Friedrich-Alexander-Universität
Erlangen-Nürnberg

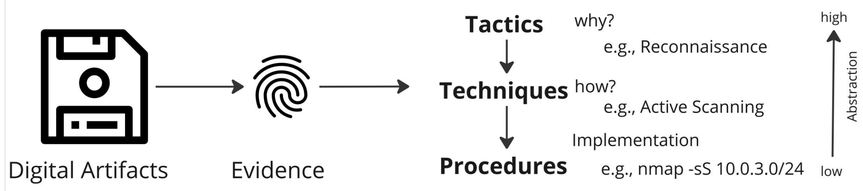
How Hard Is It to Speak ATT&CK?

Designing an Empirical Study on Subjectivity and Abstraction of MITRE ATT&CK

Ella Savchenko

Threat Hunting with TTPs and MITRE ATT&CK

Digital artifacts from cyber incidents are analyzed and classified into ATT&CK TTPs to support systematic threat hunting and standardized intelligence sharing.



Research Questions

How often are attackers' actions misclassified when mapped to the MITRE ATT&CK framework, and what impact does this have on threat hunting and cyber threat intelligence?

Possible Root Causes Under Investigation

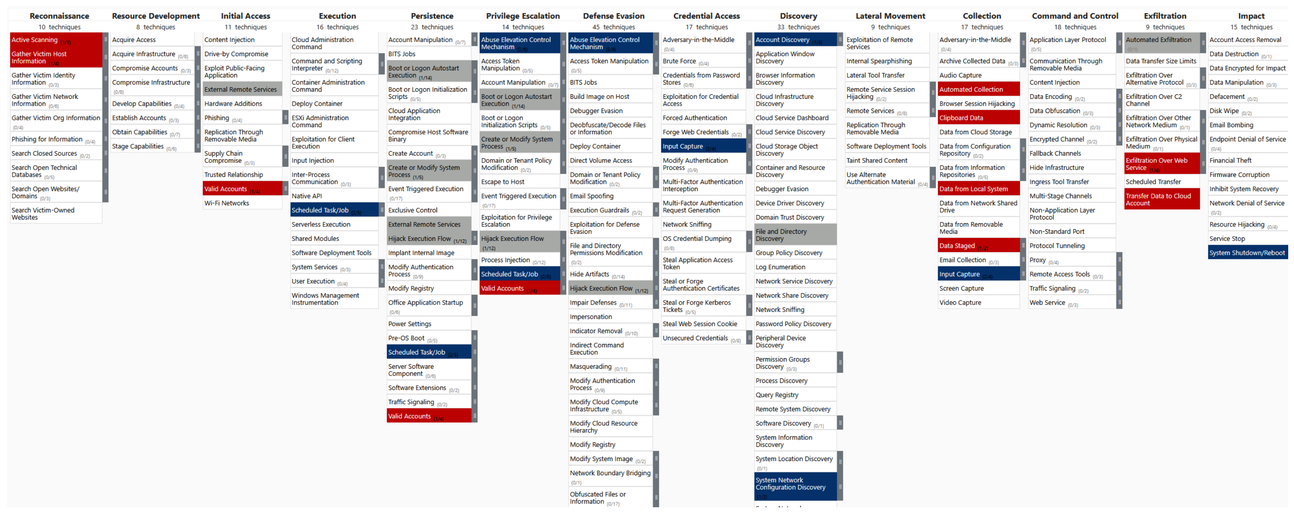
Subjectivity – from framework creators, analysts, and attackers
- To what extent does subjectivity bias the classification?
- How does this bias affect the results?

ATT&CK Framework Design
- Can changes in classification schemes reduce misclassifications?
- Which design improvements could help?

Results from Pre-Studies (2023 - 2025) with Computer Science Students

Objective:
- Reconstructing TTPs from digital attack artifacts
- Part of educational exercises for computer science students

Participants:
23 (2023) / 13 (2024) / 8 (2025)



Attack detected | Attack undetected | Defender false positives

(Preliminary) Results:

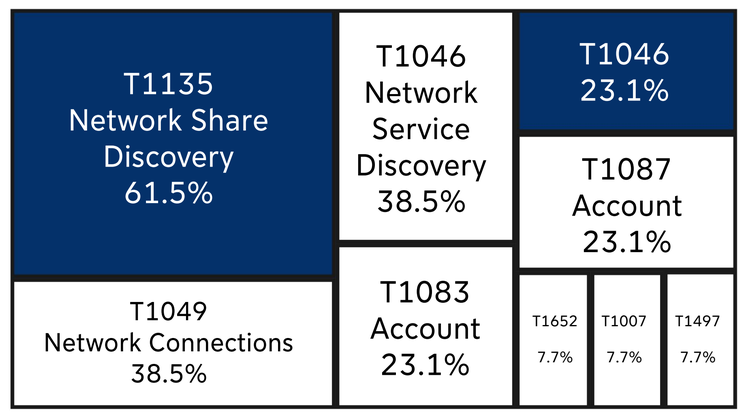
≈ 80 % recognition of procedures from artifacts, YET

≈ 2/3 misclassified when mapping to ATT&CK Techniques.

Example of an attack procedure:

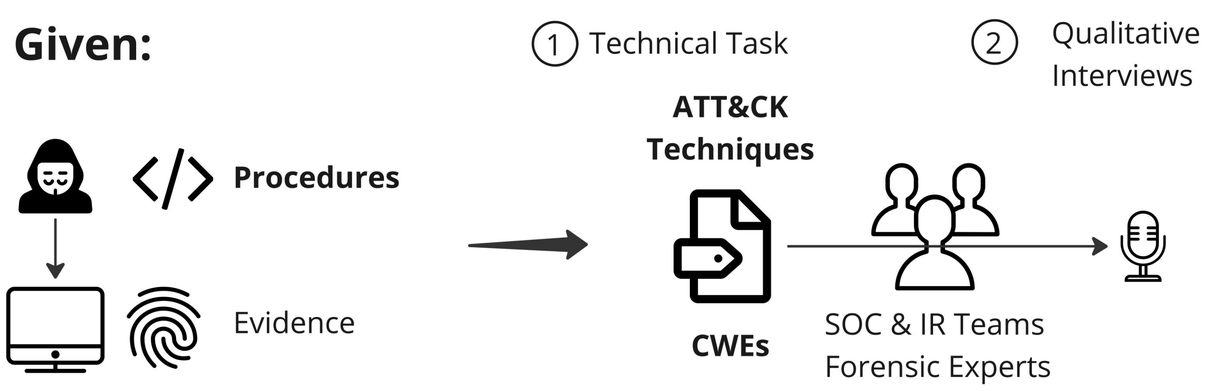
```
Get-PSDrive -PSProvider FileSystem |
Where-Object \{ \$\_.DisplayRoot -like '*'\} |
Select-Object -ExpandProperty DisplayRoot
```

Defender Recognition of Discovery Tactic



→ Need for systematic study of mapping Procedures to ATT&CK Techniques

Design of Planned Study



Contact & Further Information

Please connect with us (ella.savchenko@fau.de) to:
- participate in the study,
- give feedback on our general idea or propose further improvements.

References

[1] Wunder, Julia, Andreas Kurtz, Christian Eichenmüller, Freya Gassmann, and Zinaida Benenson. "Shedding light on CVSS scoring inconsistencies: A user-centric study on evaluating widespread security vulnerabilities." In 2024 IEEE Symposium on Security and Privacy (SP), pp. 1102-1121. IEEE, 2024.
[2] Geras, Thomas, and Thomas Schreck. "The" big beast to tackle": Practices in quality assurance for cyber threat intelligence." In Proceedings of the 27th International Symposium on Research in Attacks, Intrusions and Defenses, pp. 337-352. 2024.

We are looking for professionals interested in contributing to this study.