Norwegian Centre for Research-based Innovation

NORCICS

SFI Norwegian Centre for Cybersecurity in Critical Sectors

Addressing challenges for vulnerability management in the energy sector

Does it matter for you?

- How would you feel if energy goes down while cooking or, much worse, for a beloved one whose life depends on electric equipment?

Suppliers' challenges

- NIS 2 directive Article 21 – "vulnerability handling and disclosure"
- ENISA – national vulnerability programmes
- Feasibility given availability requirements
- Multi-criteria decision-making process

Research Design

Information Gathering Analysis	Market solutions	Research Interviews
Professional experience + IEC 62443-2-3	Criteria from larger market share	12 asset owners / semi-structured

Main results

- **Prioritization:** asset criticality, combination of risk score with other information, risk of not implementing

How would you prioritize a critical asset when performing vulnerability management?

- **Deployment:** allowed downtime, architecture topology, applicability
- Internal decision-making process diagram for vulnerability management
- Identification of main challenge

Reach out for more details!
jessica.b.heluany@ntnu.no

Expectation x reality

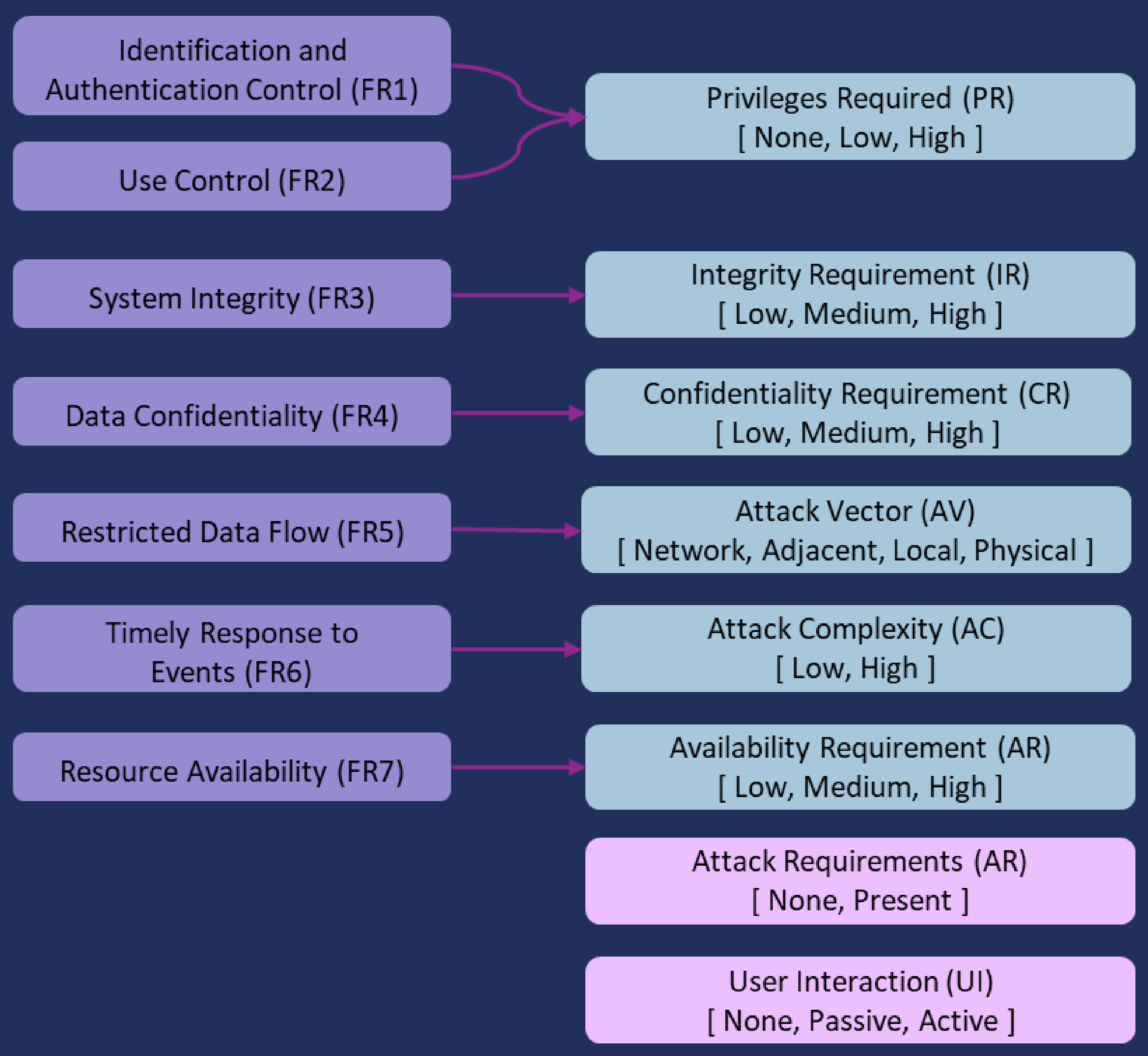
- Plan: criteria for prioritization and deployment to develop a decision-making algorithm
- Execution: main challenge identified was how to consider existing security measures

Current practices

IEC CVSS NOZOMI NETWORKS CLAROTY DRAGOS NIST CISA KEV EPSS Exploit Prediction Scoring System tenable network security

IEC 62443-3-3 & CVSS

Solution suggestion to consider existing security measures: mapping between the security systems requirements of IEC 62443-3-3 (Security for industrial automation and control systems, Part 3-3: System security requirements and security levels) to the Environmental metrics of the Common Vulnerability Scoring System (CVSS).


Identification and Authentication Control (FR1)
Use Control (FR2)
Privileges Required (PR) [None, Low, High]
System Integrity (FR3)
Integrity Requirement (IR) [Low, Medium, High]
Data Confidentiality (FR4)
Confidentiality Requirement (CR) [Low, Medium, High]
Restricted Data Flow (FR5)
Attack Vector (AV) [Network, Adjacent, Local, Physical]
Timely Response to Events (FR6)
Attack Complexity (AC) [Low, High]
Resource Availability (FR7)
Availability Requirement (AR) [Low, Medium, High]
Attack Requirements (AR) [None, Present]
User Interaction (UI) [None, Passive, Active]