CONCORDIA

Cyber security cOmpeteNCe fOr Research anD InnovAtion

Current Challenges of Cyber Threat and Vulnerability Identification Using Public Enumerations

Lukáš Sadlek, Pavel Čeleda, Daniel Tovarňák

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 830927.

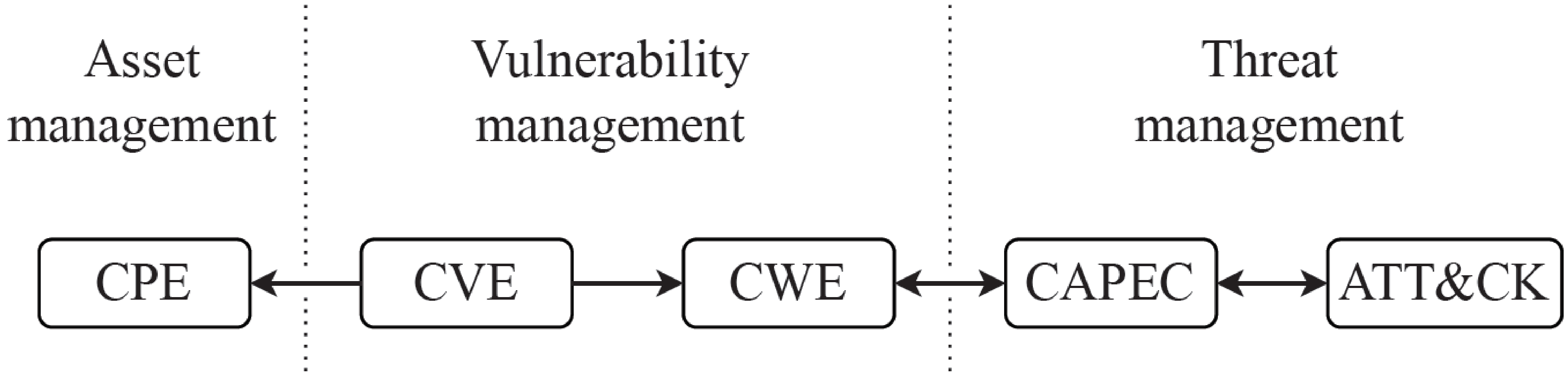
Public Enumerations

- **Identification of cyber threats and vulnerabilities**
    - Reveals **events** jeopardizing assets
    - Enumerations provide **vocabulary**

- **Enumerations**
    - Common Vulnerabilities and Exposures (**CVE**)
    - Common Weakness Enumeration (**CWE**)
    - Common Platform Enumeration (**CPE**)
    - Common Attack Pattern Enumeration and Classification (**CAPEC**)
    - MITRE **ATT&CK**

Enumeration Entries and References

Identifier	Name / Description	Identifier	Name / Description
CVE-2021-44228	Log4Shell vulnerability	CAPEC-486	UDP flood
cpe:2.3:o:debian:debian_linux:11.0:*:*:*:*:*:*:*	CPE match string for Debian 11.0	CAPEC-98	Phishing
		T1566 (in ATT&CK)	
CWE-94	Code injection	T1110 (in ATT&CK)	Brute force



Research Question

1) *What are the* ***current challenges*** *of vulnerability and cyber threat identification* ***using enumerations*** *and data about assets?*

Vulnerability Identification – I

- **General scheme**
  1. Obtain **CPE match string**
  2. Find corresponding **CVEs**

- **Methods for obtaining data**
  - **Active** and **passive** monitoring, **log** management

- **Example approaches for constructing CPE identifiers**
  - **Banner grabbing** – obtains **responses** from open ports
  - **Fingerprinting** – captures network **connection properties**

Vulnerability Identification – II

- **Challenges**
  - **Asset** management
  - Vulnerability **discovery precision**
  - **Amount** of data
  - Implementation of **CPE specifications**

- **Research directions**
  - **Interoperability** of existing approaches
  - **Current** IT environments – **types** of assets

Threat Identification – I

- **Methods**
  - **Graph-based** – events and their relationships
  - **Machine learning** – classification
  - **Natural Language Processing** – entities from CTI reports
  - **Ontologies** – CTI models and cyber threat inference

- **The use of enumerations**
  - **Data** sources
  - Ground **truth**
  - Ontology’s **entities**

Threat Identification – II

- **Challenges**
  - **Unstructured CTI** reports
  - Lack of **visibility** and **amount** of data
  - **Maturity** of methods
    - **TTPs** describe the attacker’s behavior

- **Research directions**
  - **Interoperability** of existing approaches
  - **Machine learning** for threat identification

Research Questions

2) *What is the **usability of MITRE ATT&CK** for threat modeling when only **network monitoring** is used as a source of data?*

3) *What is the **interoperability of** public **enumerations using references** between their entries?*

Analysis of Enumerations

- **Analyses**
  - **MITRE ATT&CK** and network traffic
  - **References** between enumerations
  - Accomplished in **Q1/2022**

- **Dataset**
  - CVEs from **the NVD**
  - CWE and CAPEC from **official websites**
  - Enterprise ATT&CK matrix from the **official Github repository**

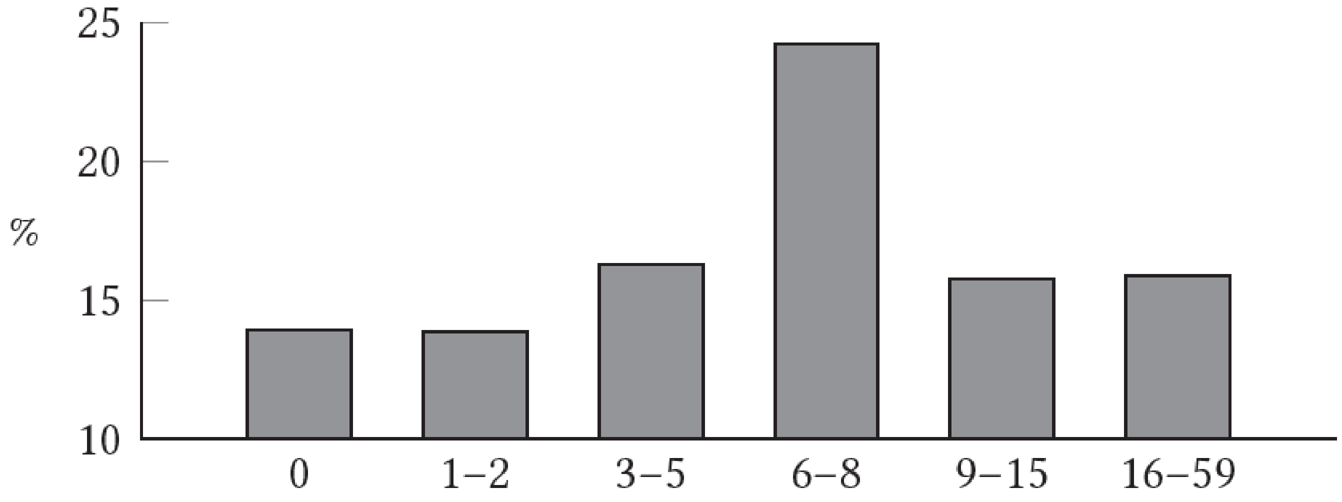
MITRE ATT&CK and Network Traffic

- **Motivation**
  - ATT&CK techniques visible **on the network level**
- **Results**
  - **131** out of 707 **techniques**
  - **13** out of 14 **tactics**
- **Conclusion**
  - ATT&CK **can** be used for threat modeling based on **network traffic**

Data Source	Count of Techniques
Command	256
Process	253
File	192
Network Traffic	**131**
Windows Registry	69
Application Log	55
Module	50

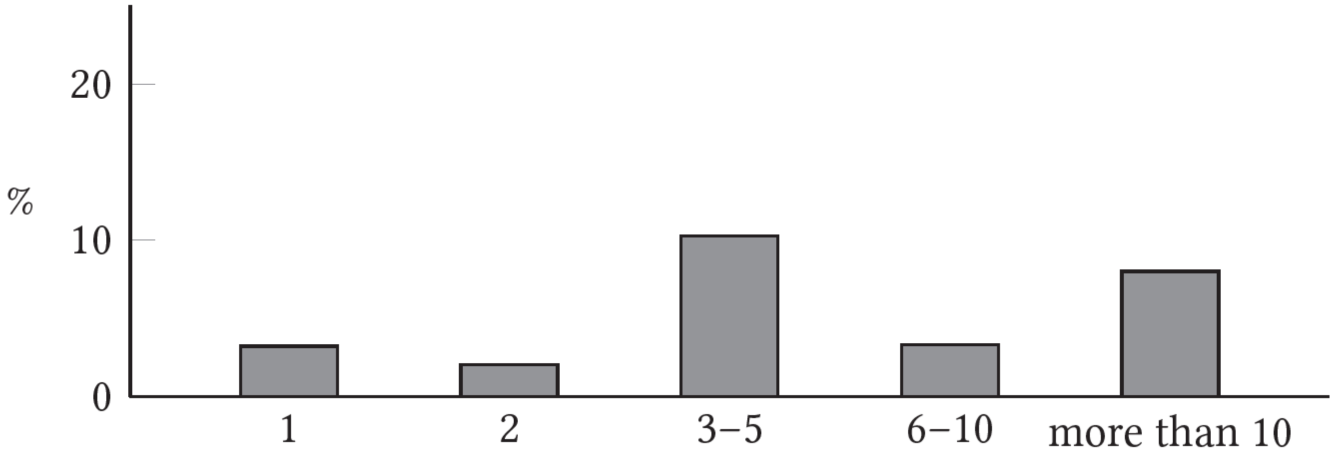
CAPEC and CVE References

- **Motivation:** determine **attack patterns** for CVE vulnerabilities
- **Results:** approximately **30%** of CVEs mapped to 1-5 CAPEC entries
- **Conclusion:** references **do not** allow determining CAPEC entries



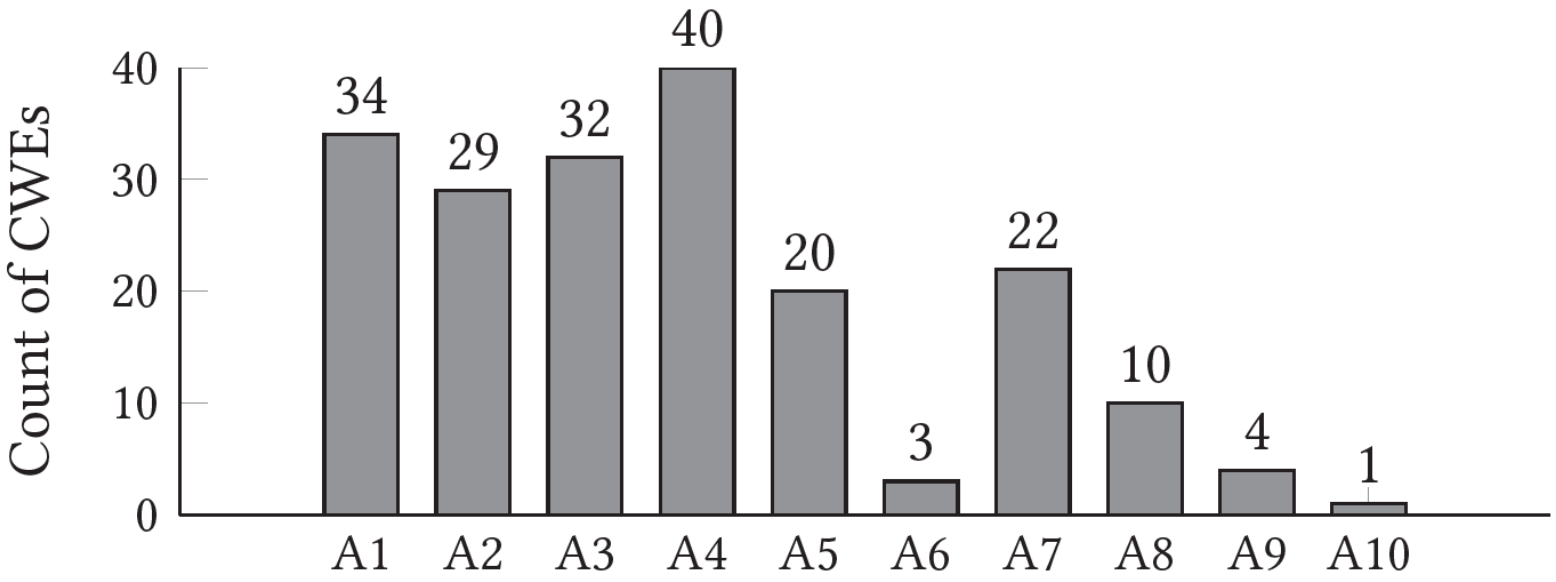
ATT&CK and CVE References

- **Motivation:** determine **ATT&CK techniques** for CVE vulnerabilities
- **Results:** more than **73%** of CVEs have no related ATT&CK techniques
- **Conclusion:** references **do not** allow determining ATT&CK techniques



CWE and OWASP Top Ten

- **Motivation:** mapping to other catalogs
- **Results:** CWEs for OWASP Top Ten categories
- **Conclusion:** CWE is more **granular**



A1	Broken Access Control
A2	Cryptographic Failures
A3	Injections
A4	Insecure Design
A5	Security Misconfiguration
A6	Vulnerable and Outdated Components
A7	Identification and Authentication Failures
A8	Software and Data Integrity Failures
A9	Security Logging and Monitoring Failures
A10	Server-Side Request Forgery (SSRF)

Summary

- **Research questions**
  1. Current **challenges**
  2. Usability of **MITRE ATT&CK** with network monitoring
  3. Interoperability between **enumerations** using their **references**

- **Results of our work**
  - **Full paper** – ACM Digital Library
    - https://doi.org/10.1145/3538969.3544458
  - **Supplementary materials** – scripts for **downloading data** and **analyses** on Zenodo
    - https://doi.org/10.5281/zenodo.6659657

Contact

Research Institute CODE
Carl-Wery-Straße 22
81739 Munich
Germany

contact@concordia-h2020.eu

Follow us

🌐 www.concordia-h2020.eu

www.twitter.com/concordiah2020

www.facebook.com/concordia.eu

www.linkedin.com/in/concordia-h2020

www.youtube.com/concordiah2020