Resilmesh
securing cyber infrastructures

Attack Surface Management: State of the Art and Operational Challenges

Martin Husák, Lukáš Sadlek
Institute of Computer Science, Masaryk University,
Brno, Czech Republic

Funded by the European Union

Introduction

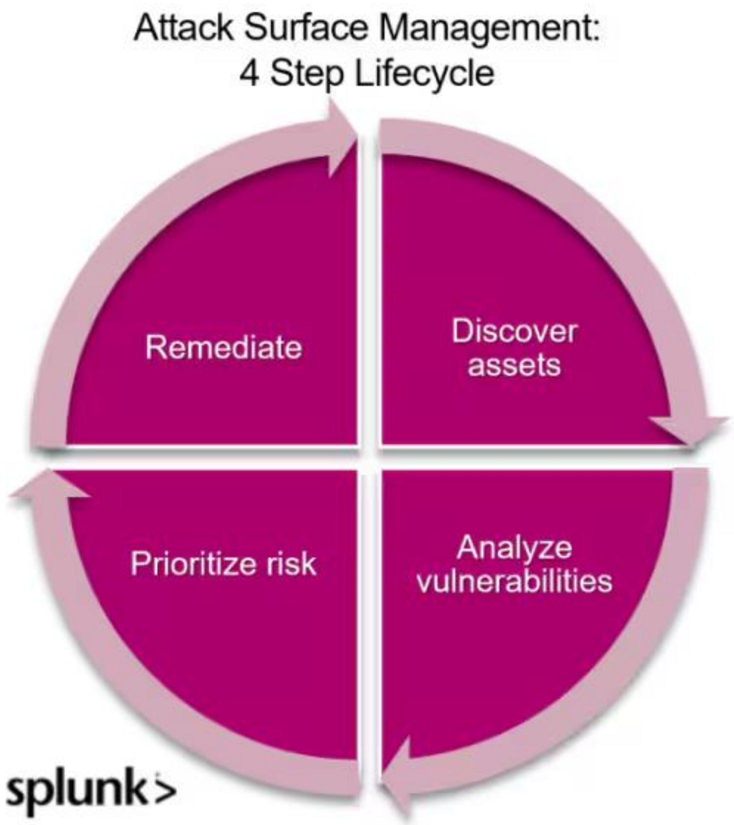
- **Attack Surface Management (ASM)**
  - **IBM**: "... is a continuous discovery, analysis, prioritization, remediation and monitoring of the cybersecurity vulnerabilities and potential attack vectors that make up an organization's attack surface."
  - **Splunk**:"... is continuous monitoring and analysis of an organization's attack surface for potential vulnerabilities and attack vectors, taking remedial measures to address them."
- **Attack surface**
  - Internet-facing assets: devices, network services, endpoints, ...
  - Software versions and configurations of the assets
  - but also organization structure and peoples' names (for social engineering)
- **External x Internal Attack Surface**
  - External - what is visible to external attacker / everybody
  - Internal - what is visible within the organization, e.g., to the insiders (or attackers moving laterally)

Funded by the European Union

Introduction

Four phases of ASM (by Splunk)

- **Asset Discovery**
  - Enumerating all the assets
  - Various approaches, tools, and toolsets
- **Vulnerability Analysis**
  - How could the assets be exploited?
  - Plethora of tools and approaches
- **Risk Prioritization**
  - Which vulnerabilities pose the greatest risk?
  - Which vulnerabilities are easiest to exploit?
  - Are there vulnerable assets exploited before?
- **Remediation**
  - Attack surface reduction
  - Not discussed in this talk - situation dependent



https://www.splunk.com/en_us/blog/learn/what-is-attack-surface-management.html

Funded by the European Union

Resilmesh
securing cyber infrastructures

Lessons Learned

- **Resilmesh project**
  - Situation aware enabled cyber resilience for dispersed, heterogeneous cyber systems
  - Explores the concept of **cybersecurity mesh** - collaborative ekosystem of tools securing modern, distributed enterprises (Gartner)

- **ASM-related components**
  - **CASM – Cyber Attack Surface Management**
    - Attack surface management toolset – network scanners, vulnerability scanners, vulnerability database connectors
    - Orchestration via Temporal.io allows for checking all tasks are done and repeating failed ones
  - **ISIM – Infrastructure and Service Information Model**
    - Data model (ontology) defines entities and relationships in computer networks and their cybersecurity posture, from cyber assets (networks, devices, services, software, data, users) to vulnerabilities (CVEs, impacts)
    - Database – Neo4j graph database, effectively a knowledge graph of local network, clean-up routines
    - REST API and GraphQL API allows access to the data from other components, consistency checks
  - **SACD – Situation Awareness Consolidated Dashboard**
    - Dashboard visualizes the content of ISIM database, e.g., details of a particular asset or vulnerability or overview of how does a vulnerability affects the whole network

Funded by the European Union

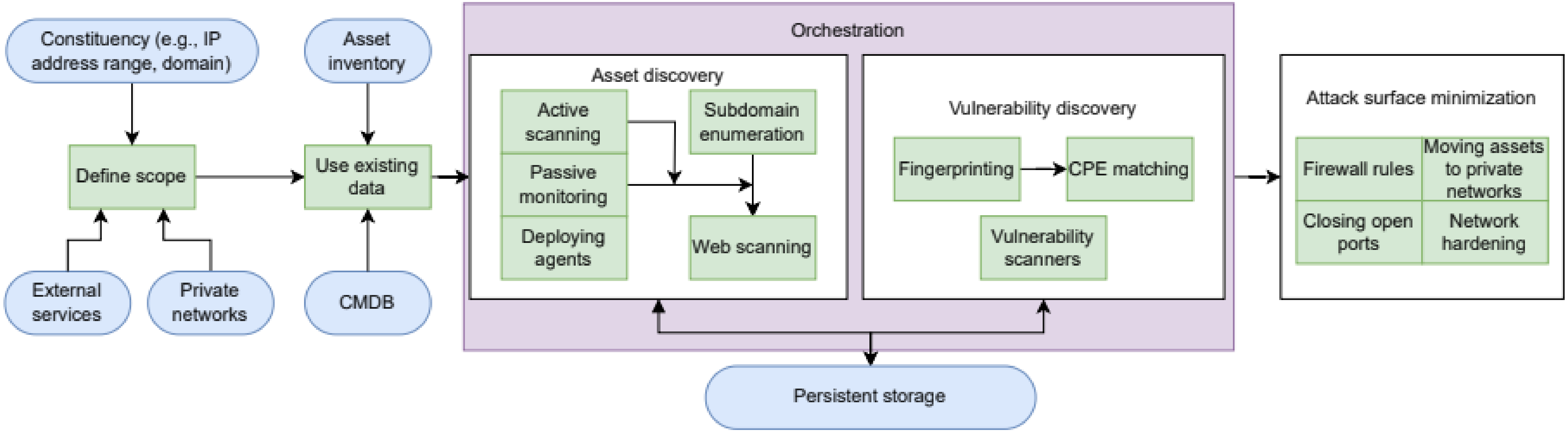
Lessons Learned

- **Research background** is nearly non-existent
  - Primarily innovated by practitioners – and evolving very fast
  - Lack of ground truth, datasets, and metrics – hard to set up an experiment
- **Tools and toolsets**
  - Plethora of tools available (e.g., Project Discovery)
  - Complex toolset, both commercial and open-source, available
  - Limited to external ASM and generic IT
- **Procedures**
  - Well known and generally understood and adopted by practitioners
  - The implementation of individual steps is an open issue
  - There are much more steps to consider and go through than expected
- **Technical limitations**
  - **Low visibility** and lack of tools for ASM outside of generic IT, e.g., in **IoT and OT**
  - **Scalability** is often not addressed and worth investigating in large network
  - **Orchestration** is a vital issue in operations, especially in large networks

Funded by the European Union

Resilmesh
securing cyber infrastructures

Enhanced ASM concept



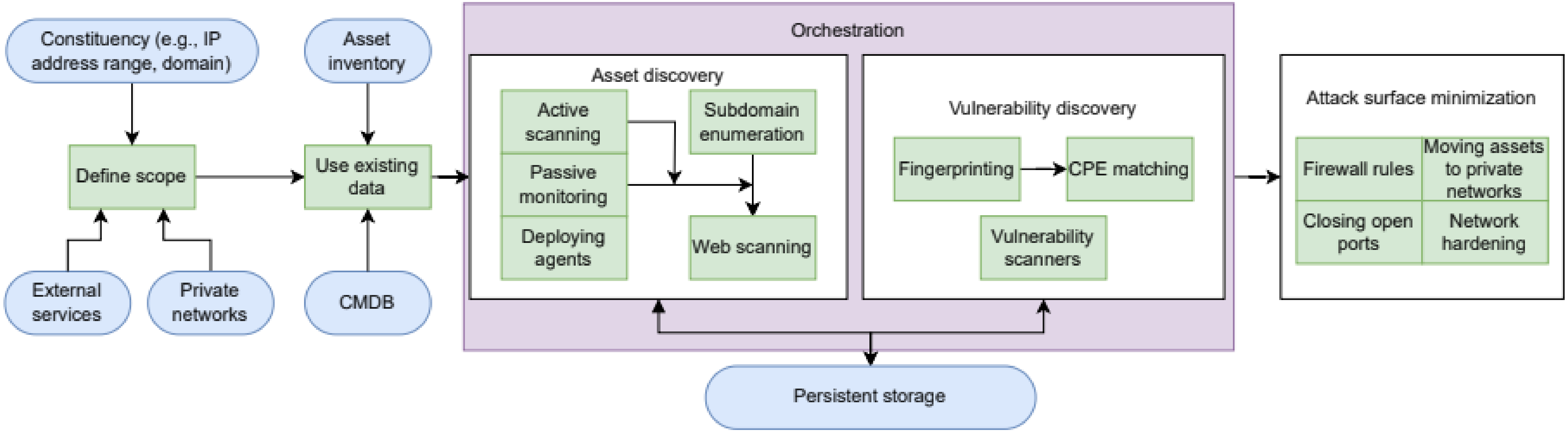
Funded by the European Union

Enhanced ASM concept

- **Define scope**
  - The initial step forgotten in the existing definitions and concepts
  - Should cover the constituency (as understood by CSIRTs), e.g., IP range, domain
  - Exceptions may arise:
    - External assets, e.g., cloud services
    - Some parts of the network may be hard to reach and assess
  - Only external or also internal? How many private networks are there?
- **Use existing data**
  - Does your organization use asset inventory or configuration database?
  - Use as many existing databases, and services as possible
  - Facilitates the discovery of new and unknown assets

Funded by the European Union

Enhanced ASM concept



Funded by the European Union

Enhanced ASM concept

- **Asset discovery via network scanning**
  - Plethora of tools available for every task and use case – Nmap, MASSCAN, web scanners…
  - Advantageous to combine the tools – scan fast for active hosts with MASSCAN, then scan open ports with Nmap to get fingerprints
  - Beware of network congestion in low-throughput parts of the network
  - Not all assets can be found by active scanning (firewall rules, scan taking too long and missing working hours, etc.)
  - Highly dynamic environments (e.g., virtual machines) are an issue
  - Fingerprinting IoTs discloses only the OS, not the purpose of the device
- **Asset discovery via network traffic monitoring (e.g., NetFlow, IPFIX)**
  - A highly viable alternative, if present in an organization (costly)
  - Higher chance of discovering an active asset, but lower quality of fingerprinting
  - Long-term behavior analysis may identify IoT device types (e.g., CCTV camera, smart TVs, various sensors)

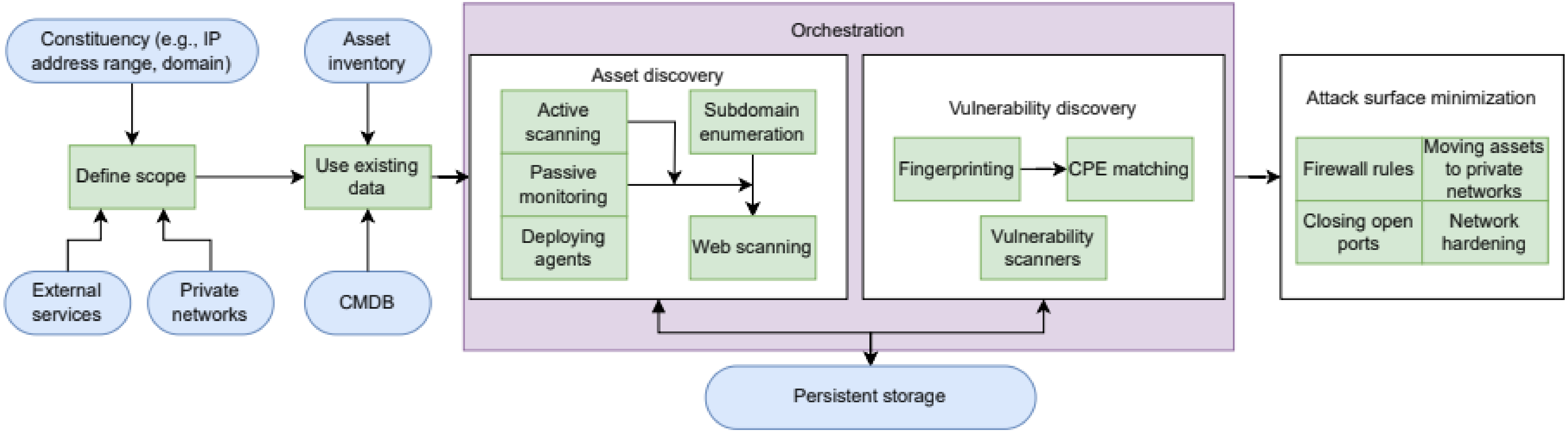
Funded by the European Union

Enhanced ASM concept

- **Vulnerability discovery and confirmation**
  - Simplest solution – get fingerprint in CPE format, look up CVEs by CPE in NVD
    - Highly error-prone, but gives you a rough idea, even in large scale
  - Dedicated vulnerability scanners are slightly better
  - Possible financial issues – high costs for running scans of large networks
    - Still a high false positive rate
  - Confirmation of discovered vulnerability to minimize false positives
    - Nuclei by Project Discovery with community-driven library of detection scripts
  - How to discover vulnerabilities like Log4j?

Funded by the European Union

Enhanced ASM concept



Funded by the European Union

Enhanced ASM concept

- **Persistent storage**
  - Vital for continuous ASM, persistent scanning, and recognizing new assets
  - Traditional relational DBs will serve well
  - ELK or similar will serve well in large scale
  - Graph databases as an emerging technology with promising future research
- **Orchestration**
  - Not addressed by most of the solutions – primary use case if one-time pentest
  - Existing toolsets have one or few hard-coded workflows or require user inputs
  - Orchestrating a toolset is rather not worth it (often no configurability)
  - Define custom workflow and orchestrate with, e.g., Temporal

Funded by the European Union

Summary

- **Attack Surface Management (ASM)**
  - Asset discovery, Vulnerability analysis, Risk prioritization, and Remediation (as defined by Splunk)
  - Common practice of cybersecurity teams, constantly evolving
  - Plethora of tools and toolsets available (e.g., Project Discovery)
- **Implementation of ASM in Resilmesh project**
  - Open-source tools cover most of the tasks of external ASM
  - Heterogeneity of data and tools makes if difficult to create one-size-fits-all solution
  - Proposed an orchestration framework and a “knowledge graph” of local network
- **Future work and research gap**
  - A need to find a solution for highly dynamic environments (virtualization, microservices)
  - Improving the **visibility** in IoT and OT realms via dedicated scanners
  - Improving vulnerability detection and confirmation
  - **Scalability** and **orchestration** in large networks
  - Improving **internal ASM** and scans from multiple vantage points

Funded by the European Union

Resilmesh
securing cyber infrastructures

THANK YOU
for your attention

Questions?

husakm@ics.muni.cz

Funded by the European Union