Panacea

People-centric cybersecurity in healthcare

Dynamic Risk Management Platform (DRMP)

Highlights and Demonstration

Silvia Bonomi
UROME

September 15th, 2020

Funded by the European Union’s Horizon 2020
Research and Innovation Programme, under Grant Agreement no 826293

DRMP in a nutshell

- DRMP aims to proactively protect a complex IT infrastructure by taking the following main steps
  - Risk Analysis
    - ▷ multi-dimensional model to support attack likelihood analysis
    - ▷ Business Dependency Analysis to support impact analysis
  - Response Analysis
    - ▷ Identification of technical and non-technical mitigation actions to reduce the risk level

Panacea

People-centric cybersecurity in healthcare

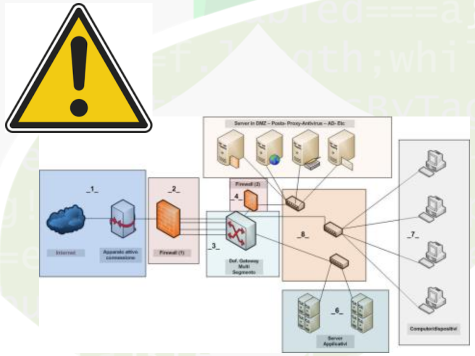
Context Overview

Health Care Organization (HCO)

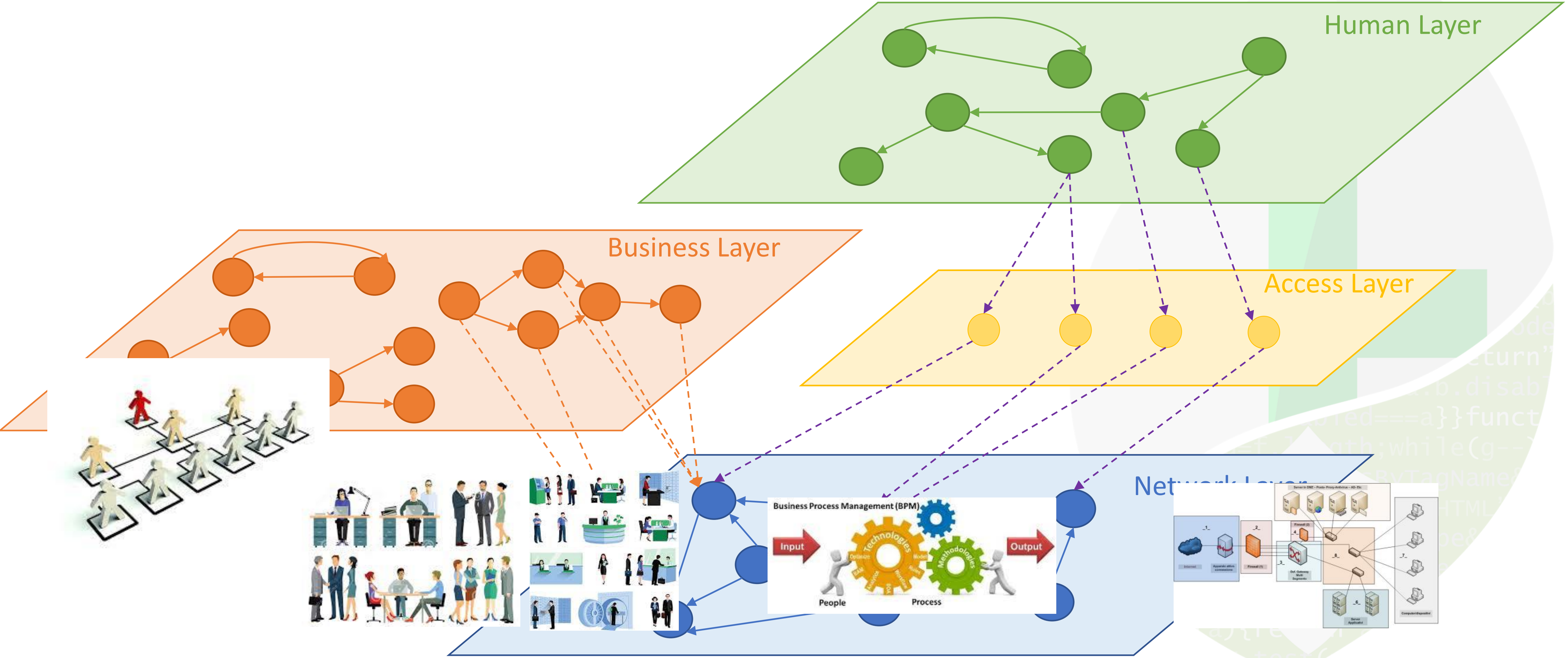
THREATS & VULNERABILITIES

- Bugs
- Errors
- Backdoors
- …

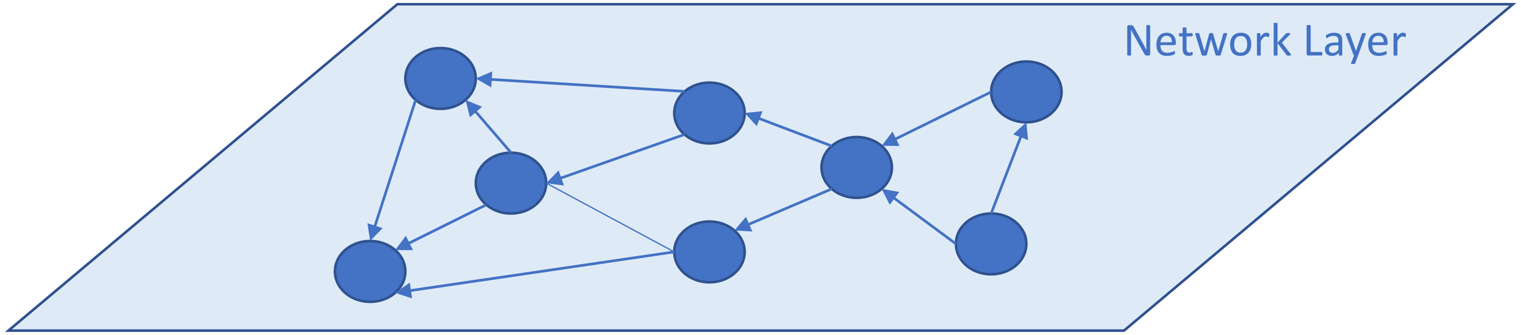
Business Process Management (BPM)
Input
Technologies
Methodologies
Output
People
Process

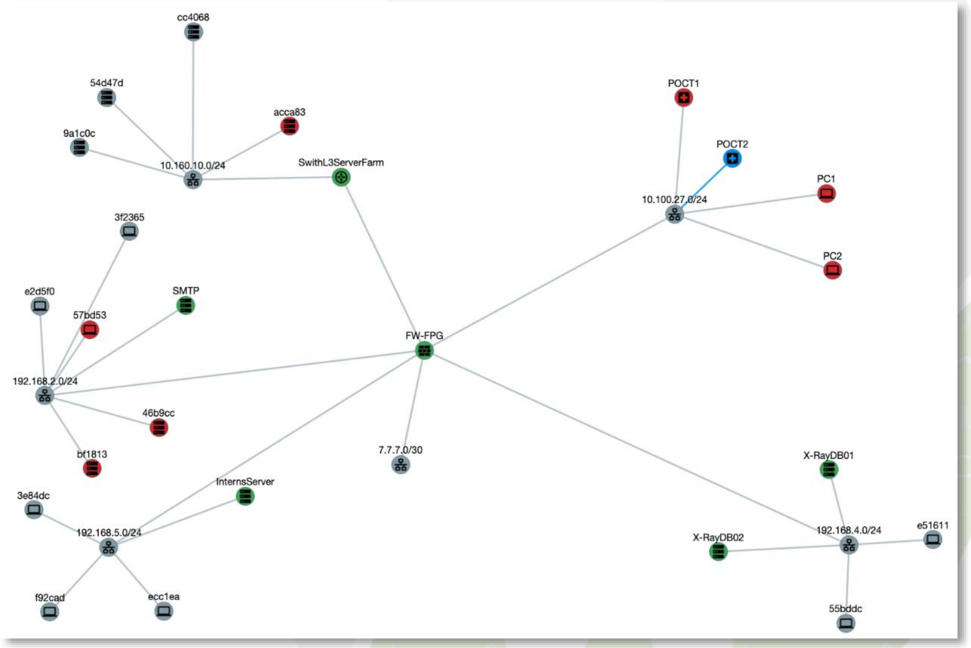


Our Model

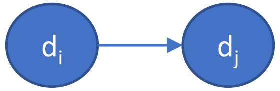

Human Layer
Business Layer
Access Layer
Network Layer
Business Process Management (BPM)
Input
Technologies
Methodologies
Output
People
Process

Modeling Network Layer



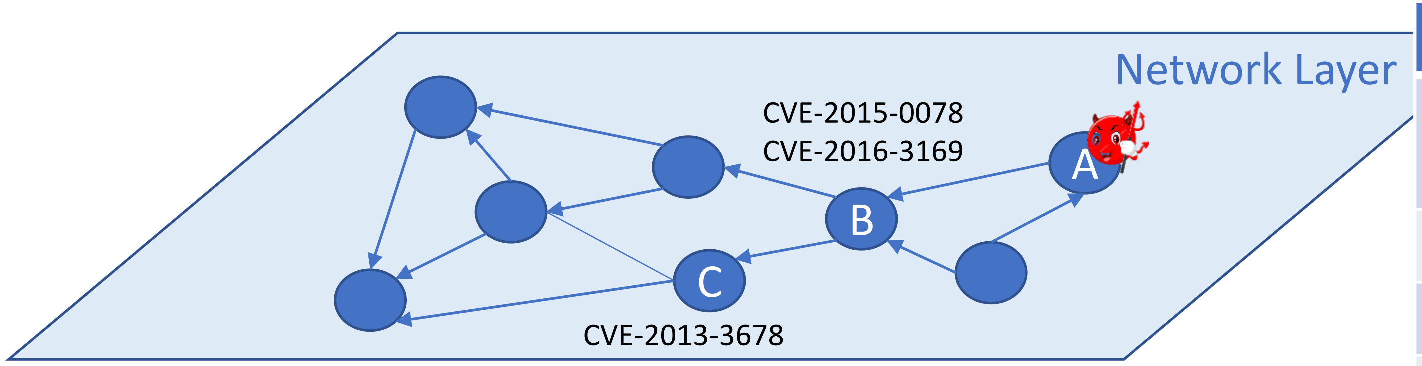


- Every Node d_i is a Device
  - Attached you can find
    - ▷ a list of its vulnerabilities (e.g., CVE-YYYY-NNNN)
    - ▷ Current level of privileges (e.g., None, User, Root)



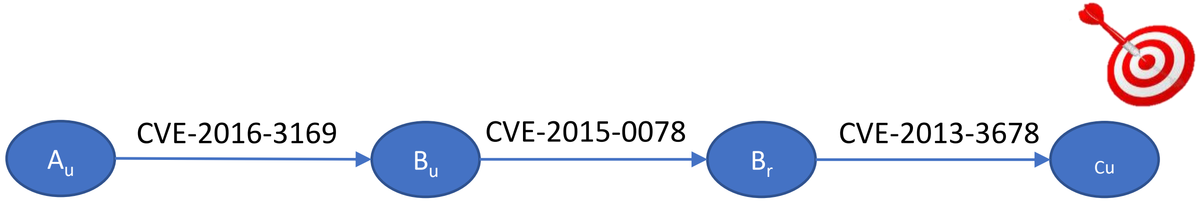
- Every Edge d_i, d_j represents the possibility to reach device d_j from d_i

Traversing the Asset Layer

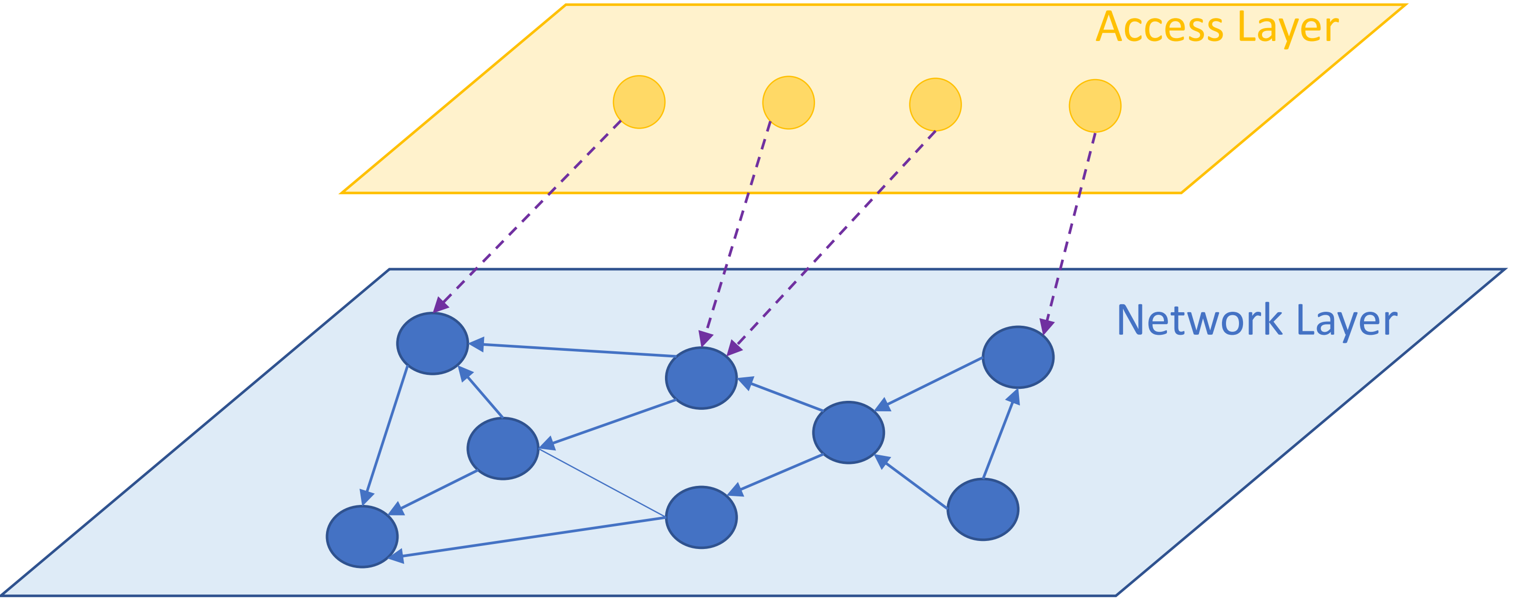


CVE-2013-3678	
Multiple unspecified vulnerabilities in SAP Governance, Risk, and Compliance (GRC) allow remote authenticated users to gain privileges and execute arbitrary programs via a crafted (1) RFC or (2) SOAP-RFC request.	
Base Score (CVSS v2)	9.0 HIGH
Access Vector (AV)	Network
Access Complexity (AC)	Low
Authentication (AU)	Single
Confidentiality (C)	Complete
Integrity (I)	Complete
Availability (A)	Complete
Additional Information:	Provides unauthorized access Allows unauthorized disclosure of information Allows disruption of service

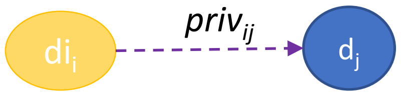
Allows disruption of service
Information:
Allows unauthorized disclosure of information
Allows disruption of service



Modeling access to Data, Devices and Applications

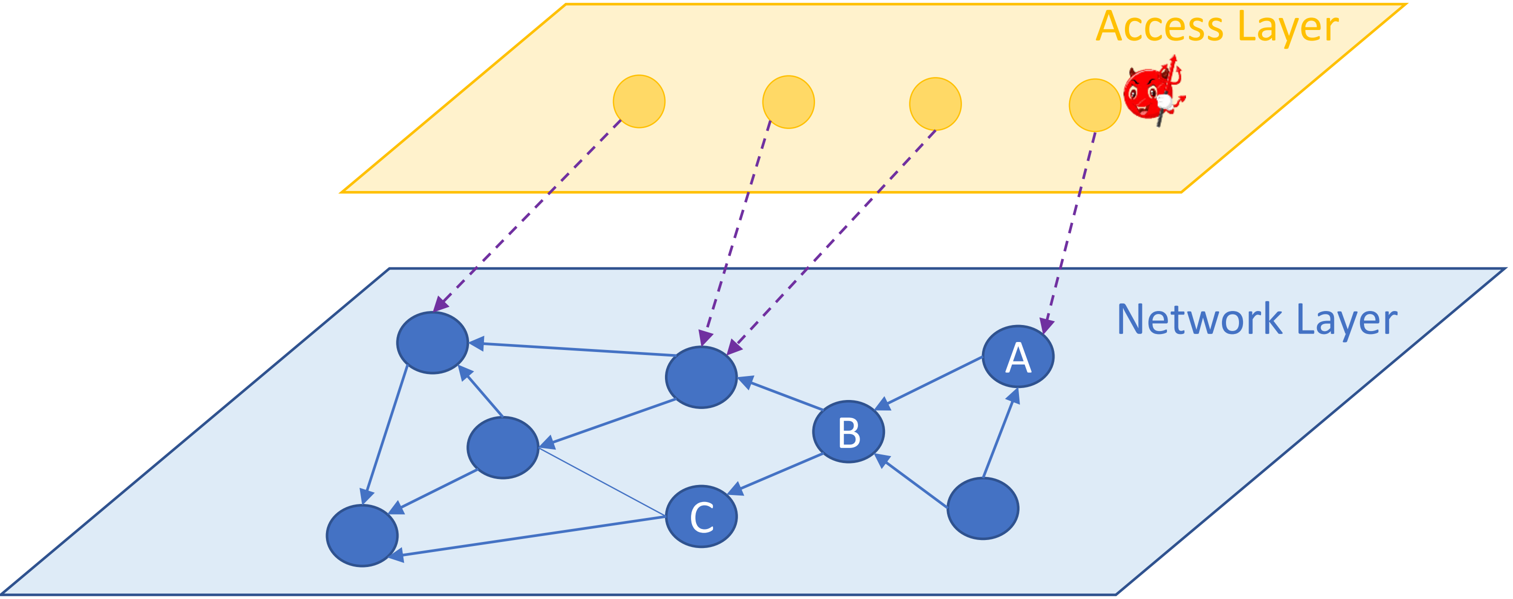


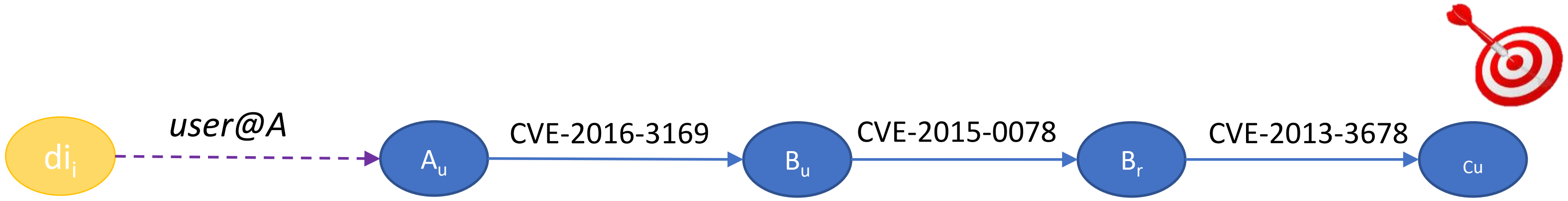
- Every Node di_i represent a digital identity/credential
  - It is characterized by the type of credential (e.g., username-password, token, biometric, etc.)



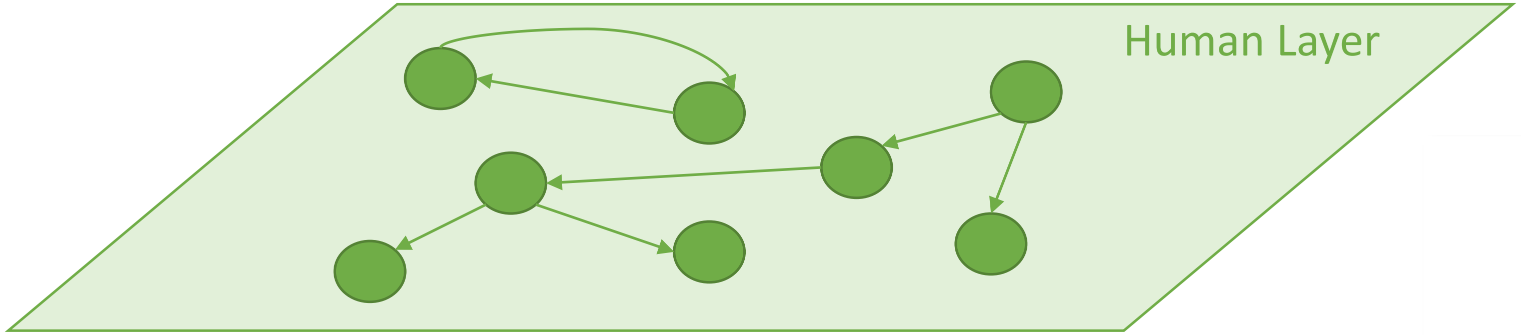
- Every Edge di_i, d_j represents the possibility to access device (or a specific application running on the device) d_j using credential di_i with privileges $priv_{ij}$

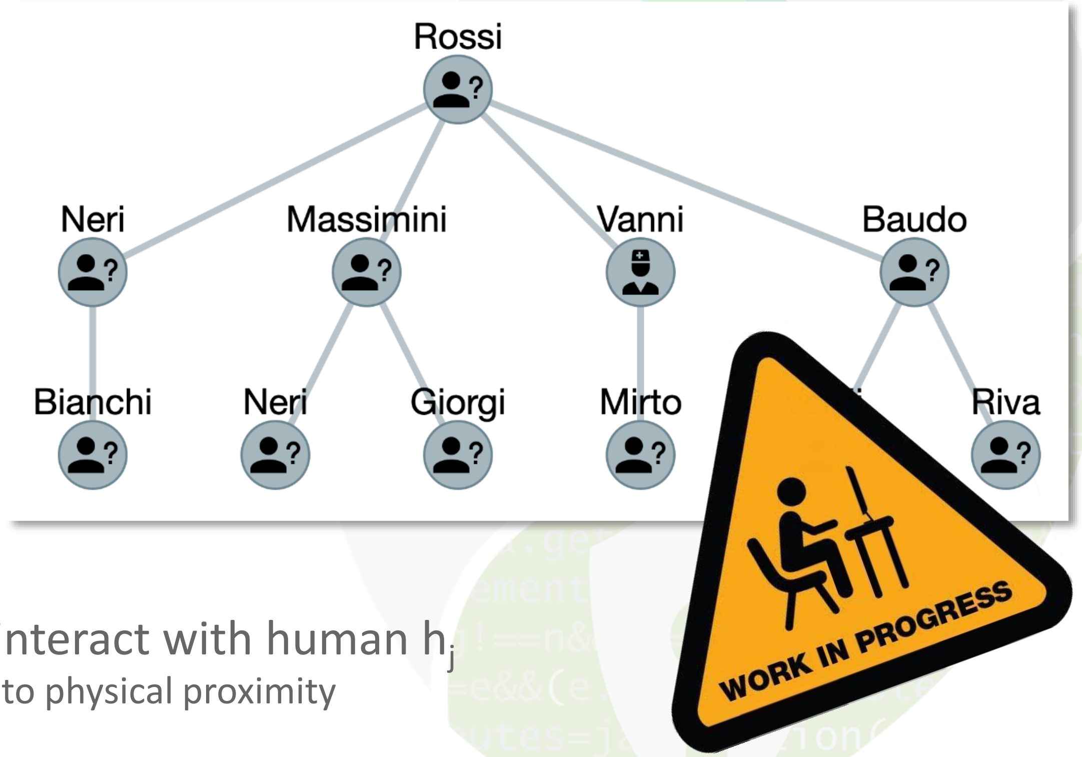
Traversing Access and Network Layers



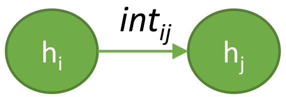


Modeling Human Layer





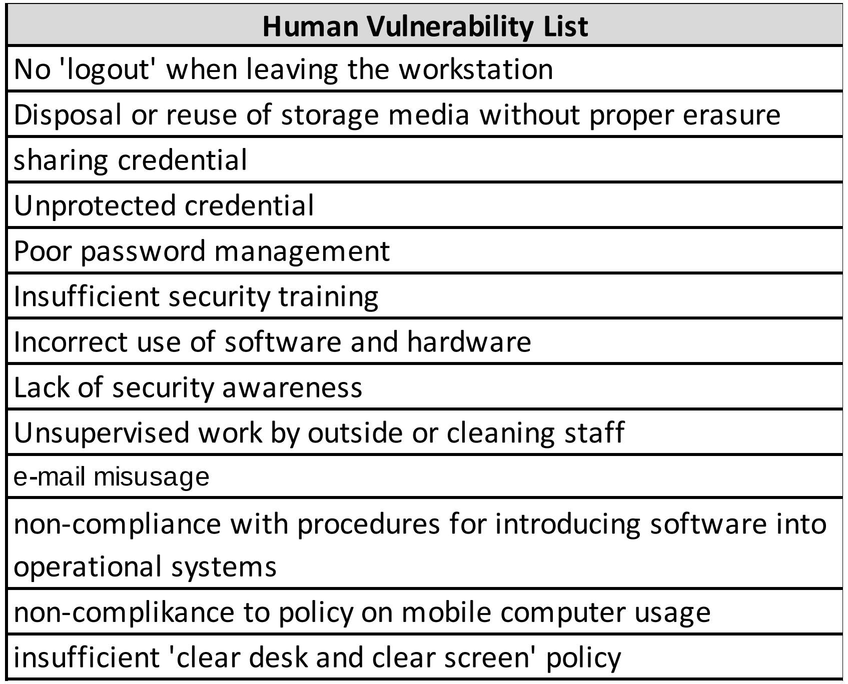
- Every Node h_i is a human
  - Attached you can find
    - a list of its vulnerabilities
    - a security profile



- Every Edge h_i, h_j represents the possibility to let h_i interact with human h_j
  1. Interaction is possible due to working collaborations or to physical proximity
  2. Interaction is characterized by an intensity int_{ij}

Human Vulnerabilities

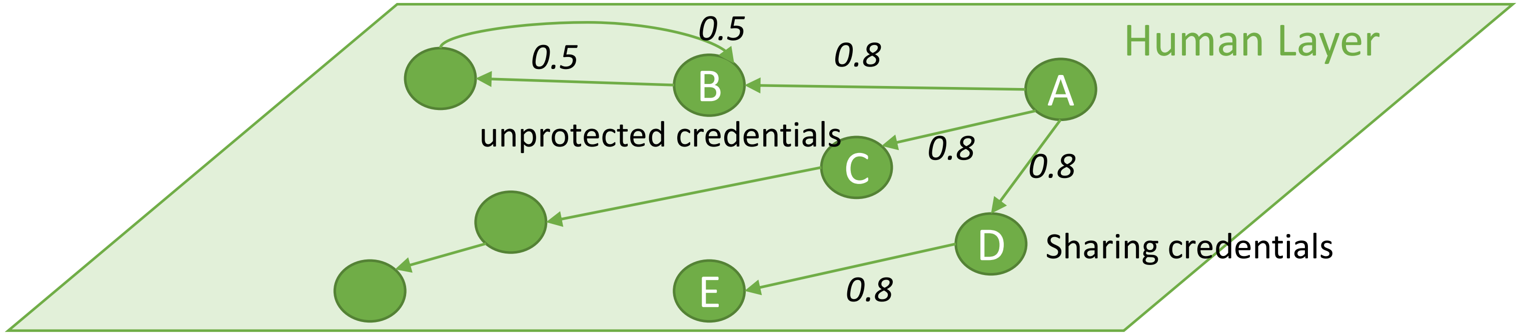
- We identified a preliminary catalogue of human vulnerabilities and metrics to define security profiles

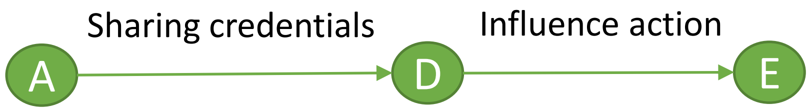


Human Vulnerability List
No 'logout' when leaving the workstation
Disposal or reuse of storage media without proper erasure
sharing credential
Unprotected credential
Poor password management
Insufficient security training
Incorrect use of software and hardware
Lack of security awareness
Unsupervised work by outside or cleaning staff
e-mail misusage
non-compliance with procedures for introducing software into operational systems
non-complikance to policy on mobile computer usage
insufficient 'clear desk and clear screen' policy

Security Profile	Quanlitative scale ?	Quantitative Scale?
Individual Security attitude	Low, medium, High	e.g., in [0, 1]
Security behavior	Low, Medium, High	e.g., in [0, 1]
Security culture at work	Low, Medium, High	e.g., in [0, 1]
Security training	Low, Medium, High	e.g., in [0, 1]
Trust in colleagues	Low, Medium, High	e.g., in [0, 1]
Trust in physical security of the building	Low, Medium, High	e.g., in [0, 1]

Traversing Human Layer

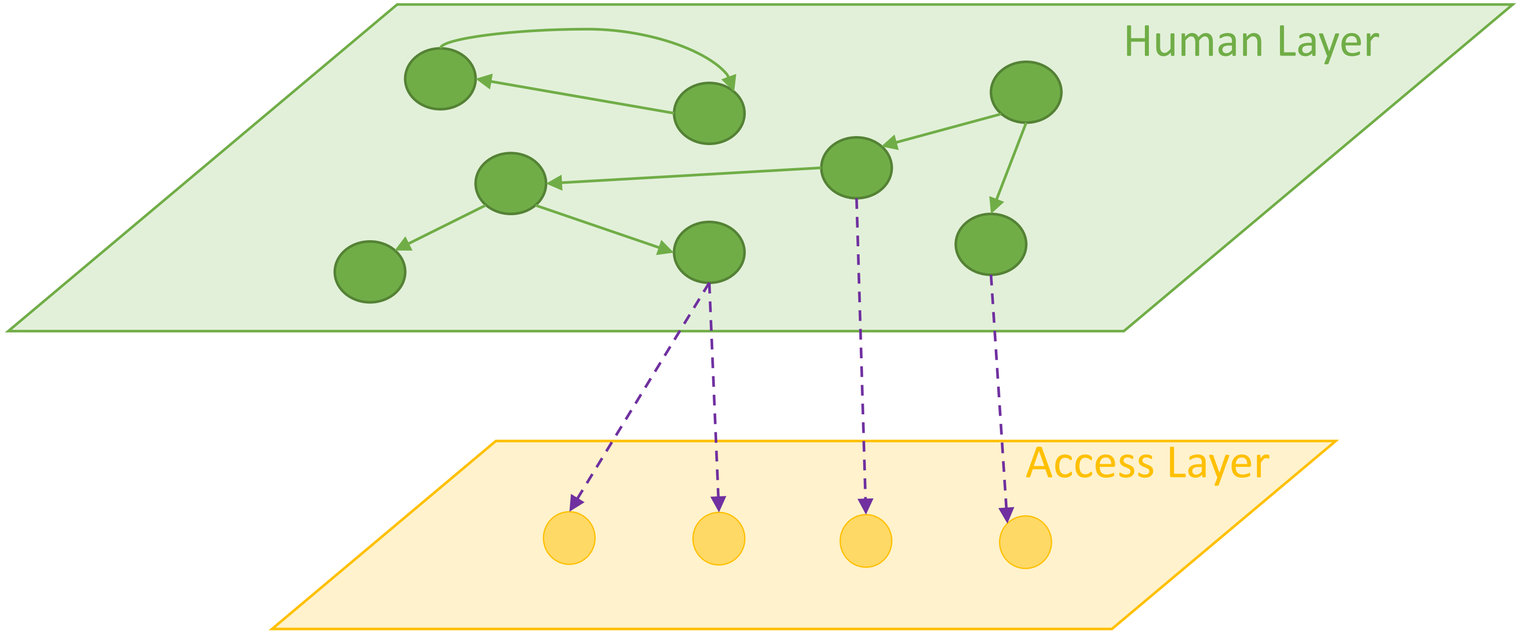


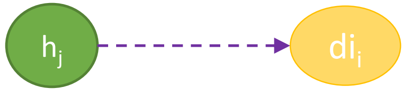


The effect of the exploit is that the attacker can impersonate D

The effect of the exploit is that the attacker can influence E in sharing information or accessing services

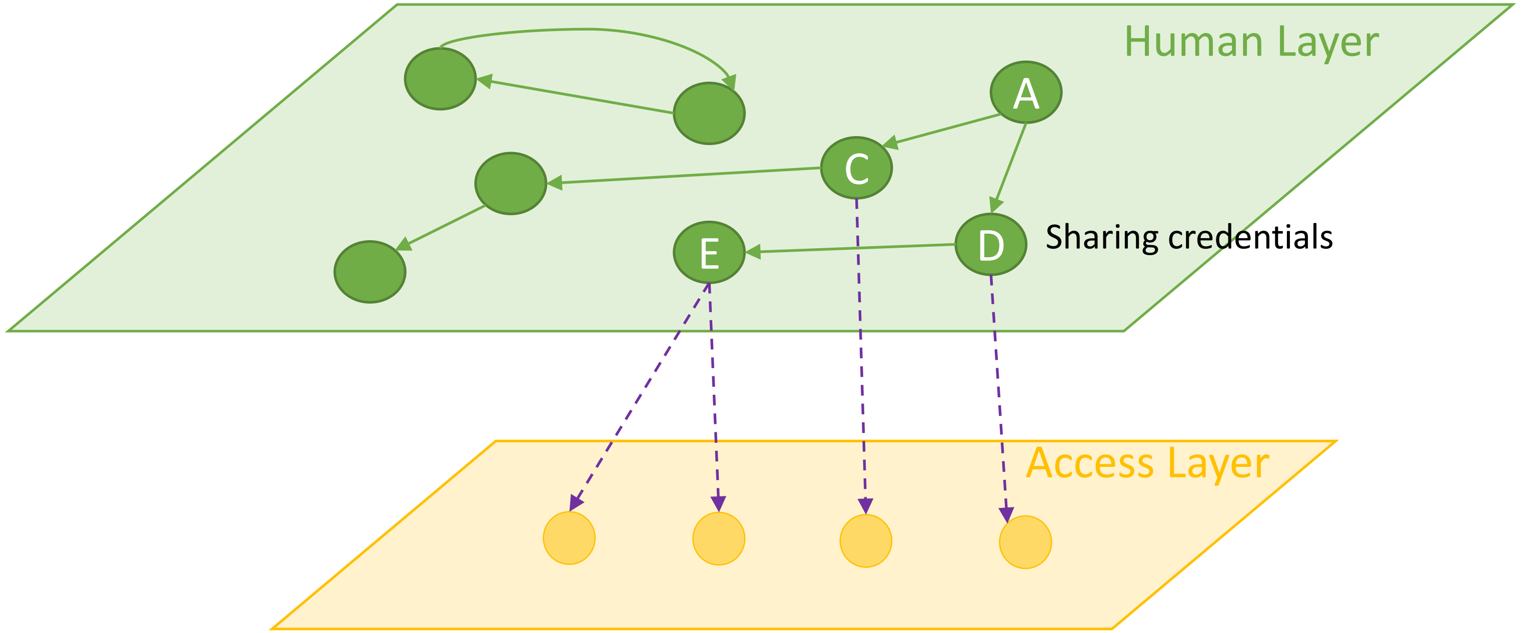
Modeling credential ownership

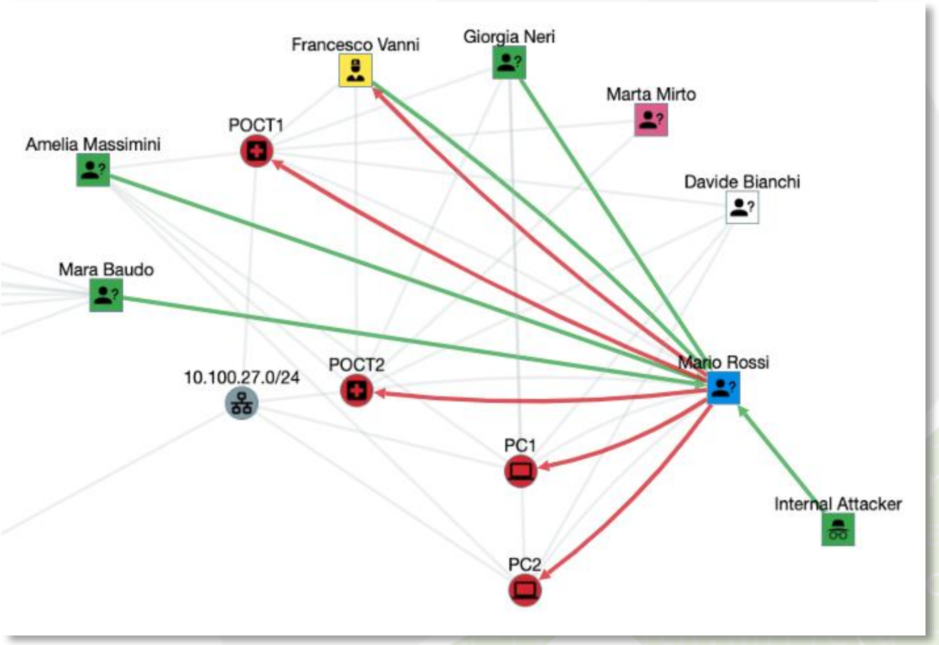


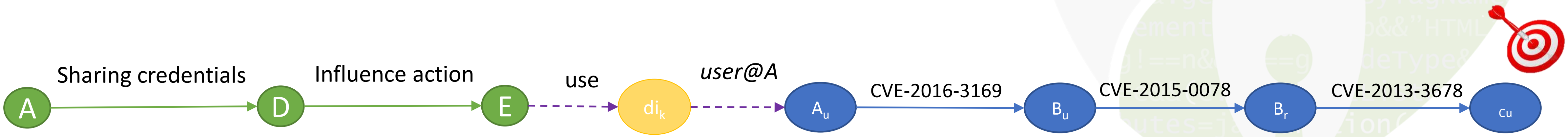


- Every Edge h_j, di_i represents the possibility for h_j to use credential di_i

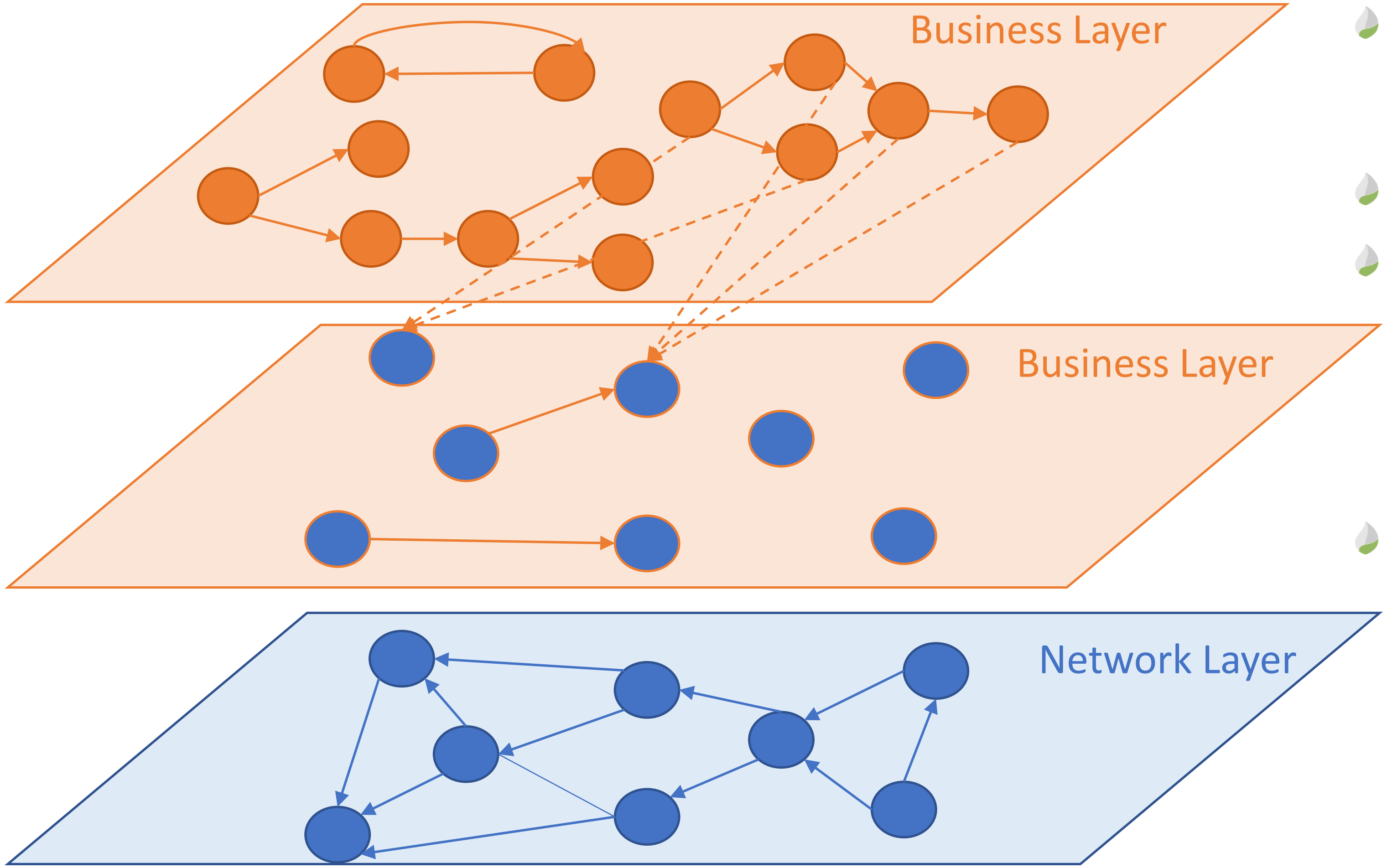
Traversing Human and Access Layer







Modeling Business Layer



- The Business Layer is aiming at representing the dependencies between basic services and between services and their supporting assets
- We use a graph-based representation where
- Nodes are
  - Basic services ●
    - e.g., access patient data
  - Components ●
    - e.g., medical device, database
- Edges represent a functional dependency between
  - Two business services ● → ●
  - A business service and its supporting component ● - - → ●
  ● → ●

Service level

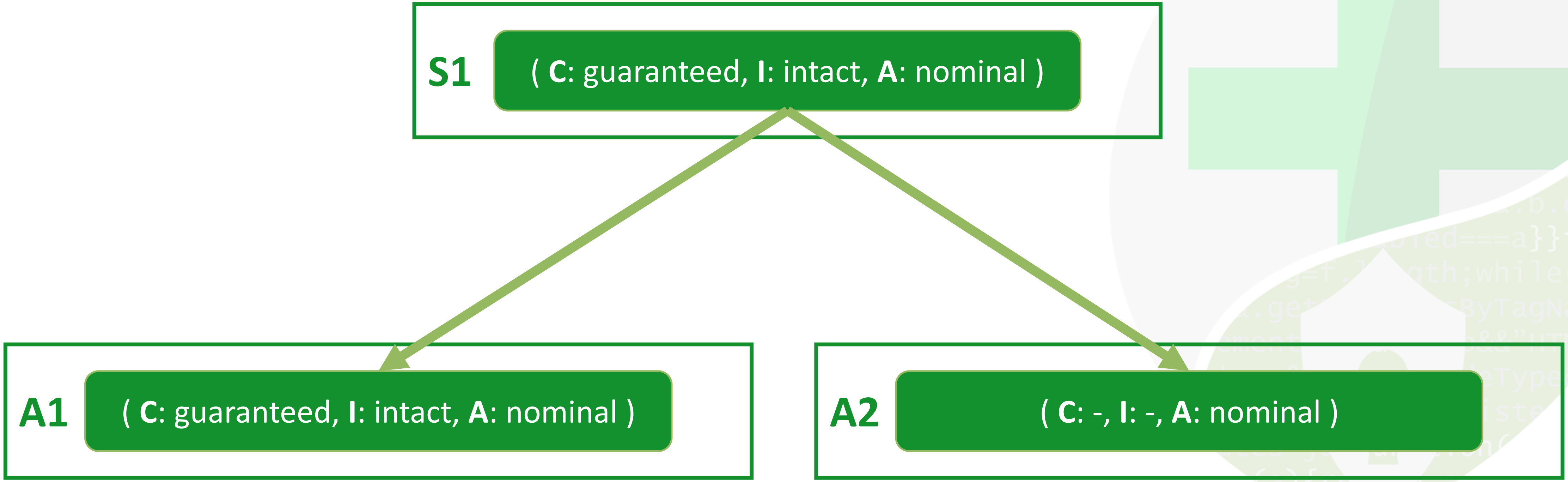
- Each service can provide its function at different service levels depending on the state of the system

Confidentiality	guaranteed, violated
Integrity	intact, corrupted
Availability	nominal, degraded, disrupted

- e.g., (**C**: guaranteed, **I**: corrupted, **A**: degraded)

Dependencies

- Guaranteeing a given service level on a given element may require a minimum service level on other elements



S1

(**C**: guaranteed, **I**: intact, **A**: nominal)

A1

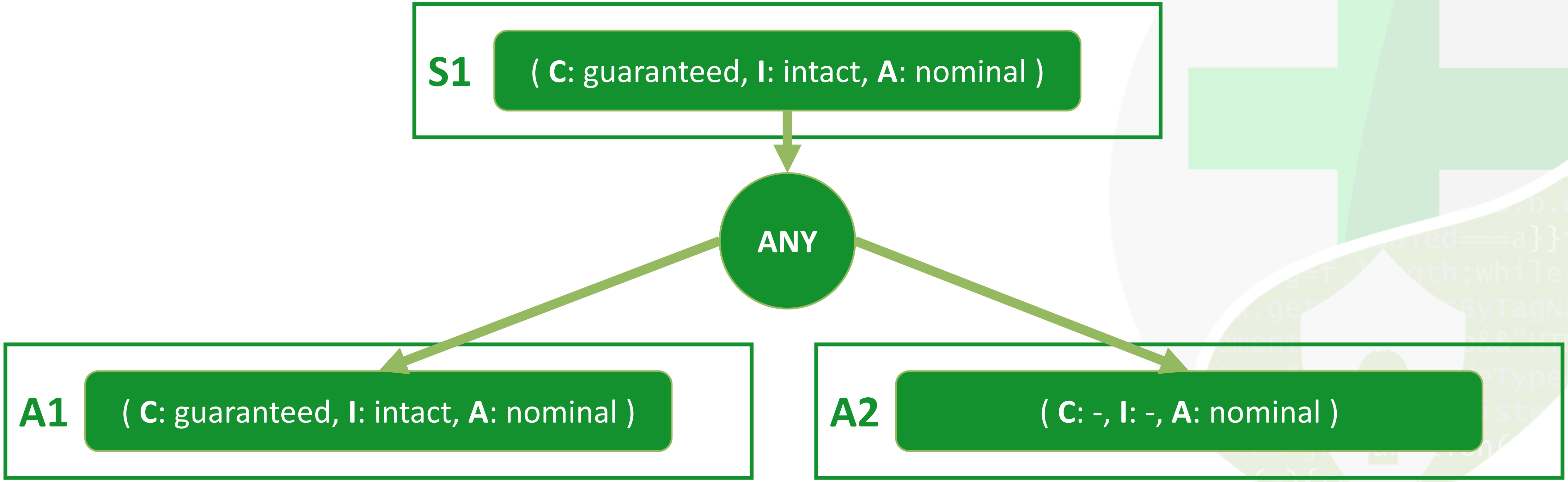
(**C**: guaranteed, **I**: intact, **A**: nominal)

A2

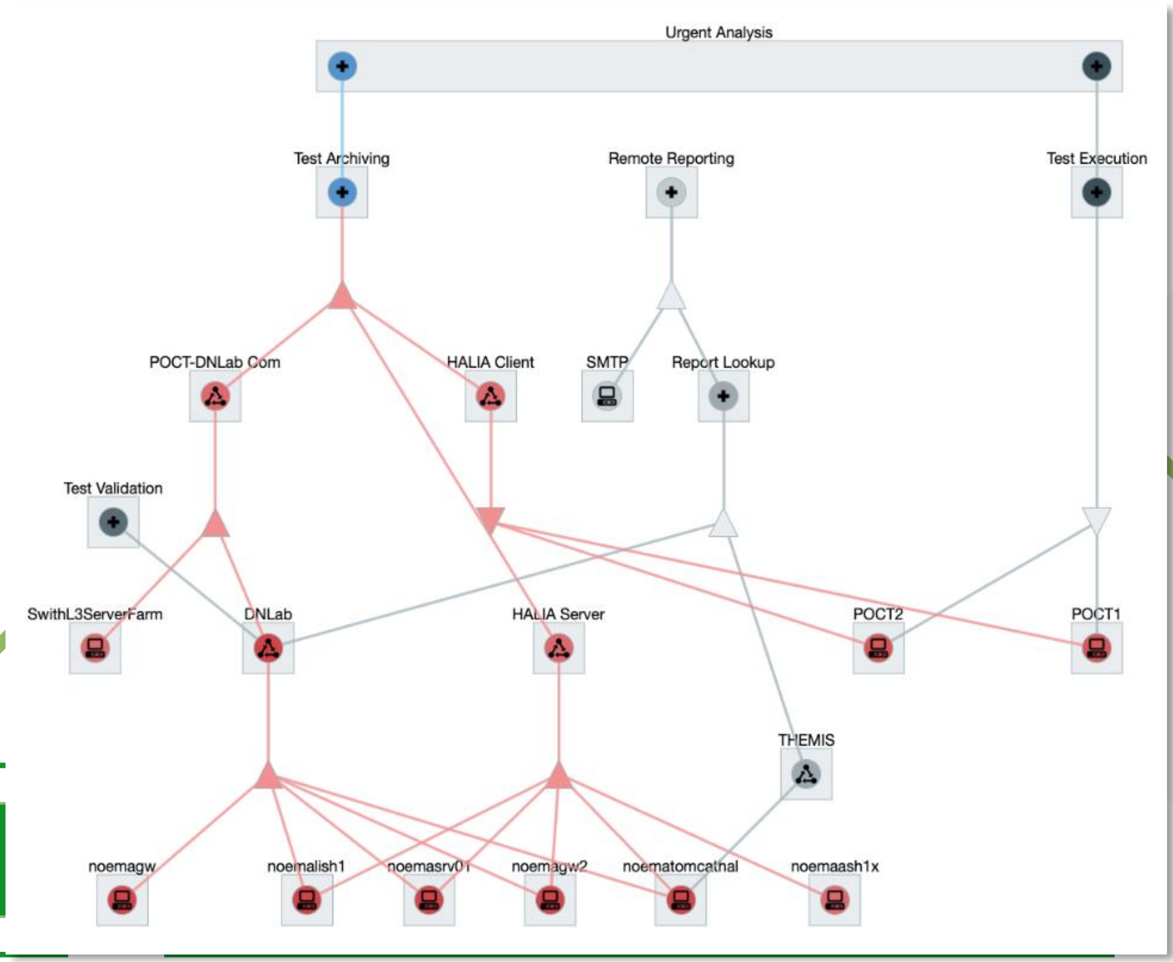
(**C**: -, **I**: -, **A**: nominal)

Dependencies

- Normally, dependencies must ALL be fulfilled while other configurations can be expressed with the ANY operator


S1
(**C**: guaranteed, **I**: intact, **A**: nominal)
ANY
A1
(**C**: guaranteed, **I**: intact, **A**: nominal)
A2
(**C**: -, **I**: -, **A**: nominal)

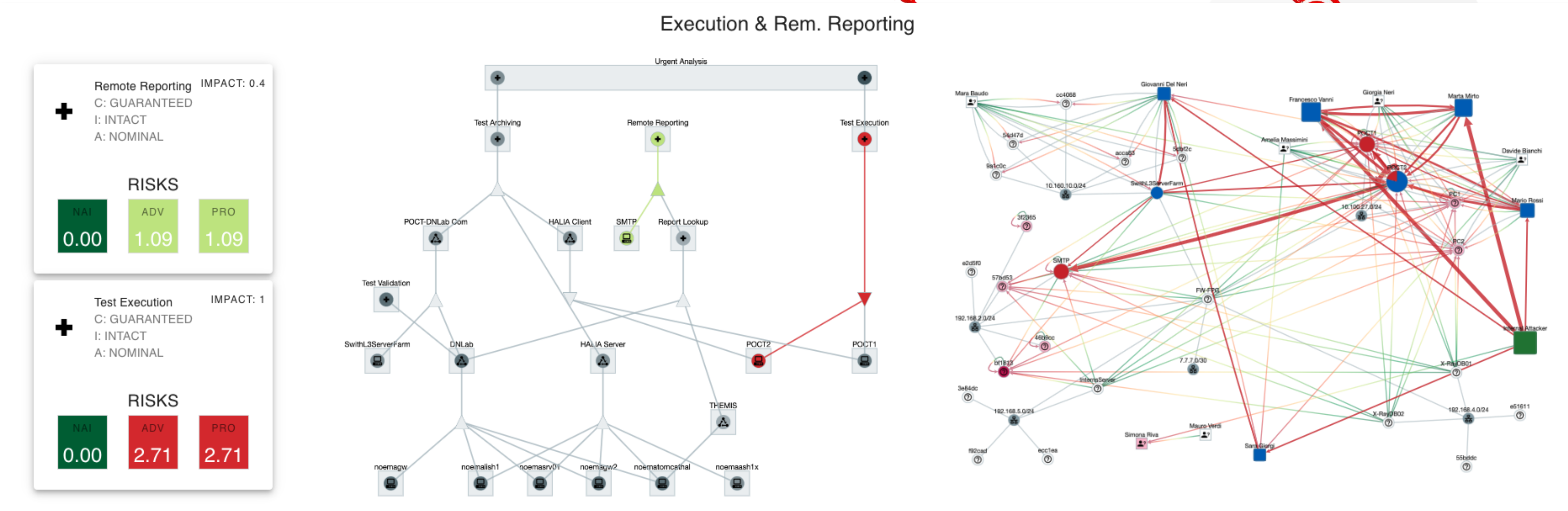
Dependency Graph Example



A1 **(C: 0, I: 0, A: 1)**

A3 **(C: 0, I: 0, A: 1)**

From Graphs to Risk



Execution & Rem. Reporting

Remote Reporting IMPACT: 0.4
C: GUARANTEED
I: INTACT
A: NOMINAL

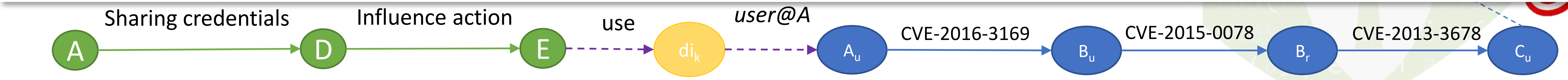
RISKS

NAI	ADV	PRO
0.00	1.09	1.09

Test Execution IMPACT: 1
C: GUARANTEED
I: INTACT
A: NOMINAL

RISKS

NAI	ADV	PRO
0.00	2.71	2.71



Risk Computation

- DRMP can support the evaluation of the following risks
  - Full compromising of a business process BP_i
  - Compromising of a specific service level for a given BP_i
  - Compromising of an asset

Thank you!

Questions?!