Verification of Forensic Readiness in Software Design and Development

Lukáš Daubner

LAB OF SOFTWARE ARCHITECTURES AND INFORMATION SYSTEMS

FACULTY OF INFORMATICS
MASARYK UNIVERSITY, BRNO

Contents

- What Is Forensic Readiness?
- Verification of Forensic Readiness Requirements
- Relevant Data in Forensic Processes
- Models for Verification of Forensic Readiness

lasaris

What Is Forensic Readiness?

What is Forensic Readiness?

- Definition by J. Tan (2001)
  - Maximizing the usefulness of incident evidence data
  - Minimizing the cost of forensics during an incident response

- General guidelines, oriented on processes
  - Planning the response
  - Training
  - Policy for handing evidence

Forensic Readiness Meets Software Engineering

- Formulated by L. Pasquale (2018)
  - Prepare software system during its development (forensic-by-design)
  - Non-functional requirement

- Requirements
  - Availability
  - Relevance
  - Minimality
  - Linkability
  - Completeness
  - Non-repudiation
  - Data provenance
  - Legal compliance

lasaris

Challenges of Forensic-Ready Systems

- Representation
- Reasoning about
- Methods for engineering
- Verification
- Specific environments (e.g., IoT)

lasaris

Challenges of Forensic-Ready Systems

- Representation
- Reasoning about
- Methods for engineering
- **Verification**
- Specific environments (e.g., IoT)

lasaris

Verification of Forensic Readiness Requirements

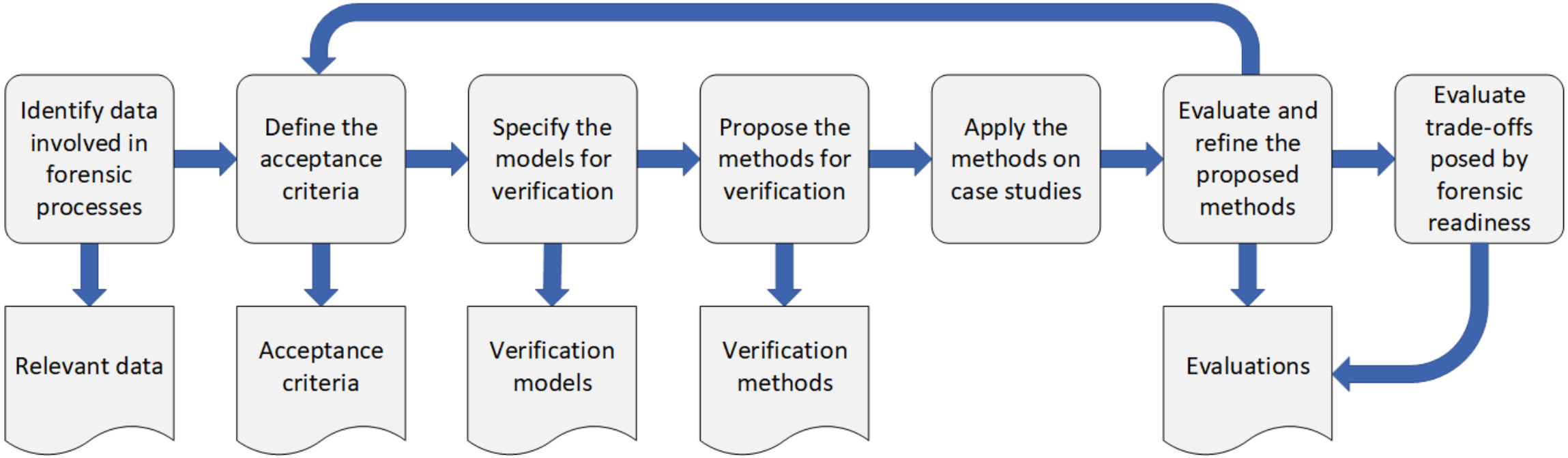
Verification of Forensic Readiness Requirements

- Answers for questions like…
  - Are the FR requirements fulfilled?
  - To what extend?

- And the more abstract…
  - Is it enough?
  - Are we showing due diligence?

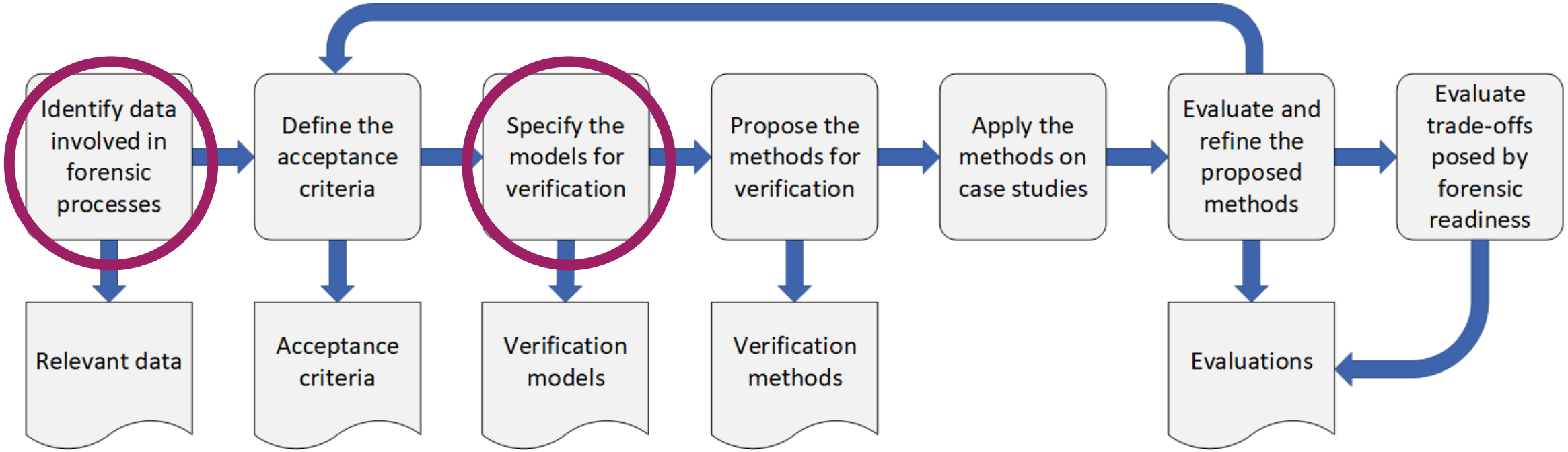
lasaris

Roadmap of Research



lasaris

Roadmap of Research



lasaris

Relevant Data in Forensic Processes

Relevant Data in Forensic Processes

- Data involved in forensic analysis
  - Primary evidence
  - Metadata
- What can we use?
- Which are/can be collected proactively?

Forensic Datasets

- Network traffic
  - PCAP files
  - Http requests
  - Emails
- Memory images
  - Disc
  - Memory snapshot
  - Phones
- Logs
  - Operating system
  - Firewall
  - IDS
  - VPN
  - Application
- Scenarios

lasaris

Forensic Data for Verification

- Evaluation of proposed methods

- Verification of running systems
  - Using what we already have
  - Process mining

Models for Verification of Forensic Readiness

Models for Verification of Forensic Readiness

- No standardized way of FR requirements representation
  - But there is for Security

- Reuse the design methods for secure software
  - UML extensions (e.g., UMLsec)
  - Model-Driven Development

UMLsec for Forensic Readiness

- UML extension
  - Stereotypes
  - Constraints
- Support for formal verification
- Subset of security concerns are relevant for FR
  - Integrity
  - Non-repudiation

Summary

- Forensic Readiness is about making the investigation effective
- Process mining for running systems
- Reusing design methods for secure software
  - UML extensions
  - Model-driven development

lasaris