EUROPEAN UNION
European Structural and Investment Funds
Operational Programme Research,
Development and Education

C4e

Secure Software Modeling Methods for Forensic Readiness

Lukáš Daubner, Tomáš Pitner

LAB OF SOFTWARE ARCHITECTURES AND INFORMATION SYSTEMS

FACULTY OF INFORMATICS
MASARYK UNIVERSITY, BRNO

lasaris

Content

- What Is Forensic Readiness?
- Forensic Readiness Concerns
- Forensic Readiness Concerns Meets Security
- Security Modeling Methods for 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
- Systematic preparation for forensic investigation
- Proactive measures
  - Opposed to actual investigation, which is reactive

lasaris

What is Forensic Readiness?

- Originally, a set of general guidelines

- Expanded in process-oriented approach
  - Collection of evidence
  - Handling of evidence
  - Presentation of evidence
  - Staff training
  - Escalation policies
  - Etc.

- Increases likelihood of successful investigation

lasaris

Forensic Readiness in Software Engineering

- Formulated by Pasquale et al. (2018)
- Prepare software system during its development
  - Forensic-by-design
- Support for:
  - Proactive evidence securing
  - Data provenance
  - Ensuring chain of custody
- Non-functional requirement

lasaris

Open Challenges For Software Engineering

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

lasaris

Open Challenges For Software Engineering

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

lasaris

Forensic Readiness Concerns

Forensic Readiness Concerns

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

lasaris

Forensic Readiness Concerns Meets Security

- Partial overlap with security concerns
- Typically specialized applications of concerns
- Difference between technical and legal understanding
  - Both needs to be addressed

lasaris

Forensic Readiness Concerns Meets Security

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

lasaris

Security Modeling Methods and Forensic Readiness

Security Modeling

- Model-Driven Security
- UML profiles
- Aspect-Oriented Modeling
- Domain Specific Languages

lasaris

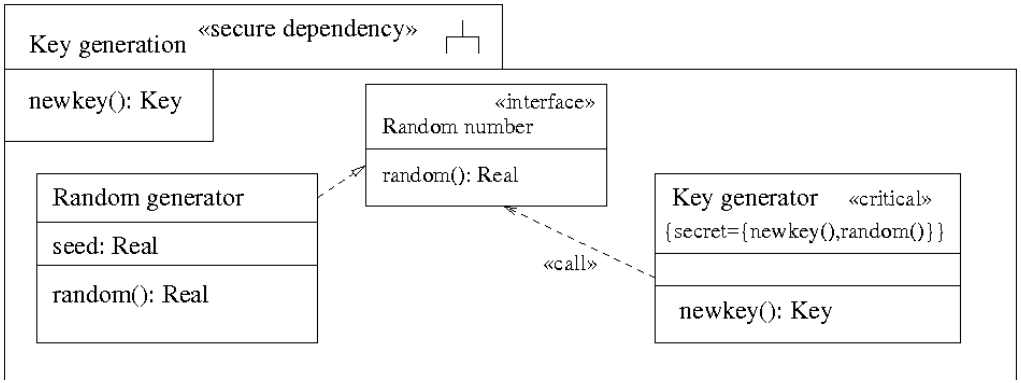
Security Modeling Methods

Method	Domain	Approach	Security concerns
UMLsec	General	UML profile	Integrity, Non-repudiation
SECTET	Distributed workflows	UML profile	Integrity, Non-repudiation
AOMsec	General	AOM, UML profile	Integrity
Sec@Runtime	General	AOM, UML	Integrity
SecureDWs	Data Warehouses	UML profile	Integrity, Non-repudiation, Auditing
ModelSec	General	DSL	Integrity

lasaris

Security Modeling Methods

- UMLsec
  - Mature
  - General-purpose
  - Object level support
  - Verification



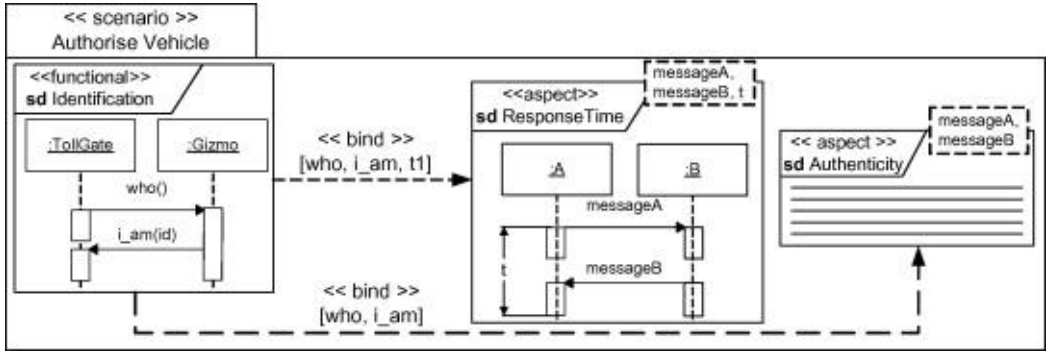
- SECTET
  - Aimed at distributed workflows
  - Relevant concerns defined at messaging level

Jürjens, J. (2002) 'UMLsec: Extending UML for Secure Systems Development', «UML» 2002 — The Unified Modeling Language, Berlin, pp. 412-425.

lasaris

Security Modeling Methods

- AOMsec
  - Separation of concerns
  - Textual specification
- Sec@Runtime
  - Aspect-oriented
  - Runtime weaving
  - Dynamic adaptation

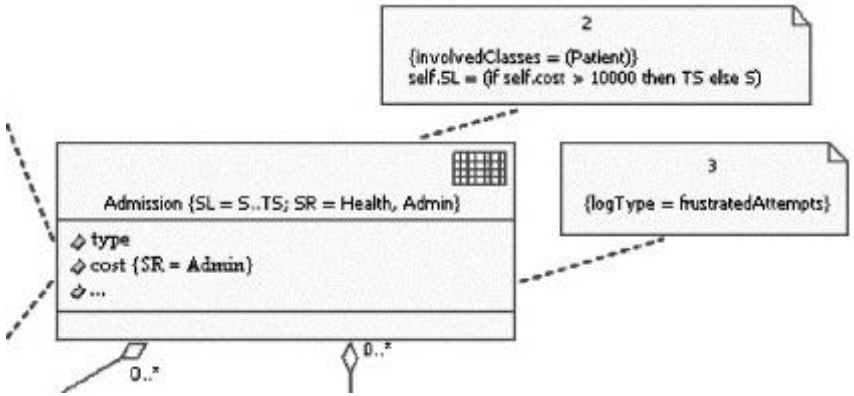


Sánchez, P., Moreira, A., Fuentes, L., Araújo, J. and Magno, J. (2010)
'Model-driven development for early aspects', *Information and Software Technology*, vol. 52, no. 3, pp. 249-273

lasaris

Security Modeling Methods

- SecureDWs
  - Aimed at Data Warehouses
  - Tackles auditing
- ModelSec
  - Chain of models
  - Generation of artifacts
  - Extendable meta-models



Fernández-Medina, E., Trujillo, J., Villarroel, R. and Piattini, M. (2007)
'Developing secure data warehouses with a UML extension'. Information Systems, vol. 32, no. 6, pp. 826-856.

lasaris

Conclusion

- Forensic readiness is about preparing for investigation
  - Yet unexplored in software engineering
- Secure modeling methods are promising in forensic readiness
  - There are overlaps in concerns
  - Although they are not directly applicable
  - They can be used as a basis for forensic readiness modeling

lasaris