PV226
Inside the insider domain: Slight insight in sight

Martin Macák

April 21th, 2022

LAB OF SOFTWARE ARCHITECTURES
AND INFORMATION SYSTEMS

FACULTY OF INFORMATICS
MASARYK UNIVERSITY, BRNO

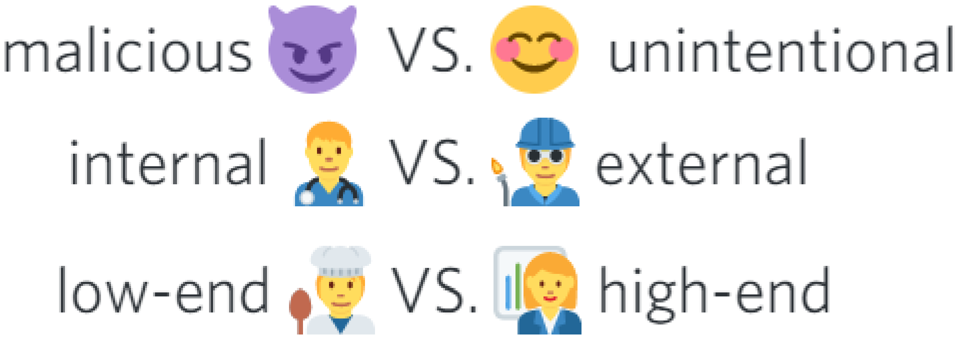
Outline

1. Introduction to insider domain
2. Current solutions
3. Research gaps
4. What do we do in Lasaris?

lasaris

Who is insider?

- Insider
  - A person with legitimate access to an organization’s resources.

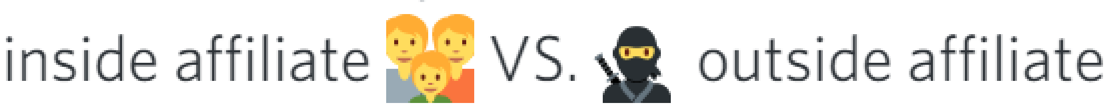


malicious 😈 VS. 😊 unintentional

internal 🧑‍⚕️ VS. 👷 external

low-end 🧑‍🍳 VS. 👩‍💼 high-end

- Affiliate
  - Do not have any justified and legitimate reason to enter the organization.



inside affiliate 👪 VS. 🥷 outside affiliate

Why do they cause harm?

- Malicious
  1. Self-motivated – get a job promotion, avenge the injustice against them, …
  2. Planted – steal intellectual property
  3. Recruited – perform a malicious act for their benefit

  The motivation can be financial, political, or personal.

- Unintentional
  1. Underminers – life is easier when I don’t respect security policies
  2. Overambitious – when I want to be more effective, I have to bypass security
  3. Socially engineered – I was tricked by someone
  4. Data leakers – ooopsie, I just leaked something

  No motivation or intent to cause harm.

How do they cause harm?

- Using legitimate access (traitors)
- Obtaining unauthorized access (masqueraders)

- Accident, mistake, slip (unintentional perpetrators)
- Theft, deception (socially engineered UPs)

What do they cause?

- Insider threat
  - Action of an employee that puts an organization or its resource at risk.
  - For example, data leakage.
- Insider attack
  - Action that intentionally misuses the computer system by a user that is authorized to access those systems and networks.
  - For example, theft of intellectual property, sabotage, and fraud.

Defense solutions

- Mitigation and prevention
- Decoy-based solutions
- Detection and assessment

Mitigation and prevention

- Deterrence of policy violations
- Data leakage prevention
- Gamification
- Disinformation by decoys
- Access control
- Training
- …

Decoy-based solutions

- Honeypot, honeytokens

Detection and assessment

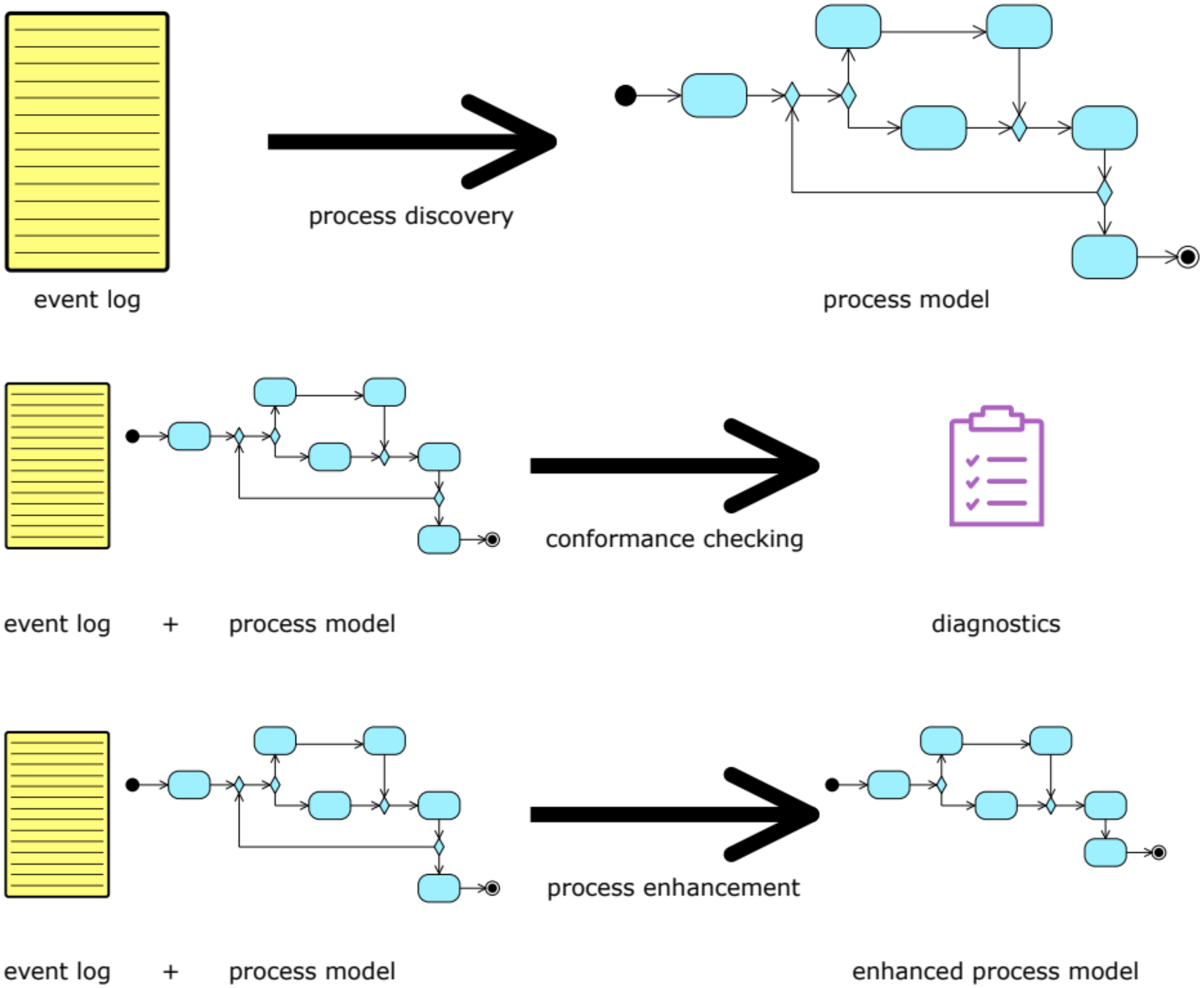
- Insider has to have motive, opportunity, and capability.
- Many conceptual and practical works focused on each element.
- Majority of them are data-oriented.
  - Support Vector Machine
  - K-Nearest Neighbours
  - Logistic Regression
  - Cluster-based approaches
  - Ensemble-based approaches
  - …

Research gaps

- The insider behavior is often encoded into a mathematical model that might not be accessible or is very abstract / complex.
- The proper response to a detected case might be challenging.
- It is hard to detect previously not seen insider attacks.

- Process-oriented approach seems like great help in this domain.

Process Mining



event log

process discovery

process model

event log + process model

conformance checking

diagnostics

event log + process model

process enhancement

enhanced process model

Challenges of Process Mining in insider domain

- Data collection and preprocessing
- Feature selection
- Process mining technique selection

Work of Lasaris lab in this context

- Insider attack detection:
    - Audit logs
    - Windows logs
- Insider threat detection
    - Simulation games platform
- Insider threat mitigation and prevention
    - Puzzle-based cybersecurity training in KYPO
- Addressing insider attacks via forensic-ready risk management
- Development of ProcessM.NET – a library (and application) that can be used for a process-oriented analysis

Conclusion

- Insider threats and attacks are currently **a hot topic** in many organizations.
- Process mining is currently **a hot topic** too.

- It is useful.
- It is fun.

- Come and join us! ☺

macak@mail.muni.cz

lasaris