Auditing scenarios for forensic-ready software

Lukáš Daubner

Summer School of Applied Informatics
Blansko, 2020

LAB OF SOFTWARE ARCHITECTURES AND
INFORMATION SYSTEMS

FACULTY OF INFORMATICS
MASARYK UNIVERSITY, BRNO

lasaris

Forensic-ready software

- Prepared for possible incident and investigation
- Assists the investigator in his task
- Is part of secure environment

lasaris

Forensic-ready software (cont.)

- Proactively collects evidence

Forensic-ready software (cont.)

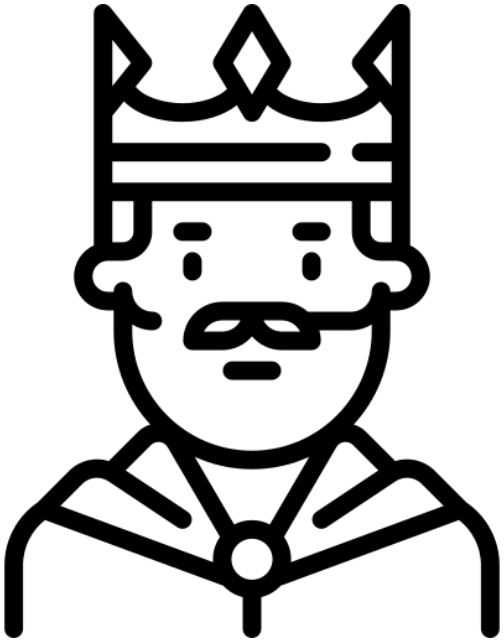
- Proactively collects evidence

?

lasaris

Forensic-ready medival castle

- Critical software

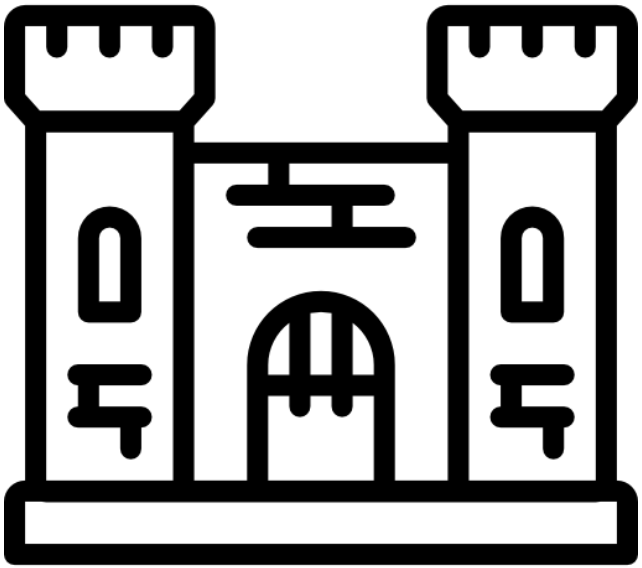


https://www.flaticon.com/free-icon/king_2701701

lasaris

Forensic-ready medival castle

- Firewall, IDS, etc.

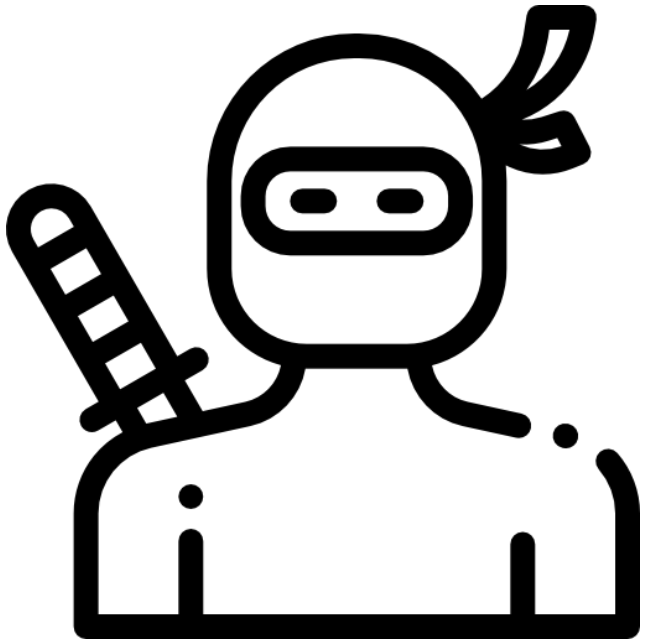


https://www.flaticon.com/free-icon/castle_542288

lasaris

Forensic-ready medival castle

- Malicious insider

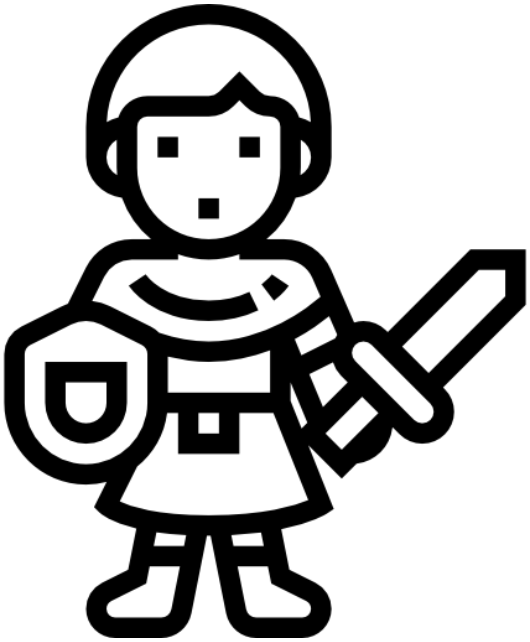


https://www.flaticon.com/free-icon/ninja_921650

lasaris

Forensic-ready medival castle

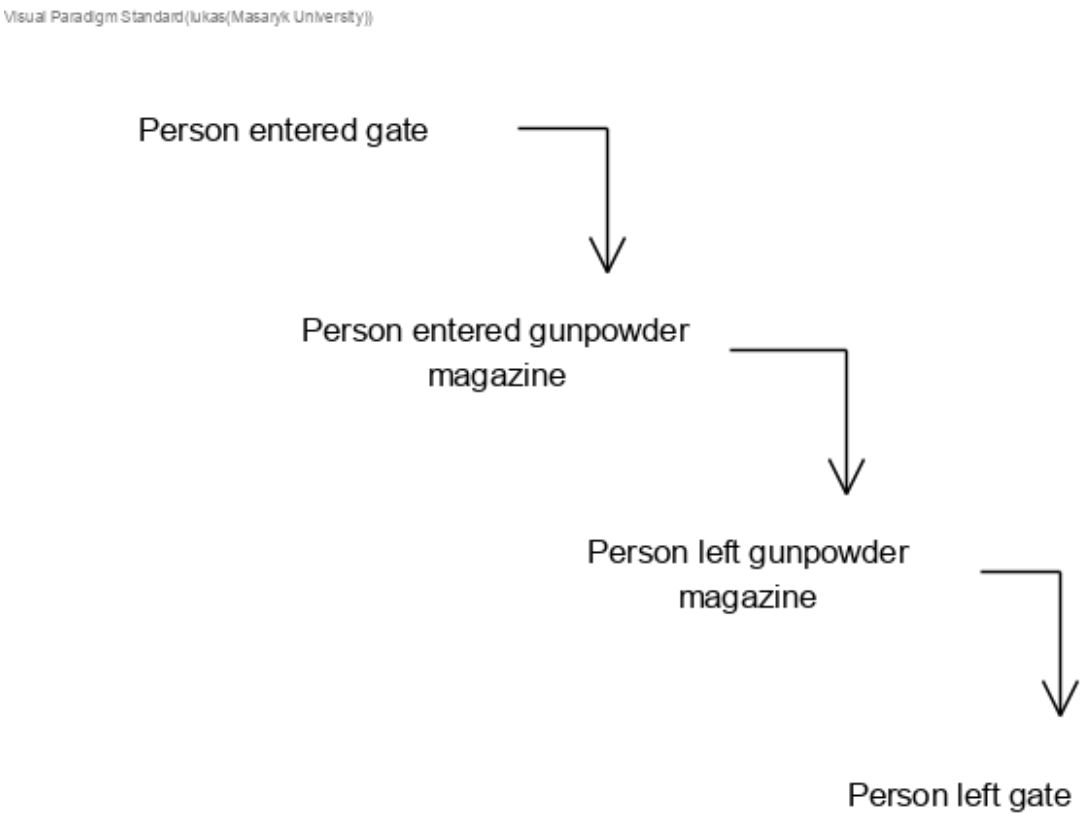
- Audit logs



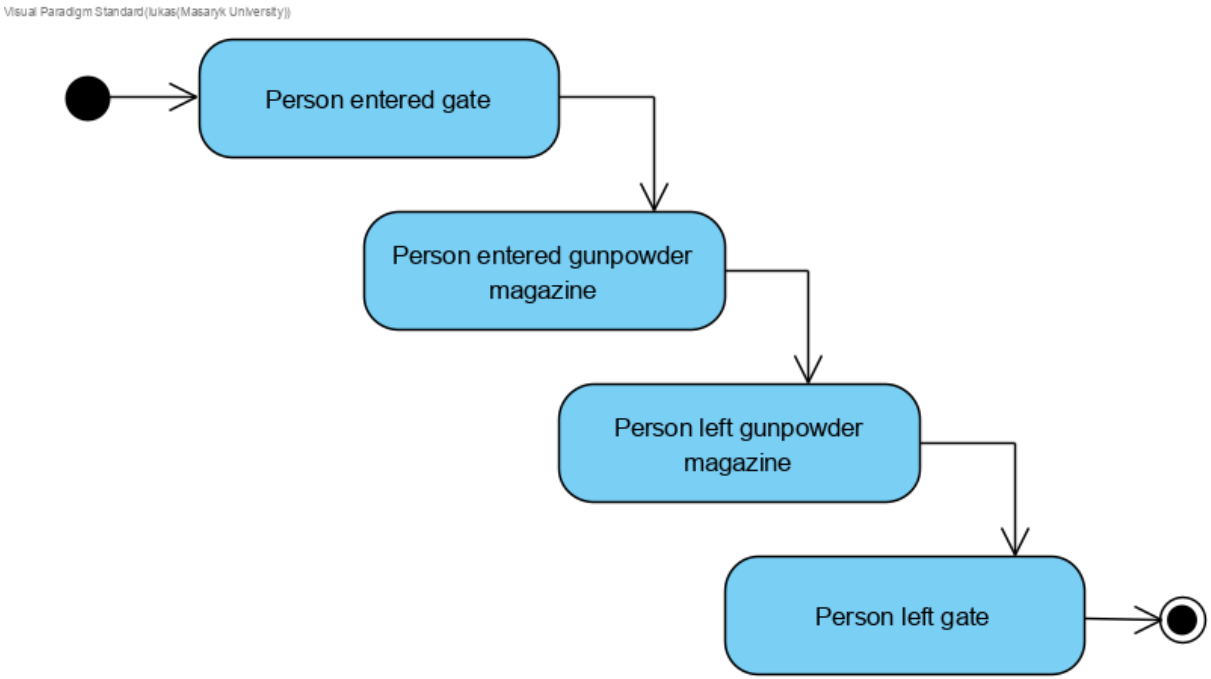
https://www.flaticon.com/free-icon/knight_571064

lasaris

Forensic-ready medival castle - scenario



Forensic-ready medival castle - scenario



lasaris

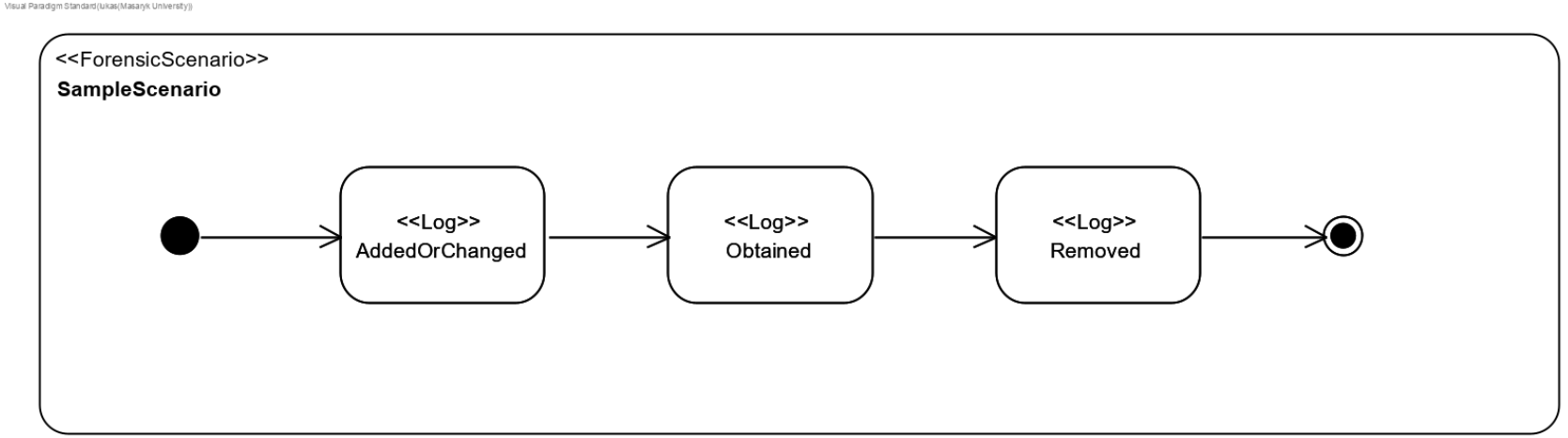
Auditing scenarios for forensic-ready software

- Representation for inner behavior
- High-level scenario
- Understandable for software engineers

lasaris

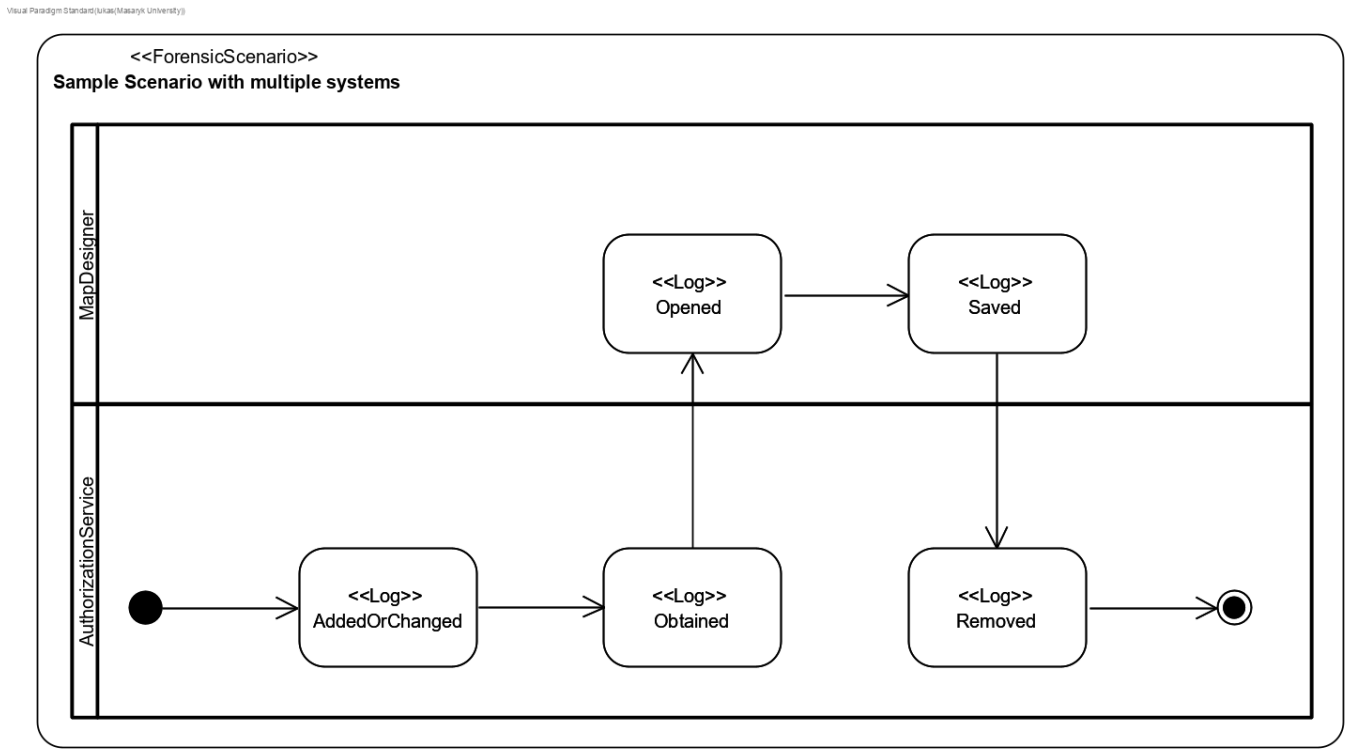
Auditing scenarios for forensic-ready software

- Access control system example



Auditing scenarios for forensic-ready software

- Access control system example



Auditing scenarios for forensic-ready software

- Representation for inner behavior
- High-level scenario
- Understandable for software engineers
- ?

lasaris

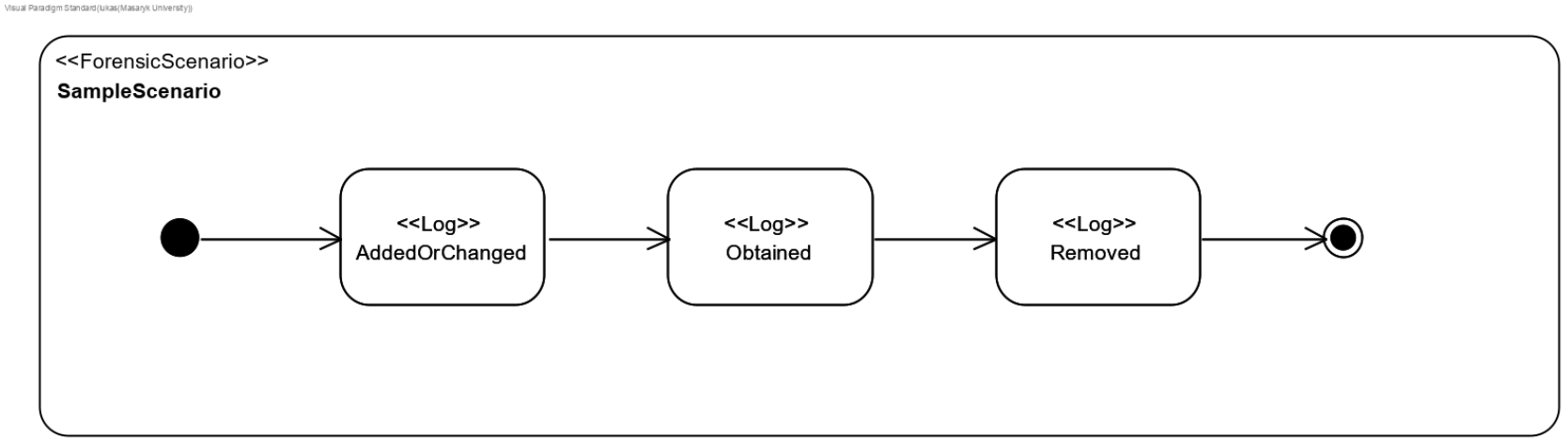
Auditing scenarios for forensic-ready software

- Representation for inner behavior
- High-level scenario
- Understandable for software engineers
- Verification

lasaris

Auditing scenarios for forensic-ready software

- Access control system example



Auditing scenarios - verification

- Verify that the system can capture the scenario
- High-level
- Automatically

lasaris

Auditing scenarios - verification

- Verification based on logs
- Process mining LTL checker
- Automatic generation of formulae

lasaris

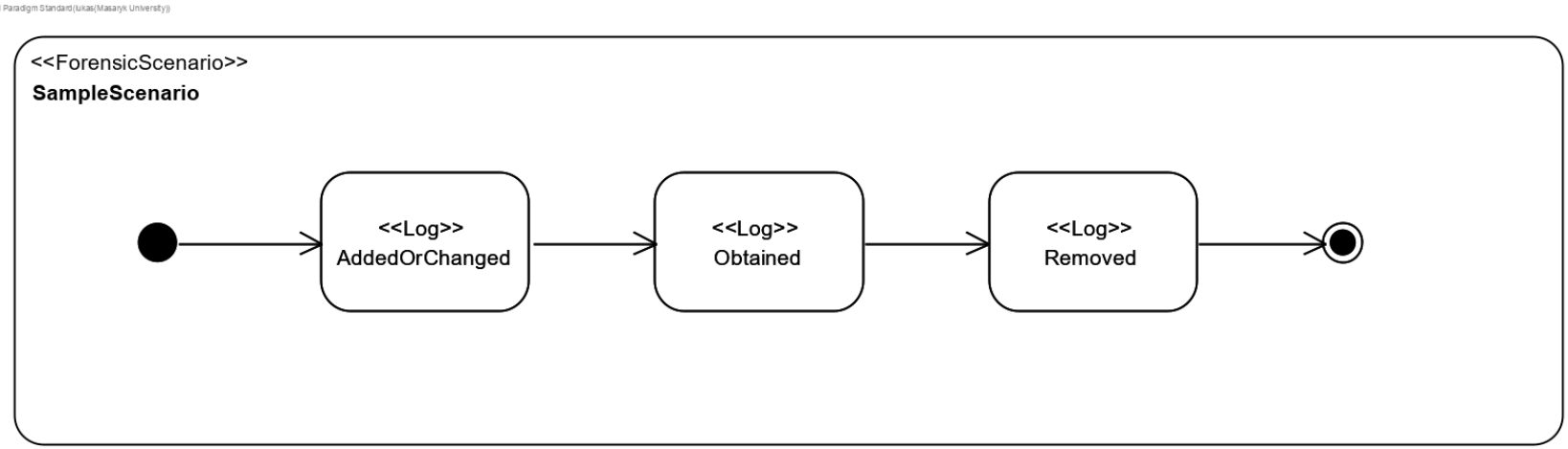
Auditing scenarios - verification

- Verification based on logs
- Process mining LTL checker
- Automatic generation of formulae

lasaris

Auditing scenarios - verification

- Access control system example



<>(AddedOrChanged /\ <>(Obtained))

<>(Obtained /\ <>(Removed))

lasaris

Auditing scenarios - verification

- Useable for live systems
- Language independent
- Implies likability of evidence

lasaris

Conclusion

- For forensic readiness it is important to consider the inner behavior of systems
- Such behavior can be captured in UML diagram
- Based on the diagram, the system can be verified

lasaris