
- Track what events have happened
- Work in real time if needed

Diagnosing safety and security

Extending LAMBDA[1] to support safety and security

Event

- Preconditions set
  - Conditions for the event to happen
- Postconditions set
  - Consequences of the event on the system state

[1] Cuppens, F., and Ortalo, R.: 'LAMBDA: A Language to Model a Database for Detection of Attacks', in Debar, H., Mé, L., and Wu, S.F. (Eds.): 'Recent Advances in Intrusion Detection: Third International Workshop, RAID 2000 Toulouse, France, October 2–4, 2000 Proceedings' (Springer Berlin Heidelberg, 2000), pp. 197-216

Extending LAMBDA[1] to support safety and security

Event

- Preconditions set
  - Conditions for the event to happen
- Postconditions set
  - Consequences of the event on the system state
- Nature
  - Security, safety

[1] Cuppens, F., and Ortalo, R.: 'LAMBDA: A Language to Model a Database for Detection of Attacks', in Debar, H., Mé, L., and Wu, S.F. (Eds.): 'Recent Advances in Intrusion Detection: Third International Workshop, RAID 2000 Toulouse, France, October 2–4, 2000 Proceedings' (Springer Berlin Heidelberg, 2000), pp. 197-216

Extending LAMBDA[1] to support safety and security

Event

- Preconditions set
  - Conditions for the event to happen
- Postconditions set
  - Consequences of the event on the system state
- Nature
  - Security, safety
- Probability distribution
  - Models the time taken for the event to happen

[1] Cuppens, F., and Ortalo, R.: 'LAMBDA: A Language to Model a Database for Detection of Attacks', in Debar, H., Mé, L., and Wu, S.F. (Eds.): 'Recent Advances in Intrusion Detection: Third International Workshop, RAID 2000 Toulouse, France, October 2–4, 2000 Proceedings' (Springer Berlin Heidelberg, 2000), pp. 197-216

Extending LAMBDA[1] to support safety and security

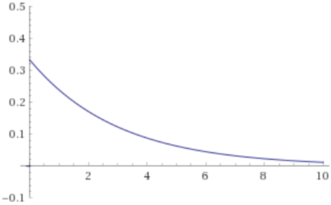
Event

- Preconditions set
  - Conditions for the event to happen
- Postconditions set
  - Consequences of the event on the system state
- Nature
  - Security, safety
- Probability distribution
  - Models the time taken for the event to happen
- Alert
  - To detect that the event has occured

[1] Cuppens, F., and Ortalo, R.: ‘LAMBDA: A Language to Model a Database for Detection of Attacks’, in Debar, H., Mé, L., and Wu, S.F. (Eds.): ‘Recent Advances in Intrusion Detection: Third International Workshop, RAID 2000 Toulouse, France, October 2–4, 2000 Proceedings’ (Springer Berlin Heidelberg, 2000), pp. 197-216

Example of an event

Event modelled: an attacker gets access to the Operator Control Network (OC_Net)

Preconditions	encryption(OC_Net, null)
Postconditions	remoteAccess(A, OC_Net)
Nature	security
Realisation	exponential distribution, param $1/\lambda = 3y$ 
Detection	IDS detects intruder

Correlation of safety and security events

Event graph identifies dependencies between events

The event graph is generated using CRIM[2]

- Take every pair of two events
- If one of the postconditions of an event match with one of the preconditions of the other event, then they are connected

Access OC_Net
Pre: encryption(OC_Net, null)
Post: remoteAccess(A, OC_Net)

Compromise PLC
Pre: remoteAccess(A, OC_Net) & vulnerable(PLC, cve-2004-1289)
Post: manInTheMiddle(A, PLC, Pump)

[2] Cuppens, F., and Miege, A.: 'Alert correlation in a cooperative intrusion detection framework', in Editor (Ed.)^(Eds.): 'Book Alert correlation in a cooperative intrusion detection framework' (2002, edn.), pp. 202-215

Correlation of safety and security events

Event graph identifies dependencies between events

The event graph is generated using CRIM[2]

- Take every pair of two events
- If one of the postconditions of an event match with one of the preconditions of the other event, then they are connected

Access OC_Net

Pre: encryption(OC_Net, null)

Post: **remoteAccess(A, OC_Net)**

→

Compromise PLC

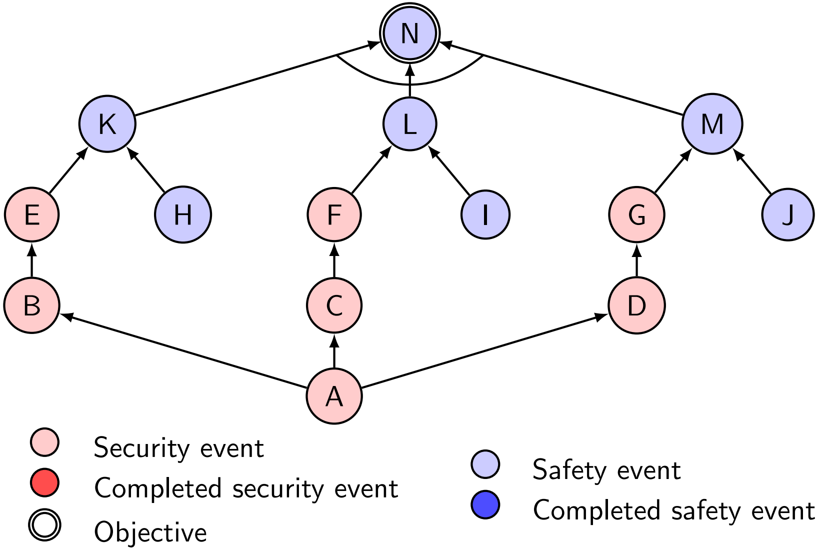
Pre: **remoteAccess(A, OC_Net)** & vulnerable(PLC, cve-2004-1289)

Post: manInTheMiddle(A, PLC, Pump)

[2] Cuppens, F., and Miege, A.: 'Alert correlation in a cooperative intrusion detection framework', in Editor (Ed.)ˆ(Eds.): 'Book Alert correlation in a cooperative intrusion detection framework' (2002, edn.), pp. 202-215

Building the event graph

Event graph after correlation



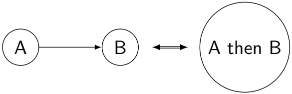
Probabilistic computations

Summary

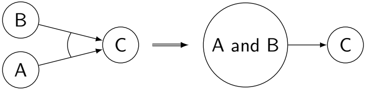
The event model has PDF associated with each events but recombinations are necessary to obtain PDF associated with scenarios

<u>Recombining rules:</u>

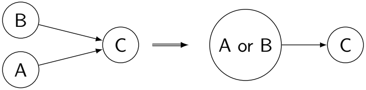
- Sequence : $f_{seq} = f_1 * f_2$



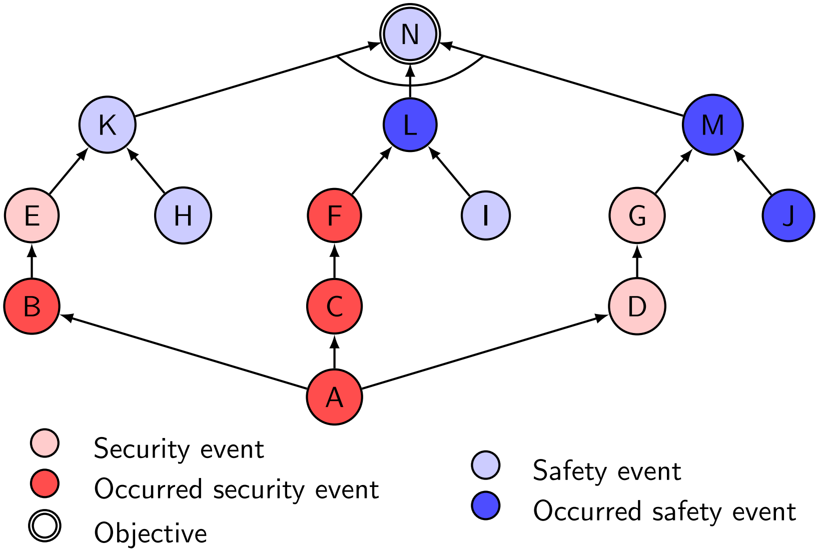
- And : $f_{and} = f_1 F_2 + F_1 f_2$



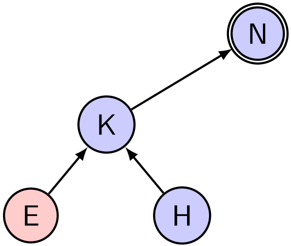
- Or : $f_{or} = f_1 + f_2 - (f_1 F_2 + F_1 f_2)$



Recombination example

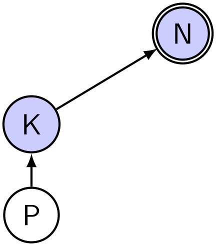


Recombination example



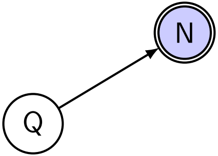
- We know of e, h, k, n

Recombination example



- We know of e, h, k, n
- $p = e + h - eH - Eh$

Recombination example



- We know of e, h, k, n
- $p = e + h - eH - Eh$
- $q = p * k$

Recombination example

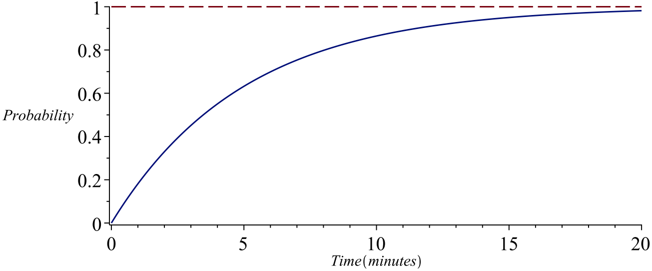
R

- We know of e, h, k, n
- $p = e + h - eH - Eh$
- $q = p * k$
- $r = q * n$

Recombination example

R

- We know of e, h, k, n
- $p = e + h - eH - Eh$
- $q = p * k$
- $r = q * n$



Recombinations result

Obtaining valuable information

We have the evolution of the probability of failure function of the time:

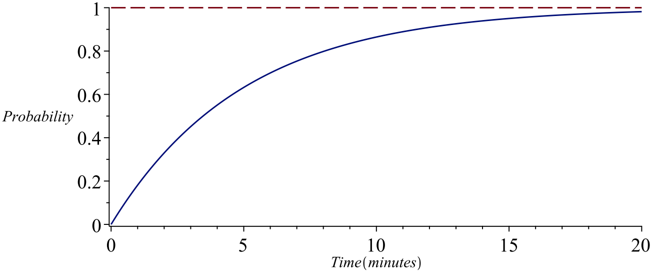


Figure: Evolution of the probabilities in the case studied

$$p := x \mapsto \begin{cases} 0 & x < 0 \\ \frac{e^{-\frac{x}{5}}}{5} & 0 \le x \end{cases} + \begin{cases} 0 & x < 0 \\ \frac{e^{-\frac{x}{5256000}}}{5256000} & 0 \le x \end{cases} - \left(\begin{cases} 0 & x < 0 \\ \frac{e^{-\frac{x}{5}}}{5} & 0 \le x \end{cases} \right) \left(\begin{cases} 0 & x \le 0 \\ -e^{-\frac{x}{5256000}} + 1 & 0 < x \end{cases} \right) - \left(\begin{cases} 0 & x < 0 \\ \frac{e^{-\frac{x}{5256000}}}{5256000} & 0 \le x \end{cases} \right) \left(\begin{cases} 0 & x \le 0 \\ -e^{-\frac{x}{5}} + 1 & 0 < x \end{cases} \right)$$

Mean Time To Failure in different cases

Obtaining more valuable information

We have an estimation of the mean time to failure: how long do we have to deploy a response before a critical failure?

Case	Alerts raised	MTTF
1	$\emptyset$	3y 23min 27sec
2	A	23min 27sec
3	A, B	21min 13sec
4	A, B, E, K	20min 54sec
5	A, C, D	14min 54sec
6	A, B, C, D, G, M	7min 30sec
7	A, I, L	20min 54sec
8	A, B, C, F, L, J, M	5min 0sec

Conclusion

Conclusion

Event model that enable diagnosis

- Logical event graph
  - Identify the origin
  - Conjecture possible outcomes of the incident
- Probabilistic model
  - Compute the likelihood
  - Compute probabilities of global scenarios

Can be easily extended

- Add an impact metric to compute the risk
- Showcase identifying roots of incidents

Diagnosis of failures and of malicious acts in industrial control systems

Edwin Bourget

IMT Atlantique

2nd October 2018

CHAIRE
CYBERCNI
Sécurité des infrastructures critiques