CHESS

Cyber-security Excellence Hub in Estonia and South Moravia

Impact of Forensic-Ready Information Systems on the Security Posture

Lukas Daubner, Raimundas Matulevičius, Barbora Buhnova, Matej Antol, Michal Růžička, Tomas Pitner

35th International Conference on Advanced Information Systems Engineering

Zaragoza, June 15, 2023

Funded by the European Union under Grant Agreement No. 101087529. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Research Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

Co-funded by the European Union

The Story …

SensitiveCloud and Forensic Readiness

- Platform for storage and processing of sensitive data
  - E.g., supporting life sciences researches
  - Strong need for information security
  - Build on Kubernetes (K8s), accessible by VPN

- Aspiring for ISO/IEC 27k certification

CHESS
Cyber-security Excellence Hub in Estonia and South Moravia
TARTU ÜLIKOOL 1632 UNIVERSITAS TARTUENSIS
MUNI C4E
Co-funded by the European Union

The Story …

SensitiveCloud and Forensic Readiness

- Platform for storage and processing of sensitive data
  - E.g., supporting life sciences researches
  - Strong need for information security
  - Build on Kubernetes (K8s), accessible by VPN
- Aspiring for ISO/IEC 27k certification
- “I heard that you are doing some logging…”

CHESS
Cyber-security Excellence Hub in Estonia and South Moravia

TARTU ÜLIKOOL 1632 UNIVERSITAS TARTUENSIS

MUNI C4E

Co-funded by the European Union

Forensic Readiness & Forensic-Ready Systems

- Proactive steps for potential (security) incident investigation
  - By-design, for the systems
  - Enhancement of security practices
- When security measures fail
  - Know: Why? Who? How? When? Where?
- Why should you care?
  - ISO/IEC 27001:2013 Annex A.12.4 (observability), Annex A.16.1 (incident response), ...
  - GDPR (quickly assess the scope of a data leak)
  - Local legal obligations (evidence release)

CHESS
Cyber-security Excellence Hub in Estonia and South Moravia
TARTU ÜLIKOOL 1632 UNIVERSITAS TARTUENSIS
MUNI C4E
Co-funded by the European Union

Forensic-Ready Information Systems Security Risk Management

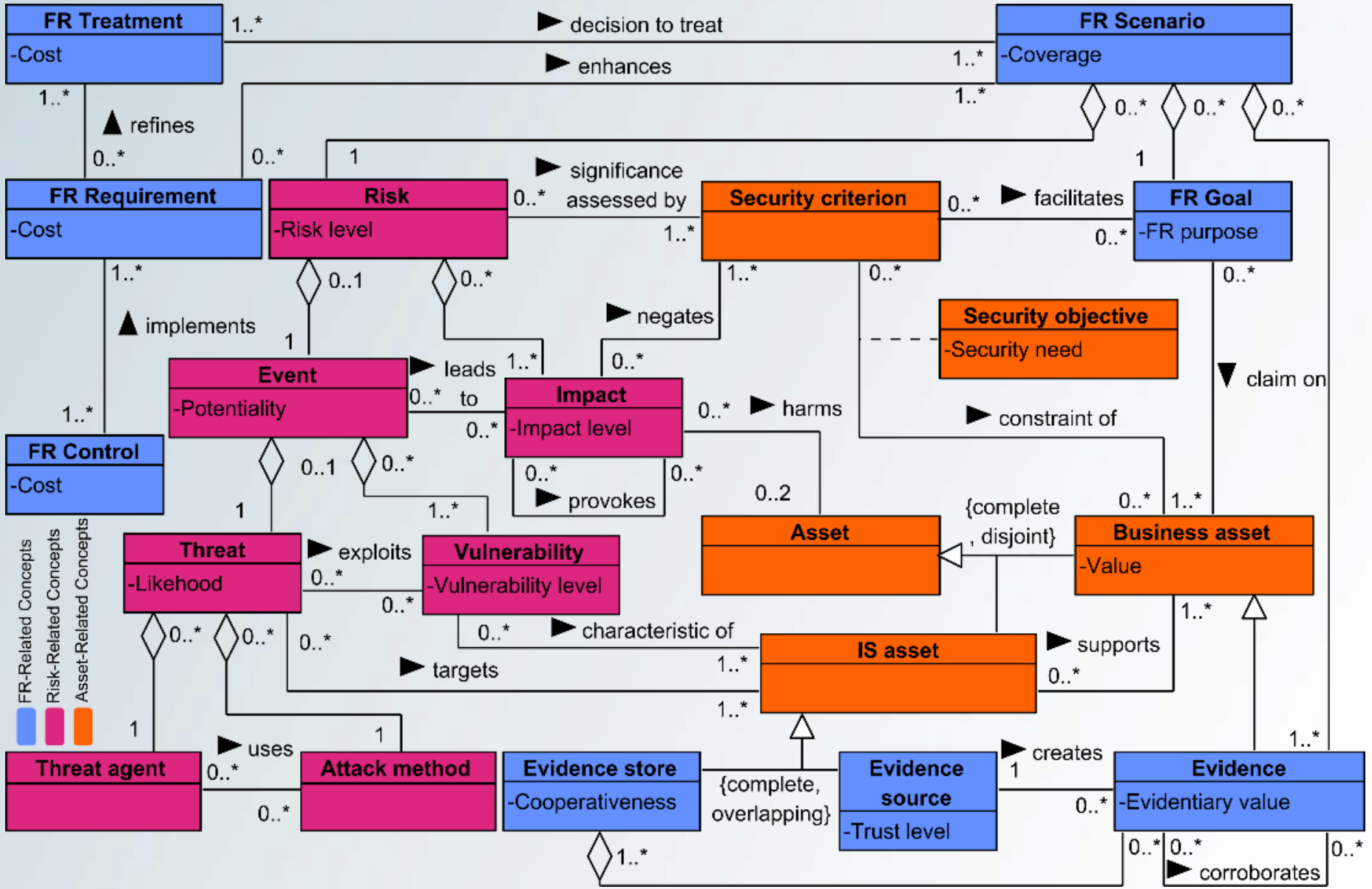
- Risk management is a standard practice in information security
  - Build on its results to assess the forensic readiness
- ISSRM (only security)
  - Risk, Asset, …
- FR-ISSRM (plus forensic readiness)
  - Evidence – information usable for investigation
  - Goal – purpose for implementation
  - Scenario – how is a Goal addressed, given a Risk

CHESS
Cyber-security Excellence Hub in Estonia and South Moravia

TARTU ÜLIKOOL 1632 UNIVERSITAS TARTUENSIS

MUNI C4E

Co-funded by the European Union



CHESS
Cyber-security Excellence Hub in Estonia and South Moravia

TARTU ÜLIKOOL 1632 UNIVERSITAS TARTUENSIS

MUNI C4E

Co-funded by the European Union

Case Study: SensitiveCloud

Research questions

- RQ1: What data is needed to establish a forensic readiness model of an existing information system?
  - Artifacts? Enquiries? How to gather it in a real system?
- RQ2: How can the forensic readiness of a system be evaluated based on the established model and empirical knowledge?
  - How to evaluate the system? Establish its current state to (maybe) improve.
- RQ3: What are the effects of FR-ISSRM process execution and its artefacts on the security posture?
  - How did it help in security? Maybe in monitoring, incident handling, …

CHESS
Cyber-security Excellence Hub in Estonia and South Moravia
TARTU ÜLIKOOL 1632 UNIVERSITAS TARTUENSIS
MUNI C4E
Co-funded by the European Union

Case Study: SensitiveCloud

Phases

- Mapping
  - Review security risk management documentation
  - Establish incentives for forensic readiness
  - Create model of the system
- Evaluation
  - Assess the readiness based on the model
  - Metrics
  - Simulated incident investigation
- Feedback
  - Process the results, interview participants
  - Propose requirements to enhance the system

CHESS
Cyber-security Excellence Hub in Estonia and South Moravia

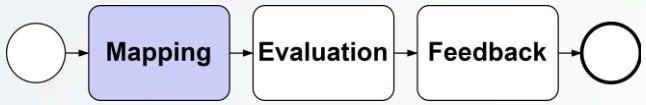
TARTU ÜLIKOOL 1632 UNIVERSITAS TARTUENSIS

MUNI C4E

Co-funded by the European Union

Mapping Phase

Security Risk Management Issues



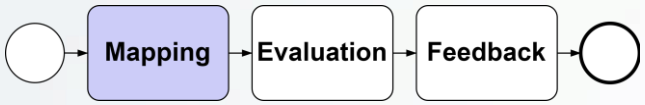
- Focus on technical point of view
  - Only IS Assets / Supporting Assets were considered
  - Remedy: Business Assets / Primary Assets introduced
  - E.g.: VPN vs. logical perimeter

- Abstract formulation of risks
  - Catalogue-like entries
  - Risks instantiated using a description of nominal behavior and how risks can affect it
  - E.g.: *Wireguard VPN Connection* (Asset) can be affected by a *Leaked VPN key* (Impact) due to a *Physical theft of the admin's laptop* (Event)

CHESS
Cyber-security Excellence Hub in Estonia and South Moravia
TARTU ÜLIKOOL 1632 UNIVERSITAS TARTUENSIS
MUNI C4E
Co-funded by the European Union

Mapping Phase

Forensic Readiness Goals

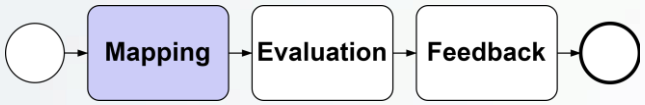


- Prove access to user data
  - E.g., to address disputes or impact
- Enable investigation of logical perimeter access process breach
  - Explain potential breaches
- Prove misuse of user identity
  - Track impersonations
- Enable evidence release of perimeter access process
  - Legal requirement

CHESS
Cyber-security Excellence Hub in Estonia and South Moravia
TARTU ÜLIKOOL UNIVERSITAS TARTUENSIS 1632
MUNI C4E
Co-funded by the European Union

Mapping Phase

Forensic Readiness Scenarios



- Direct instantiation of goals was difficult on abstract risks
  - Asset-level descriptions and models mapped on the risks
- We identified initial potential evidence
  - Based on discussion with technical team
- We chose a high-risk scenario for further analysis
  - Leakage of data on user side
  - Impersonation and misuse of resources

CHESS
Cyber-security Excellence Hub in Estonia and South Moravia
TARTU ÜLIKOOL 1632 UNIVERSITAS TARTUENSIS
MUNI C4E
Co-funded by the European Union

Evaluation Phase

Metrics and Simulation

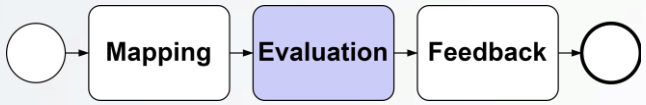
- Forensic readiness metrics based on the model
  - Scenario coverage
  - Relative evidentiary value

- Simulated incident
  - Simulate a realistic attack
  - Let the team handle the incident

CHESS
Cyber-security Excellence Hub in Estonia and South Moravia
TARTU ÜLIKOOL 1632 UNIVERSITAS TARTUENSIS
MUNI C4E
Co-funded by the European Union

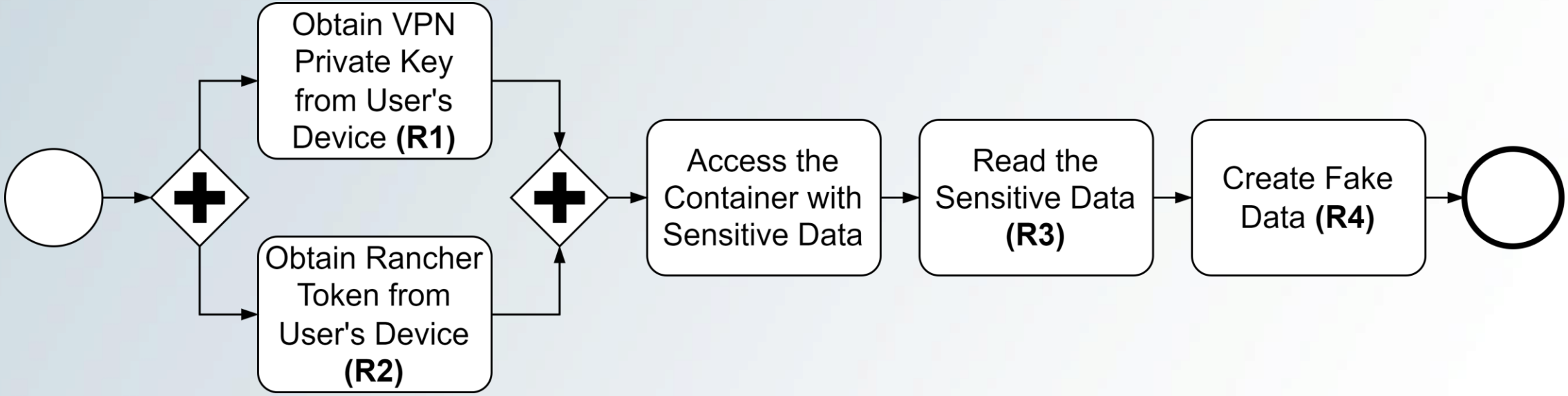
Evaluation Phase

Investigation



- Question:

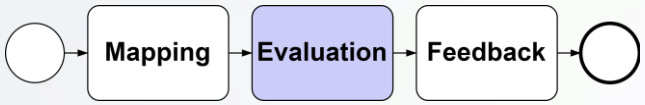
  Which data was accessed, who accessed it and how?



CHESS
Cyber-security Excellence Hub in Estonia and South Moravia
TARTU ÜLIKOOL 1632 UNIVERSITAS TARTUENSIS
MUNI C4E
Co-funded by the European Union

Evaluation Phase

Investigation



- Question:

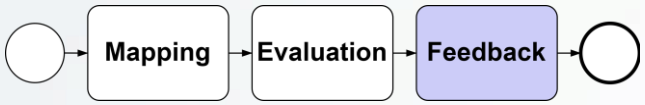
  Which data was accessed, who accessed it and how?

- Problems
  - Mishandling of evidence led to its deletion
  - VPN handshakes not recorded
  - Audit log was misconfigured and missing critical data
  - Proxied IP did not allow tracing
  - Dependance on unreliable data

CHESS
Cyber-security Excellence Hub in Estonia and South Moravia
TARTU ÜLIKOOL 1632 UNIVERSITAS TARTUENSIS
MUNI C4E
Co-funded by the European Union

Feedback Phase

Requirements (in high-level)

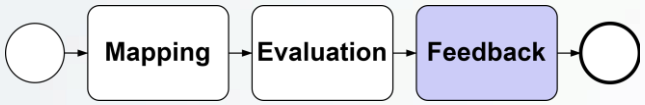


- Independent copies of the important evidence
  - Wireguard Log
- Record the missing evidence
  - Wireguard Handshakes
  - Kube-API Audit
- Correlate with the proxied IP
- Reduce the possibility of evidence tampering
  - Store shell access log outside container

CHESS
Cyber-security Excellence Hub in Estonia and South Moravia
TARTU ÜLIKOOL 1632 UNIVERSITAS TARTUENSIS
MUNI C4E
Co-funded by the European Union

Feedback Phase

Incident Handling Shortcoming

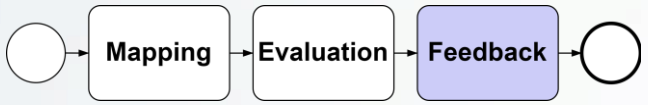


- Incomplete documentation
  - Corruption of the evidence
- Single point of failure
  - Only a single person had the needed expertise
- Incident report handling
  - Establishing the eligibility of the reporter

CHESS
Cyber-security Excellence Hub in Estonia and South Moravia
TARTU ÜLIKOOL 1632 UNIVERSITAS TARTUENSIS
MUNI C4E
Co-funded by the European Union

Feedback Phase

Interview Findings



- Simulation presented a hands-on learning opportunity
- Modeling motivated to look at the system from a different angle
  - Where is the evidence?
  - How does it actually work?
  - On the other hand, it was challenging for the technologically-oriented team
- Practical complement to ISO/IEC 27k certification
  - Iteration of an Information Security Management System
  - Forced people to start thinking about the business side of how to make the system secure

CHESS
Cyber-security Excellence Hub in Estonia and South Moravia
TARTU ÜLIKOOL 1632 UNIVERSITAS TARTUENSIS
MUNI C4E
Co-funded by the European Union

Research Questions Answers

What data is needed to establish a forensic readiness model of an existing information system?

- Risks need to be described in detail
  - Asset-level scenarios helped in understanding how it can happen in the system
- Forensic readiness goals to steer the implementation
  - But the incentive is on the technical parts
  - Need to define high-level business drivers
- Modelling (BPMN process models) is challenging

CHESS
Cyber-security Excellence Hub in Estonia and South Moravia
TARTU ÜLIKOOL 1632 UNIVERSITAS TARTUENSIS
MUNI C4E
Co-funded by the European Union

Research Questions Answers

How can the forensic readiness of a system be evaluated based on the established model and empirical knowledge?

- Metrics
  - Quick, but hard to compare between scenarios
  - Was able to point out issues

- Simulated incident
  - Costly to conduct but very insightful
  - Tests the availability and usefulness of modelled evidence
  - Identifies gaps in the evidence
  - Allows to observe and experience the cooperation during incident handling

CHESS
Cyber-security Excellence Hub in Estonia and South Moravia
TARTU ÜLIKOOL 1632 UNIVERSITAS TARTUENSIS
MUNI C4E
Co-funded by the European Union

Research Questions Answers

What are the effects of FR-ISSRM process execution and its artefacts on the security posture?

- Supports incident handling and investigation process
  - Pre-prepared data pointing to the circumstances
- Security audit
  - Validation of configuration
  - Uncover weaknesses of the system
- Insights into the system
  - Inspection of systems' internal behavior
  - Documentation

CHESS
Cyber-security Excellence Hub in Estonia and South Moravia
TARTU ÜLIKOOL 1632 UNIVERSITAS TARTUENSIS
MUNI C4E
Co-funded by the European Union

Lessons Learned

- Uncovered issues in the system
  - Blind spots, misconfiguration, unreliable data
- Contributed to the overall environment maturity
  - Understating of the system, incident handling
- Continuous evaluation proposed
  - Maintaining the readiness as system and environment changes

Cite, Share, and Subscribe!

CHESS
Cyber-security Excellence Hub in Estonia and South Moravia

TARTU ÜLIKOOL 1632 UNIVERSITAS TARTUENSIS

MUNI C4E

Co-funded by the European Union