Identification of Attack Paths Using Kill Chain and Attack Graphs

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.

Introduction

- **Multi-step** attacks
- **Early identification** of event sequencies
- **Attack graphs**
- **Custom rules** for chaining of attack steps
- **Research question**:
  - *Can we merge kill chains and attack graphs to determine targeted cyber threats that jeopardize protected infrastructure and defense against them?*

Threat Models

- **Kill chain**
  - Attacks are **sequences** of steps
  - **Cyber kill chain**
    - Phases are **skipped or duplicated**
- **Attack graphs**
  - Depict **attack paths** in a network
  - Attack paths **not mapped** to the kill chain
  - **Custom set** of attack techniques
  - The right **level of details** required

Step	Name of Phase
1	Reconnaissance
2	Weaponization
3	Delivery
4	Exploitation
5	Installation
6	Command and control
7	Actions on objectives

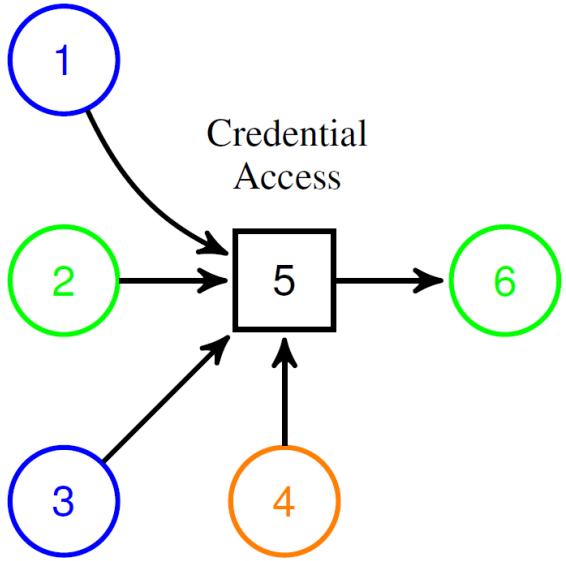
Chaining of Attack Steps

- **STRIDE**
  - Acronym for **six categories:**
    - **Taxonomy** for chaining of attack steps
- Four **types of assets**
  - **Actors**
    - **Examples**: external actor, user accounts
  - **Actions**
    - **Examples**: sending an email, network connection
  - **Data**
    - **Examples**: file, email message
  - **Secondary assets**
    - **Examples**: operating systems, applications

Threat Category	Security Property
Spoofing	Authentication
Tampering	Integrity
Repudiation	Non-repudiation
Information disclosure	Confidentiality
Denial of service	Availability
Elevation of privilege	Authorization

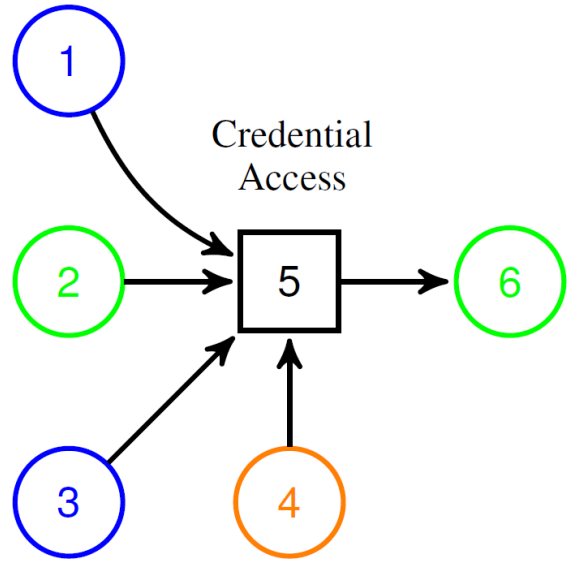
Definition of a Kill Chain Attack Graph

- The **kill chain attack graph** (KCAG) is a triple ***(G, P, f)***:
  - ***G*** = *(V, E)* denotes a **directed graph**
  - ***P*** contains **kill chain phases**
  - ***f*** **assigns** kill chain **phases to** attack **techniques**



Types of Vertices

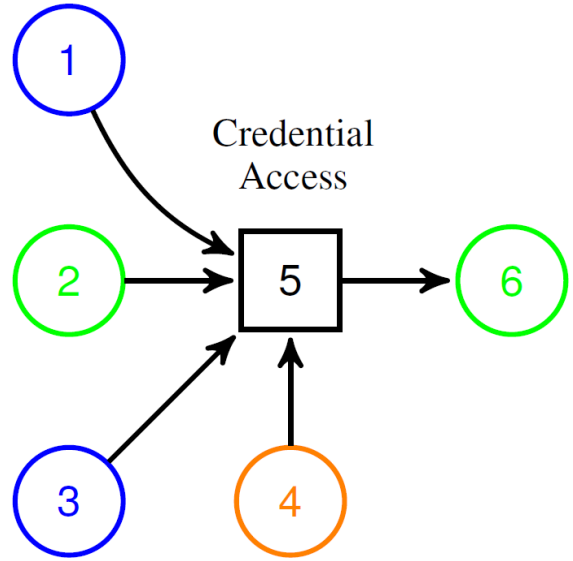
- Attacker's **level of control** over an asset
  - **Level zero**
    - Asset's existence was **not revealed**
    - Represented by an ***external actor***
  - The **first level**
    - Asset's existence was **revealed**
  - The **second level**
    - The attacker **can compromise** asset's security properties taxonomized by STRIDE



ID	Description
2	Violated authentication of SSH network connection to the server.
5	T1110 - Brute Force.
6	Violated authentication of SSH service user account on the server.

Types of Vertices

- **Property** of an asset
  - Information about
    - network **services**
    - vulnerable **applications**
    - user **accounts**
- **Countermeasure**
  - An **employed countermeasure** hinders the use of related attack techniques



ID	Description
1	A user account on SSH service running on the server.
3	SSH service on the server accessible on TCP port 22.
4	The organization does not use a strong password policy.

Types of Vertices

- **Attack technique**
  - Rules describe **input and output** vertices
  - **Incoming edges** from:
    - Asset control **levels**
    - Asset **properties**
    - Not employed **countermeasures**
  - **Outgoing edge** to:
    - **Level** of asset's control
    - Attack **goal**
  - Only **some combinations** of input and output asset types are allowed

Input \ Output	Ext. Actor	Actor	Sec. Asset	Action	Data
Ext. Actor	-	-	-	✓	-
Actor	-	-	✓	✓	-
Sec. Asset	-	✓	✓	✓	✓
Action	-	✓	✓	✓	✓
Data	-	-	✓	✓	-

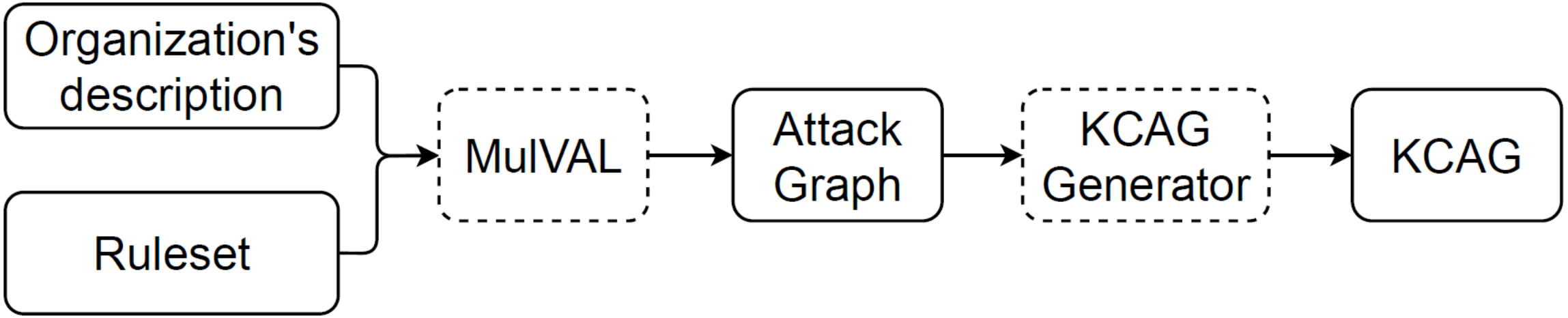
Types of Vertices

- **Attack technique**
  - Mapped to **kill chain phases** using set *P* and mapping function *f*
- **Attack goal**
  - Attacker's objectives – mission-**critical assets**
  - Only **incoming edges**

Tactic (Kill Chain Phase)	ATT&CK ID	Technique Name	Violated Property (STRIDE)
Initial Access	T1190	Exploit Public-Facing Application	Authorization
Execution	T1203	Exploitation for Client Execution	Authorization
Credential Access	T1110	Brute Force	Authentication
Impact	T1485	Data Destruction	Integrity, Availability

Implementation

- Steps
  - **Input files**
    - Organization's **description** – secondary assets, vulnerabilities, and other information
    - **Ruleset** based on MITRE ATT&CK
  - **Attack graph** generated by MulVAL
  - **KCAG** created by the KCAG generator

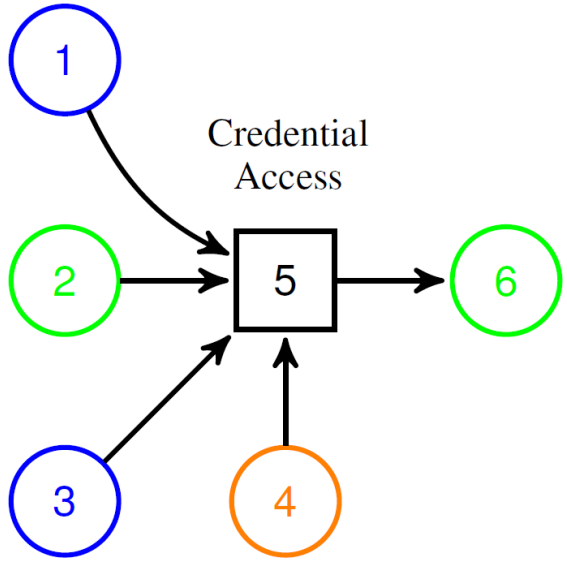


Implementation Workflow

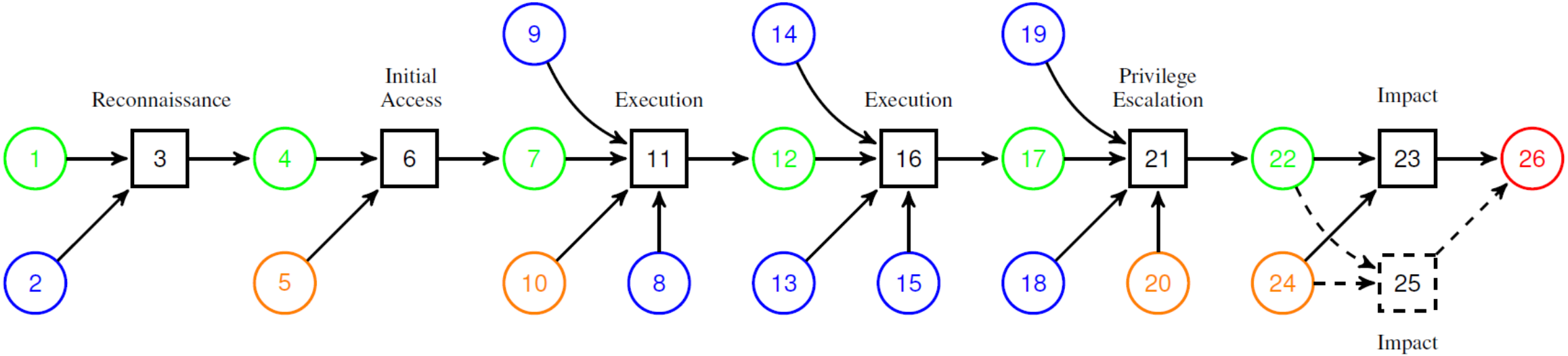
- **Example rule** for brute force:

```
account(2, authentication, User, Identity, H, Software) :-
    networkConnection(2, authentication, H, Protocol, Port),
    networkService(H, Software, Protocol, Port, _),
    hasAccount(Identity, User, H, Software),
    strongPasswordPolicy(no).
```

- **KCAG generator**
  - **Labeling** of vertices
  - Assignment of **kill chain phases**
    - **Partial ordering** of phases
  - **Strategic** techniques and countermeasures

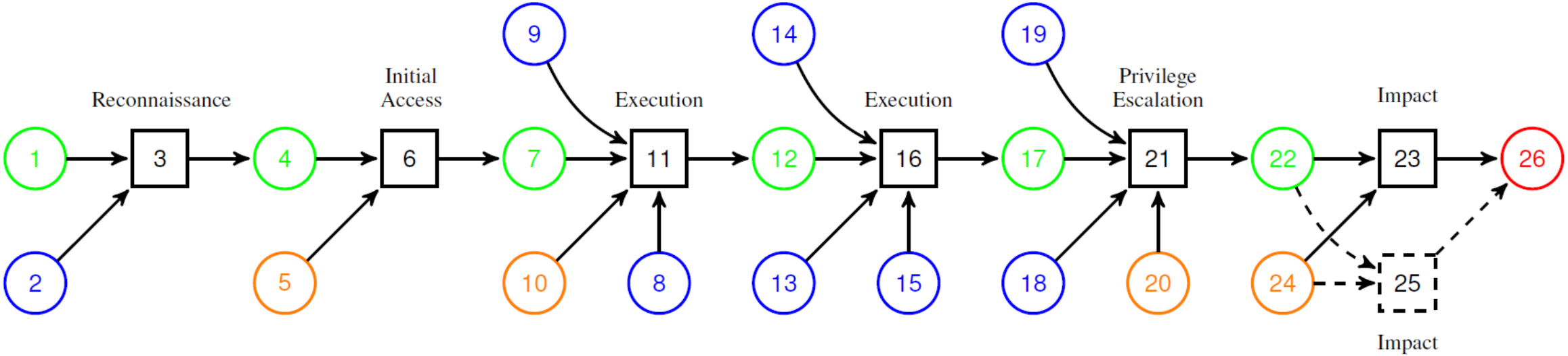


Validation - Kill Chain Attack Graph



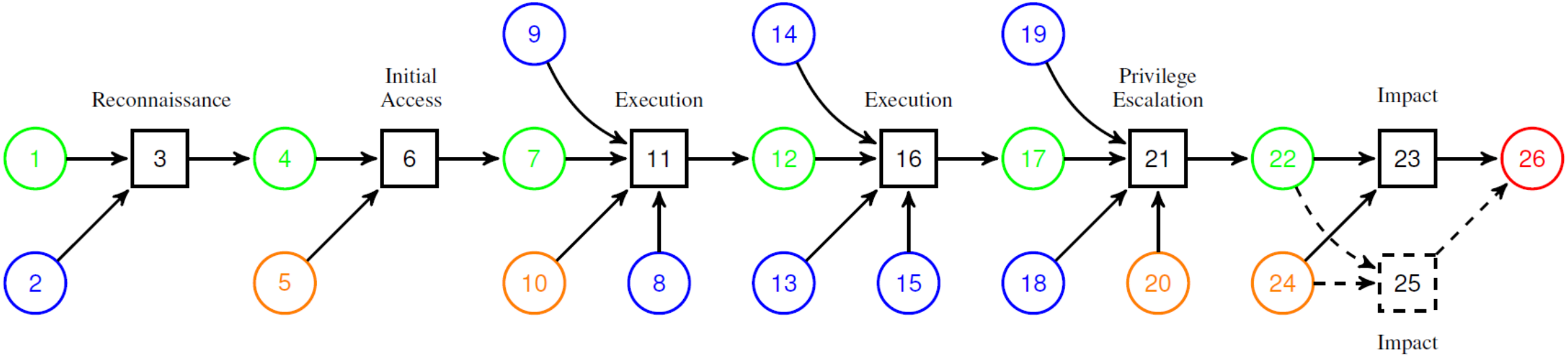
ID	Description	ID	Description
1	External actor.	6	T1566.001 – Spearphishing Attachment.
2	Employee's email address published on a website.	7	Authentication of sending an email was violated.
3	T1594 – Search Victim-Owned Websites.	8	The employee can click on the attachment.
4	The attacker knows that the email address exists.	9	The employee has a user account on a PC.
5	Sender reputation analysis was not accomplished.	10	Training of users was not accomplished.

Validation - Kill Chain Attack Graph



ID	Description	ID	Description
11	T1204.002 – User execution: Malicious file.	16	T1203 – Exploitation for Client Execution.
12	Authentication of opening file action was violated.	17	System's authorization was violated (user rights).
13	Microsoft Office opens files.	18	Microsoft Windows 8.1 is installed on the PC.
14	Microsoft Office is installed on the PC.	19	Microsoft Windows 8.1 contains CVE-2017-0263.
15	Microsoft Office 2016 contains CVE-2017-0262.	20	Software is not regularly updated.

Validation - Kill Chain Attack Graph



ID	Description	ID	Description
21	T1068 – Exploitation for Privilege Escalation.	24	Data backup was not accomplished (countermeasure).
22	The attacker violated the system's authorization (admin rights).	25	T1486 – Data Encrypted for Impact.
23	T1485 – Data Destruction.	26	Integrity of a sensitive file was violated.

Summary

- **Contribution**
  - **A novel** kill chain attack graph
  - **Chaining** of individual attack steps
    - **Asset** type
    - STRIDE **security property**
  - The right **level of details**
    - MITRE ATT&CK
  - **KCAG generator**
- **Future work**
  - Generation in an **imperative language**
  - **Alerts** from detection systems

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