Attack Detection

Jonathan Jogenfors
Leonardo Iwaya

2016-09-26

Introduction

- About us

- Model of information security: Prevention, Detection, Reaction (PRD)
  - Prevention: Difficult because attacker has the advantage. Large attack surface.
  - Reaction: Too late!
  - Detection: What our papers are all about

When prevention fails

Anomaly detection

IDS

Honeypots

Papers

Motivation

- Papers [2] and [1] were **selected** based on their **relevance** to the theme of *"attack detection methods"* for *"critical infrastructures"*.
- Paper [3] was in the course's reading list.

Paper	Year	CI Sub-area	Citations	Journal IF
Pasqualetti et al [2]	2013	Attack Detection	210	2.777
Genge et al [1]	2015	Attack Prevention & Detection	12	1.351
Vasilomanolakis et al [3]	2016	Attack Detection	1	n.a

Attack detection and identification in cyberphysical systems (2013)

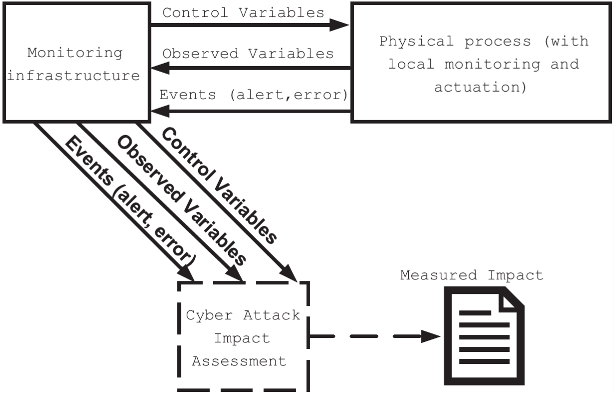
A system dynamics approach for assessing the impact of cyber attacks on CI (2015)

Aim & Contribution

- To **identify** and **rank** assets in complex, large-scale and heterogeneous CIs.
- **Cyber Attack Impact Assessment** (CAIA) methodology that helps system admins to understand:
  1. How cyber attacks affect the normal functioning of physical processes?
  2. What cyber assets would cause the most negative impact if compromised?

A system dynamics approach for assessing the impact of cyber attacks on CI (2015)

CAIA Methodology



A system dynamics approach for assessing the impact of cyber attacks on CI (2015)

Experiments & Comparisons

- First, the **basic functioning** of CAIA is demonstrated using IEEE 14-bus electric grid model.
- Second, CAIA's **scalability** is proven by using attack scenarios in the context of IEEE 300-bus electric grid model.
- Third, CAIA's **cross-sector applicability** is evaluated using Tennessee Eastman chemical process system.
- The methodology was also **compared** with other approaches (i.e., graph-theoretic and electrical centrality metric techniques).

A system dynamics approach for assessing the impact of cyber attacks on CI (2015)

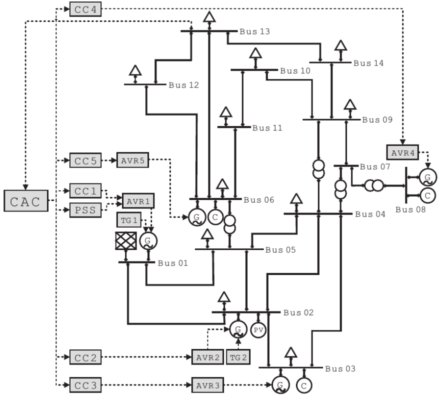


Fig. 5 – IEEE 14-bus model and its associated controllers.

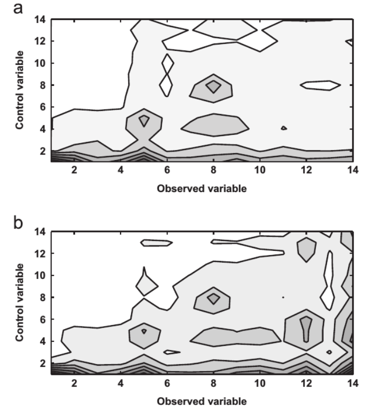


Fig. 7 – Effects of observed variable weights on the impact matrix for the IEEE 14-bus model. (a) Equal weights for all observed variables and (b) increased weights for observed variables (bus line voltage levels) 10, 12 and 14.

A system dynamics approach for assessing the impact of cyber attacks on CI (2015)

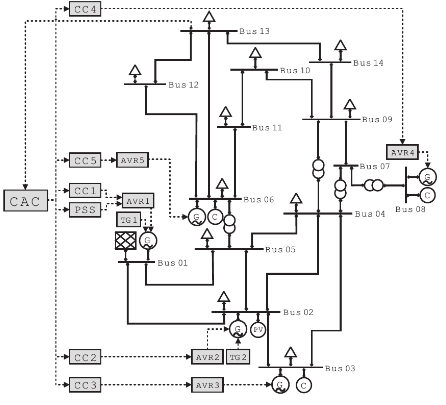


Fig. 5 – IEEE 14-bus model and its associated controllers.

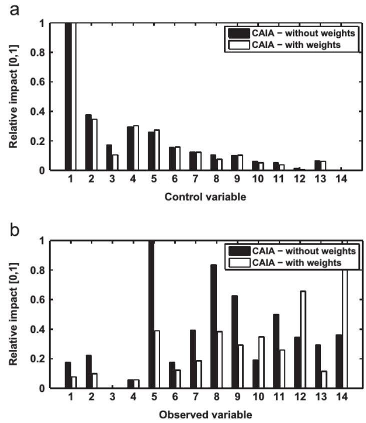


Fig. 8 – Effects of observed variable weights on impact rankings for the IEEE 14-bus model. (a) Impacts on control variables and (b) impacts on observed variables.

A system dynamics approach for assessing the impact of cyber attacks on CI (2015)

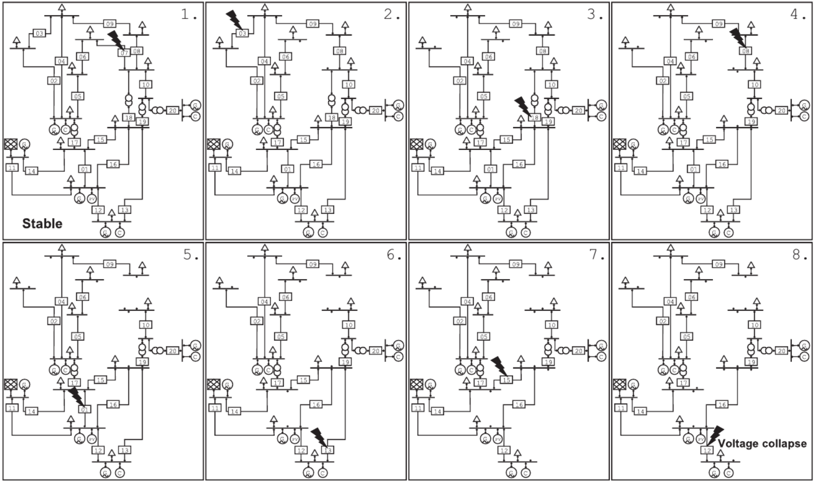


Fig. 20 – Stealthy cyber attack sequence that disconnects substation lines.

A system dynamics approach for assessing the impact of cyber attacks on CI (2015)

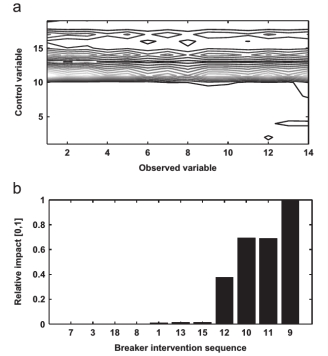


Fig. 19 – Stealthy cyber attack on the IEEE 14-bus model line breakers. (a) CAIA impact matrix and (b) ordered impact ranking of breakers.

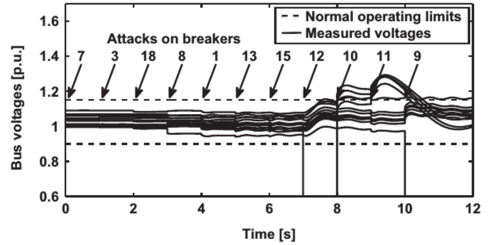


Fig. 21 – Operator's view of the stealthy attack sequence.

A system dynamics approach for assessing the impact of cyber attacks on CI (2015)

Limitations

- CAIA helps to identify and rank assets given specific interventions (e.g., an attack)
- Which interventions are relevant to test (?), and, how to protect the assets after generating the impact matrix (?) are open questions; out of the paper's scope.
- Obvious Note: the knowledge of impact matrices would be definitely valuable to attackers(!); as any risk assessment information.
- Seems hard to reproduce since no detailed information is given about the simulations; plus, no source code.

Multi-stage Attack Detection and Signature Generation with ICS Honeypots (2016)

Aim & Contribution

- HosTaGe: honeypot for detecting multi-stage attacks in ICS networks.
- Honeypot extension with capabilities of ICS protocols, i.e., Modbus, S7, SNMP, HTTP, Telnet, SMB and SMTP.
- Basic functions:
  1. notify the network administrators;
  2. produce an attack signature;
  3. forward the signature to the internal IDSs.

Multi-stage Attack Detection and Signature Generation with ICS Honeypots (2016)

Expermients & Comparisons

- HosTaGe was compared with “CONPOT ICS/SCADA Honeypot” [1]
- Criteria:
  1. ability to not be evade (i.e., be perceived by attackers);
  2. ability to detect multi-stage attacks;
  3. ability to generate valid signatures for Bro IDS [2].

[1] http://conpot.org/
[2] https://www.bro.org/

Multi-stage Attack Detection and Signature Generation with ICS Honeypots (2016)

Formal Model - Extended Finite State Machine (EFSM)

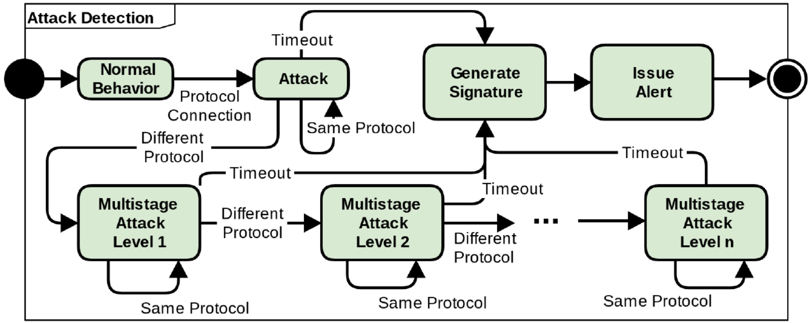


Fig. 1. EFSM of the attack detection and signature generation mechanism.

Multi-stage Attack Detection and Signature Generation with ICS Honeypots (2016)

Formal Model - Extended Finite State Machine (EFSM)

- Detection Mechanism
  1. Single-Protocol Level Detection (SPLD)
  2. Multi-Stage Level Detection (MSLD)
  3. Payload Level Detection (PLD)
- Time window (*tw*) determines whether an attack should be mapped as SPLD or MSLD

Multi-stage Attack Detection and Signature Generation with ICS Honeypots (2016)

Example - Signature Generation

- Automatically generate signature for well-known Metasploit script[3] for Modbus services identification.

Listing 1. Modbus attack signature generated by *HosTaGe*

```
signature modbus-signature{
   ip-proto == tcp
   dst-port == 502
   payload
       /\x21\x00\x00\x00\x00\x06\x01\x04\x00
   event "Modbus attack"
   }
```

[3] No further information given by the authors...

Multi-stage Attack Detection and Signature Generation with ICS Honeypots (2016)

Comparison - Honeypot x CONPOT

- Controlled environment, no firewalls, 8 to 12 weeks, probing by Shodan[4].

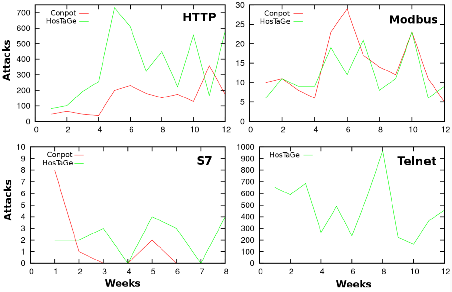


Fig. 3. Comparison of attacks on *HosTaGe* and Conpot for HTTP, Modbus, $S7$ and Telnet. Note, that Conpot does not support the Telnet protocol.

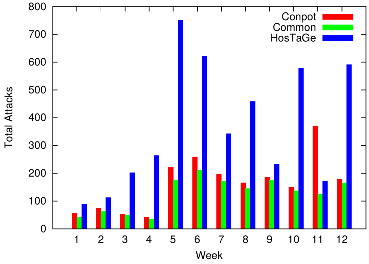


Fig. 4. Comparison of unique and common malicious IP addresses targeting *HosTaGe* and Conpot

[4] https://www.shodan.io/

Multi-stage Attack Detection and Signature Generation with ICS Honeypots (2016)

Limitations

- The evaluation of multi-stage signature generation was rather shallow.
- Shodan's probes were not explained in details, i.e., how Shodan detect a honeypot?

More info about HosTaGe can be found at Darmstad's research group website[5].

[5] https://www.tk.informatik.tu-darmstadt.de/de/research/secure-smart-infrastructures/hostage/

Discussions

References I

Béla Genge, István Kiss, and Piroska Haller.
A system dynamics approach for assessing the impact of cyber attacks on critical infrastructures.
International Journal of Critical Infrastructure Protection, 10:3–17, 2015.

Fabio Pasqualetti, Florian Dörfler, and Francesco Bullo.
Attack detection and identification in cyber-physical systems.
IEEE Transactions on Automatic Control, 58(11):2715–2729, 2013.

References II

E. Vasilomanolakis, S. Srinivasa, C. G. Cordero, and M. Mühlhäuser.

Multi-stage attack detection and signature generation with ics honeypots.

In *NOMS 2016 - 2016 IEEE/IFIP Network Operations and Management Symposium*, pages 1227–1232, April 2016.