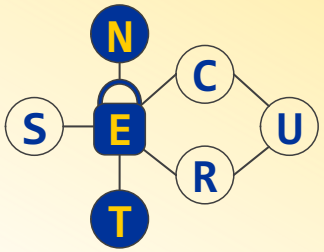


Enhancing Cross-Sectoral Collaboration in Cybersecurity in Estonia, Czechia, Lithuania, Ukraine, and the Netherlands

Funded by the European Union

Analysing Tamper-Resistant Forensic Evidence Storages

Talent 1 Secondment Experience

Lukáš Daubner (University of Tartu)

SECURE-NET Mutual Training Event, 27/08/2026, Kaunas

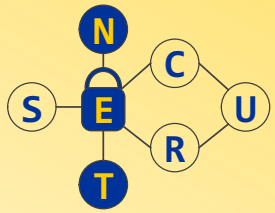
Funded by the European Union Horizon Europe programme under Grant Agreement No. 101217315. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Research Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.


UTARTU
Talent 1 Secondment
Lukáš Daubner
Funded by the European Union

Talent 1

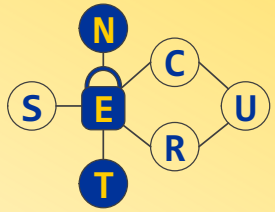
- Local secondment to Cybernetica
  - From academia to industry
- Sharing expertise in forensic readiness
  - Asset discovery
  - Modelling of forensic-ready systems
    - *Assets, risks, potential evidence*
  - Tamper resistance of digital evidence

Talent 1



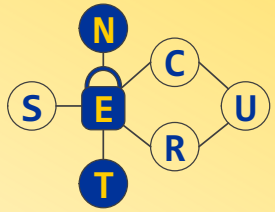
- Local secondment to Cybernetica
  - From academia to industry
- Sharing expertise in forensic readiness
  - Asset discovery
  - Modelling of forensic-ready systems
    - *Assets, risks, potential evidence*
  - **Tamper resistance of digital evidence**

Towards the Paper



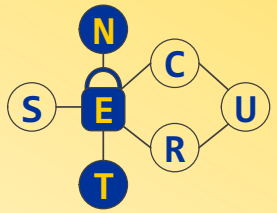
- Tamper-Resistant Evidence Storage
  - Typical requirement in frameworks, guides, …
- There are intuitive ideas
  - Hashing, blockchain, etc...
- But what actually makes and breaks the tamper resistance?

Towards the Paper



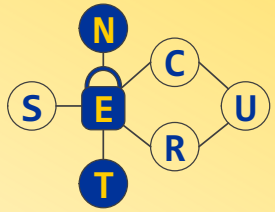
- Tamper-Resistant Evidence Storage
  - Typical requirement in frameworks, guides, …
- There are intuitive ideas
  - Hashing, blockchain, etc...
- But what actually makes and breaks the tamper resistance?
  - **How to implement tamper-resistance of evidence, given a threat model?**

Threat Model



- Tampering attacks on evidence *at rest*
- Threat Actors
  - Origin Access, Storage Access, Infrastructure Admin
- Goals
  - Change the past, Forge evidence, Destroy evidence
- Impacts/Effects
  - Resistant, Evident, Auditable, None

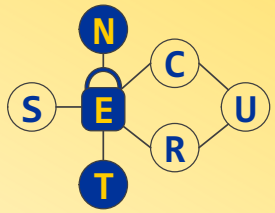
Systematic Literature Review



- Systematic survey of the literature
  - 3129 unique hits
  - 357 relevant publications from the first phase
  - 80 relevant publications from the second phase

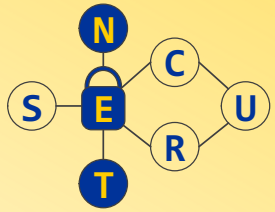
- Analysing what is used
  - Methods & technology
  - Threat model
  - Qualitative factors – dissection of features

Observations: Methods



- Only 10 % provided implementation
  - Despite the presented evaluations
- Distinction between “evidence” and “proof”
  - Booth needs to be protected
  - How?
    - *Distributed consensus*
    - *Replication*
    - *Public release*

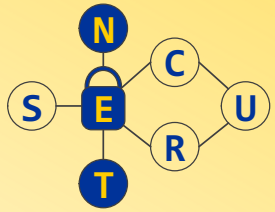
Observations: Methods



- Protection from origin
  - Narrowing the “window of opportunity”
  - Additional layers of protection
  - How?
    - *Forward security shames*
    - *Trusted computing*

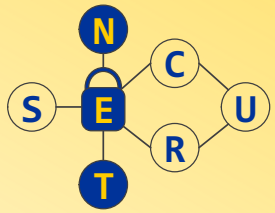
- Specialised hardware

Observations: Factors



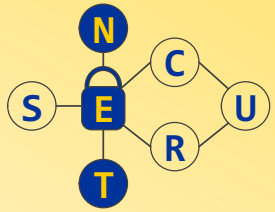
- Timeliness
  - Where is the time recorded?
    - *Origin vs. Storage*
  - Chained Structure = Explicit sequence
- Authenticity
  - Avoids origin impersonation
- Non-repudiation
  - Independent proof

Observations: Factors



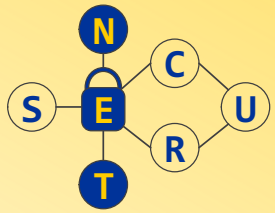
- Integrity
  - From when is it assured?
  - Can I recompute it?
- Redundancy
  - Basic, but underused
- Provenance & Corroborability
  - Underreported

Observations: Attacks



- Origin Access – Forge evidence
  - Time guarantees are critical
  - Who provides the time?
    - *Origin – Forgeable*
    - *Storage – Detectable discrepancy*
    - *Chained structure – Obvious discrepancy*
- Storage Access – Destroy evidence
  - Can the proof show omission?
    - *Standalone proof loses reference*
  - Preventing data loss = resistance
    - *Copies, Backups*

Observations: Attacks



- Storage Access – Change the past
  - Tamper evidence
    - *If there is independent proof, but the evidence is lost*
    - *Origin authenticity plays a role*
  - Tamper resistance
    - *Same as with destruction*

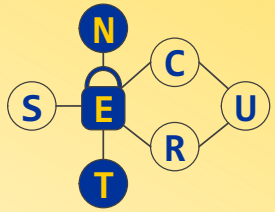
- Infrastructure Admin
  - Distributed or external proof
  - Dependence between entities is often omitted

The Paper

- Submitted to NordSec 2026
  - L. Daubner (UTRATU), M. Merzin (CYBER), R. Matulevičius (UTARTU)
  - Report + Data

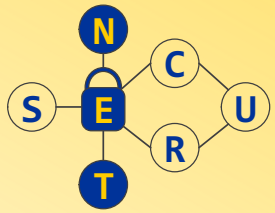
- Dataset
  - Systematic literature review protocol
  - Analysis of the 80 publications
  - Grounds for future work

Future Collaboration



- Follow-up papers
  - Further synthesis from the dataset
- Review of forensic readiness risk management method
  - Based on lessons learned at CYBER
  - Tweaking the tooling
- Further research ideas
  - Exploration of potential evidence links

Conclusion



- Tamper-resistant evidence storage
  - Start from the basics
    - *Backups, Access Control*
  - Consider what provides timing
  - Consider the relationship between evidence and proof
  - Map and provide contextual information
  - Layer in more defences

- Next steps: Actionable steps grounded in the data