MITIGATE

University of Brighton

Multidimensional, IntegraTed, rIsk assessment framework and dynamic, collaborative risk manaGement tools for critical information infrAstrucTurEs

Automated Attack Paths Discovery

MICHALIS PAVLIDIS

NIKOLAOS POLATIDIS

HARALAMBOS MOURATIDIS

Introduction

- Critical Infrastructures rely on the use of information systems, which consist of software and hardware assets that are interconnected through networks
- Vulnerability:
  - A weakness or a flaw in a software asset, raised either from implementation, design, or other processes, that can be exploited or triggered by an attack. Vulnerabilities could be induced through poor configuration or lack of security patching
- If a vulnerability can be exploited and movement achieved to another asset then we have an attack path
- Attack Paths show all possible paths that an attacker can follow in order to intrude a network and compromise a software asset
- They represent the relationships between vulnerabilities exploited by an attacker and the privileges gained by the attacker

Motivation for attack path discovery

- Vulnerability scanners do not verify that all conditions for a complete attack are met, or identify linked attacks potentially more harmful than individual attacks
- Though they can suggest fixes for local potential problems, they don't consider the network as a whole, proposing a global set of cost-effective defenses designed to protect the network' s most critical assets
- Attack paths can answer "what-if" questions regarding security effects of configuration changes
- Support risk assessment and decision making process in terms of identifying appropriate security measures

MITIGATE

University of Brighton

Input data

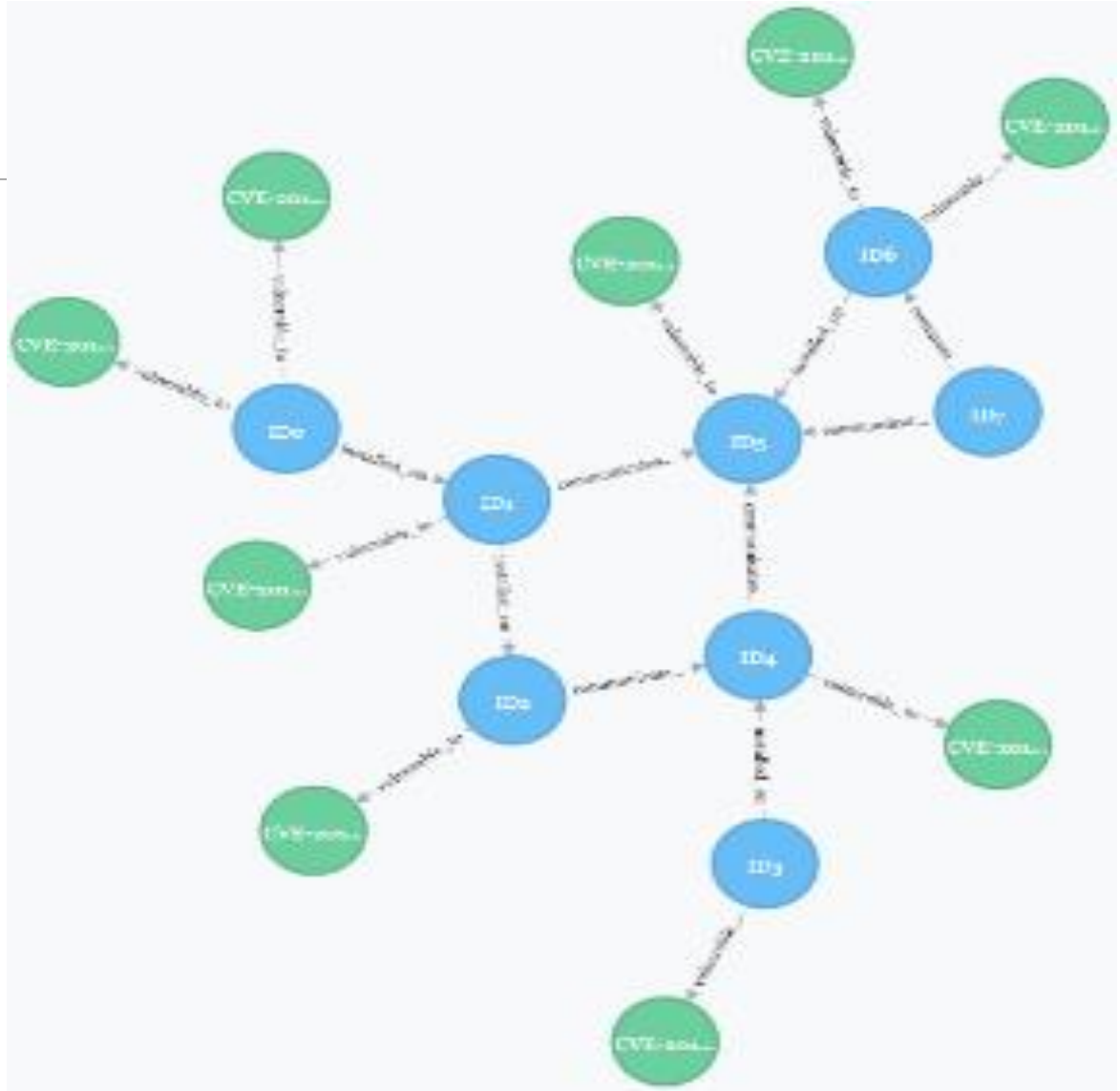
- Network topology and configuration
  - Assets
  - Relationships between assets
    - *Communicates with*
    - *Installed on*
- Software asset vulnerabilities
  - Retrieved from CVE (Common Vulnerabilities & Exposures) & CWE (Common Weakness Enumeration) databases
  - Attributes:
    - Access vector (network, adjacent, local)
    - Access complexity (low, medium, high)

MITIGATE

University of Brighton

Network example

- Use of Neo4j graph database
- Other input data:
  - *Entry asset*
  - *Target asset*
  - *Maximum length*
  - *Propagation length*



MITIGATE

University of Brighton

Input data

- Attacker profile
  - Attacker capability
    - High - The attacker is an expert and has the sufficient resources to perform an attack
    - Medium - The expertise and the resources of the attacker are of a moderate level
    - Low - The attacker has limited resources and expertise to perform an attack
  - Attacker location
    - Local – The attacker has physical access to the asset
    - Adjacent – The attacker is located within the network or in a network that currently communicates with the target network
    - Network – The attacker is in a wider network, such as the internet
  - The attackers profile is used to induce whether a particular attack can exploit an asset's vulnerability

MITIGATE

University of Brighton

Output data

A. Attack paths from the entry asset to the target asset
B. Attack paths from the entry asset to the the k-neighbours around an entry asset. In this case the attacker doesn't have a target asset.

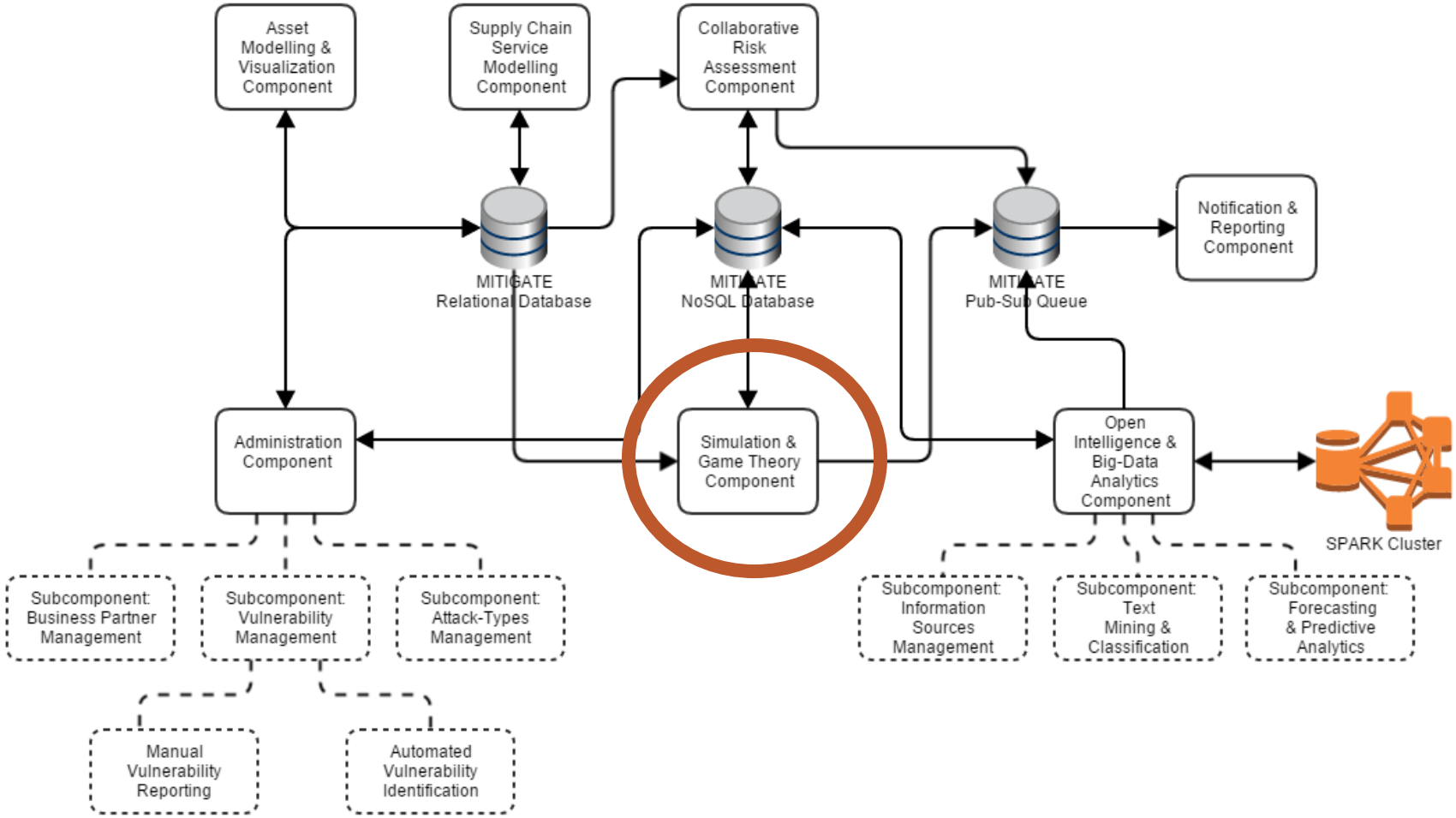
MITIGATE

University of Brighton

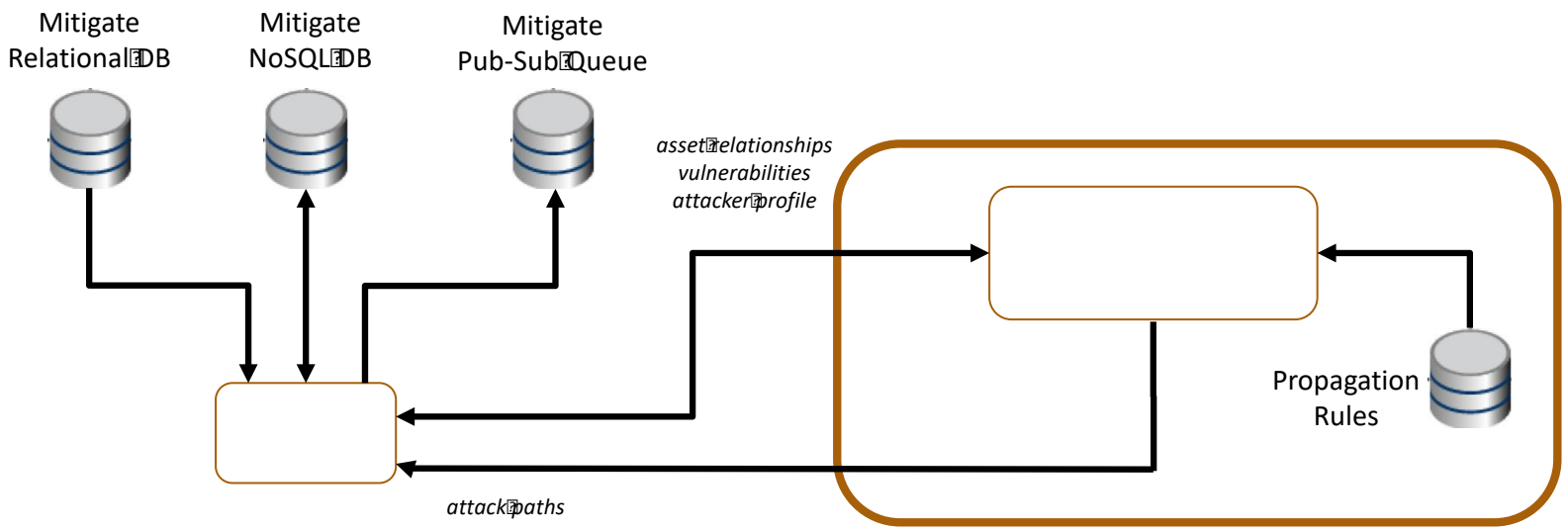
Attackers exploit vulnerabilities

- If an attacker has the required characteristics
  - Is in the right location (location>=access vector) and has the right competence level (capability>=complexity)
  - Can exploit the vulnerability and gain access
  - We map the main threat categories to specific vulnerability categories and access rights
- A connection between two assets is traversable if the starting vulnerability has been successfully attacked and its vulnerability type allows the attacker to use it as a stepping stone to access the end asset

Attack paths discovery as a MITIGATE component



Attack paths discovery as a MITIGATE component

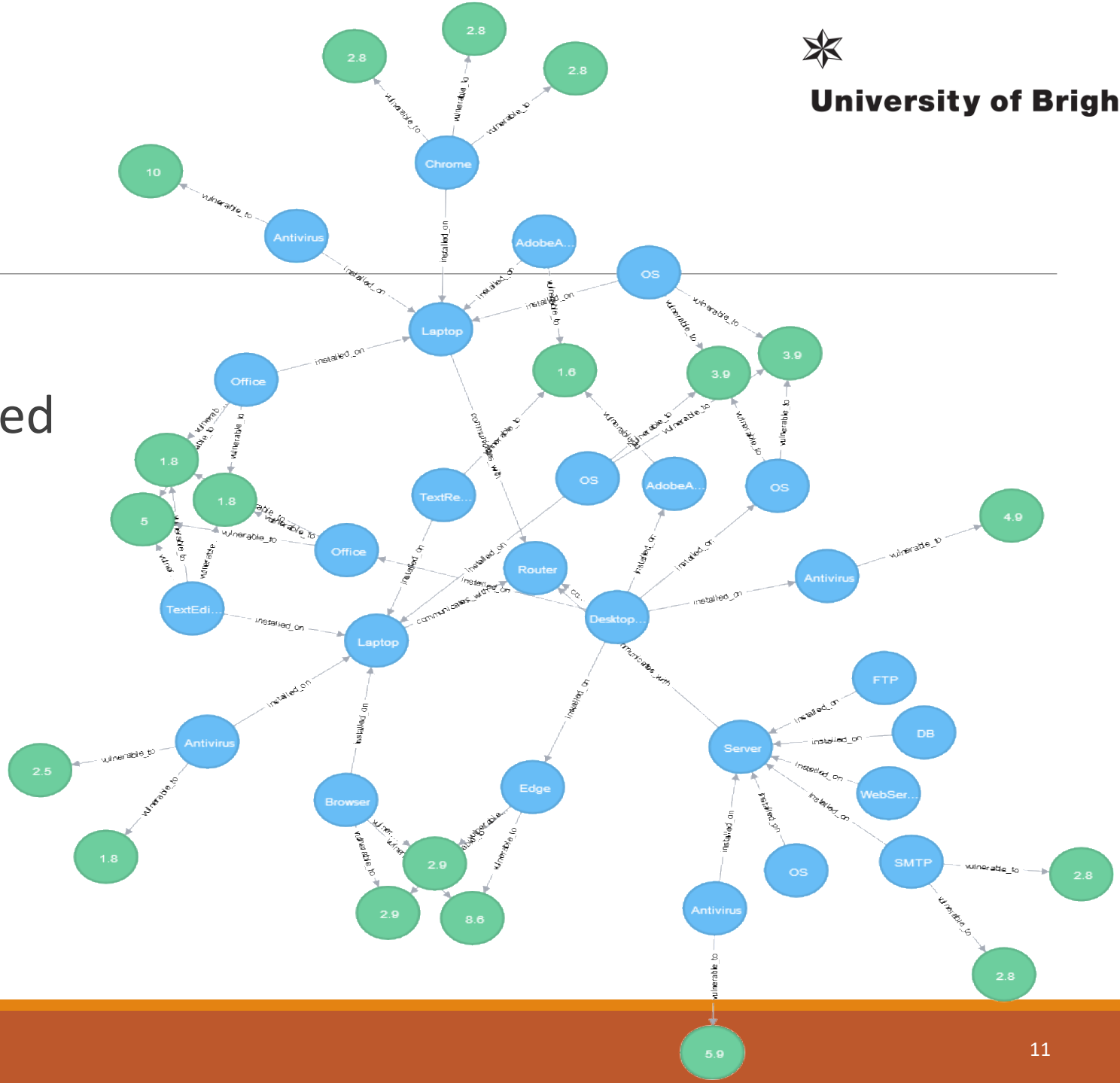


MITIGATE

University of Brighton

Illustration

- 26 assets
- All assets are considered entry points
- Attacker:
  - location: local
  - Capability: high
- maximum length:10



MITIGATE

University of Brighton

Illustration

- Attack paths discovered:

[[5, 0], [5, 0, 1], [5, 0, 1, 8], [5, 0, 1, 14], [5, 0, 1, 14, 15], [5, 0, 1, 14, 16], [5, 0, 1, 14, 17], [5, 0, 1, 14, 18], [5, 0, 1, 14, 19], [5, 0, 1, 20], [7, 0], [7, 0, 1], [7, 0, 1, 8], [7, 0, 1, 14], [7, 0, 1, 14, 15], [7, 0, 1, 14, 16], [7, 0, 1, 14, 17], [7, 0, 1, 14, 18], [7, 0, 1, 14, 19], [7, 0, 1, 20], [9, 8, 1, 0], [9, 8, 1], [9, 8], [9, 8, 1, 14], [9, 8, 1, 14, 15], [9, 8, 1, 14, 16], [9, 8, 1, 14, 17], [9, 8, 1, 14, 18], [9, 8, 1, 14, 19], [9, 8, 1, 20], [10, 8, 1, 0], [10, 8, 1], [10, 8], [10, 8, 1, 14], [10, 8, 1, 14, 15], [10, 8, 1, 14, 16], [10, 8, 1, 14, 17], [10, 8, 1, 14, 18], [10, 8, 1, 14, 19], [10, 8, 1, 20], [11, 8, 1, 0], [11, 8, 1], [11, 8], [11, 8, 1, 14], [11, 8, 1, 14, 15], [11, 8, 1, 14, 16], [11, 8, 1, 14, 17], [11, 8, 1, 14, 18], [11, 8, 1, 14, 19], [11, 8, 1, 20], [12, 8, 1, 0], [12, 8, 1], [12, 8], [12, 8, 1, 14], [12, 8, 1, 14, 15], [12, 8, 1, 14, 16], [12, 8, 1, 14, 17], [12, 8, 1, 14, 18], [12, 8, 1, 14, 19], [12, 8, 1, 20], [21, 20, 1, 0], [21, 20, 1], [21, 20, 1, 8], [21, 20, 1, 14], [21, 20, 1, 14, 15], [21, 20, 1, 14, 16], [21, 20, 1, 14, 17], [21, 20, 1, 14, 18], [21, 20, 1, 14, 19], [21, 20], [22, 20, 1, 0], [22, 20, 1], [22, 20, 1, 8], [22, 20, 1, 14], [22, 20, 1, 14, 15], [22, 20, 1, 14, 16], [22, 20, 1, 14, 17], [22, 20, 1, 14, 18], [22, 20, 1, 14, 19], [22, 20], [23, 20, 1, 0], [23, 20, 1], [23, 20, 1, 8], [23, 20, 1, 14], [23, 20, 1, 14, 15], [23, 20, 1, 14, 16], [23, 20, 1, 14, 17], [23, 20, 1, 14, 18], [23, 20, 1, 14, 19], [23, 20], [24, 20, 1, 0], [24, 20, 1], [24, 20, 1, 8], [24, 20, 1, 14], [24, 20, 1, 14, 15], [24, 20, 1, 14, 16], [24, 20, 1, 14, 17], [24, 20, 1, 14, 18], [24, 20, 1, 14, 19], [24, 20]]

MITIGATE

University of Brighton

Performance evaluation – 26 assets

No. of test	Attacker capability	Attacker location	Propagation length	Max length	No. of entry points	No. of target points	No. of Paths found	Time in Sec
1	Low	Local	3	3	2	2	0	0.7
2	Low	Local	3	3	3	3	0	0.9
3	Low	Adjacent	3	3	2	2	0	0.8
4	Low	Adjacent	3	3	3	3	0	0.9
5	Low	Network	3	3	2	2	0	0.7
6	Low	Network	3	3	3	3	0	0.7
7	Medium	Local	4	4	2	2	0	0.8
8	Medium	Local	4	4	3	3	0	0.8
9	Medium	Adjacent	4	4	2	2	0	0.8
10	Medium	Adjacent	4	4	3	3	0	0.8
11	Medium	Network	4	4	2	2	0	0.9
12	Medium	Network	4	4	3	3	0	0.9
13	High	Local	5	5	4	4	4	0.9
14	High	Local	5	5	5	5	3	0.9
15	High	Adjacent	5	5	4	4	0	0.9
16	High	Adjacent	5	5	5	5	0	0.9
17	High	Network	5	5	4	4	4	0.9
18	High	Network	5	5	5	5	5	1.2
19	High	Local	3	3	26	26	36	2.7
20	High	Local	4	4	26	26	74	3.0
21	High	Local	5	5	26	26	77	3.3

- With 182 assets
  - 4 to 5 seconds

Conclusions

- Attack paths discovery is essential part of risk management
- Supports the identification of security measures
  - Avoid security breaches similar to EQUIFAX security breach
  - 143 million customers affected
  - Apache Struts vulnerability CVE-2017-5638 allows remote attackers to execute arbitrary commands
- We currently work for better visualization of attack paths

MITIGATE

University of Brighton

Thank you for your attention!

- Questions?

- Contact details:
  - Nikolaos Polatidis n.polatidis@brighton.ac.uk
  - Michalis Pavlidis m.pavlidis@brighton.ac.uk