5G-FORAN

DFIR IN OPEN RAN

Präsentation im Kolloquium

Implementierung eines Dashboards für Pentesting
in einer Digital Forensics and Incident Response (DFIR) Umgebung in Open RAN

24.01.2025

Jurek Jesse, Bachelor Technische Informatik

5G-FORAN
DFIR IN OPEN RAN

Technology
Arts Sciences
TH Köln

Inhalt

- Allgemein
  - Vision
  - Architektur
- Implementierungen
  - Angriffspfad, Matrix-Rework,
  - ACEMA O-RAN (Klement et al.)
- Ergebnisse

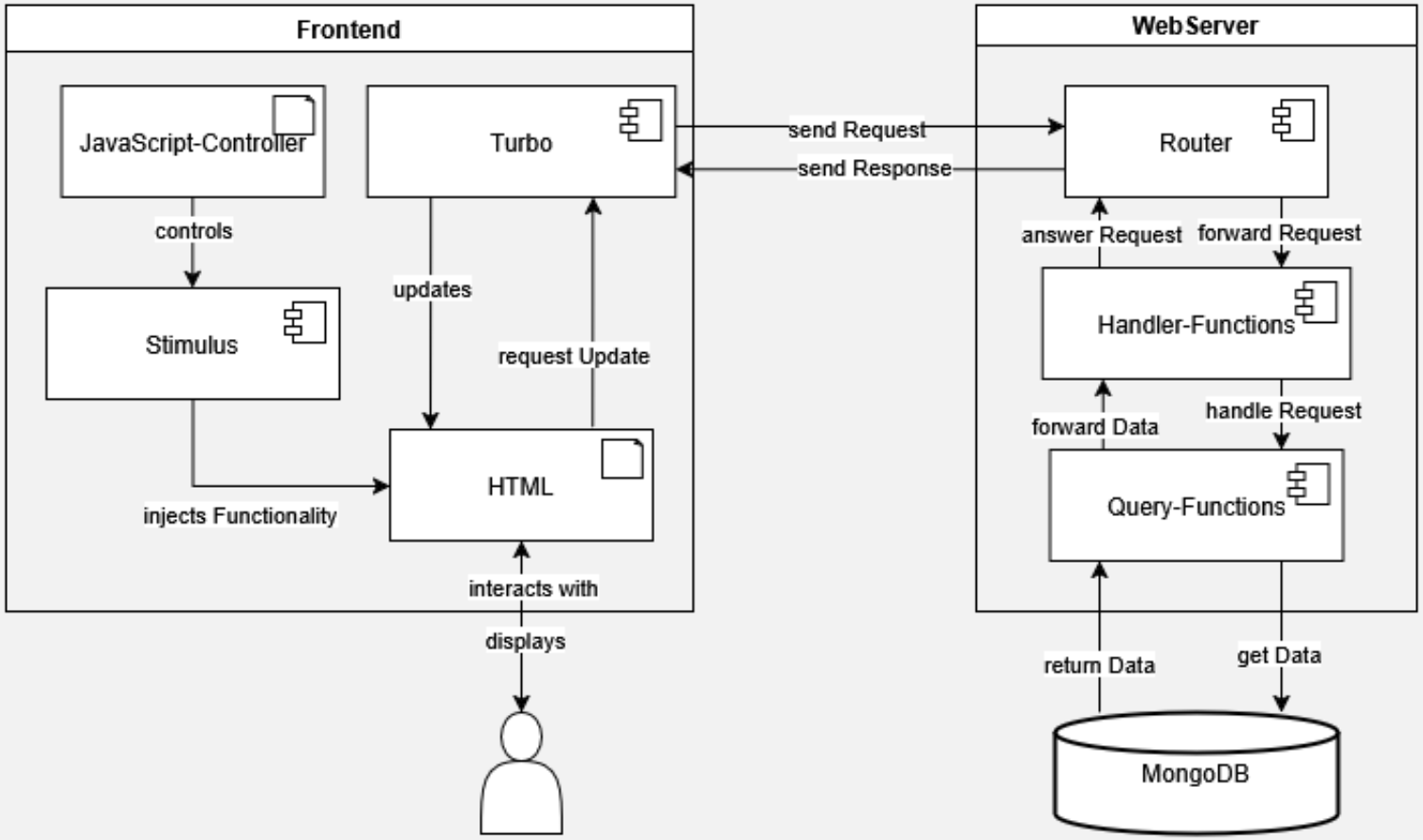
5G-FORAN
DFIR IN OPEN RAN
Technology
Arts Sciences
TH Köln

Vision

„ Es existiert ein Dashboard zur aussagekräftigen Visualisierung aller Angriffe des Attacktools. Die Daten aus dem AT werden mit CVSS-Werten anreichert und es lassen sich Relationen zu anderen Klassifikationssystemen, insbesondere dem ORAN Threat-Model[1] herstellen. “

[1] “O-RAN Security Threat Modeling and Risk Assessment 4.0.” Oktober 2024. Available: https://specifications.o-ran.org/download?id=774

Architektur



5G-FORAN
DFIR IN OPEN RAN

Technology
Arts Sciences
TH Köln

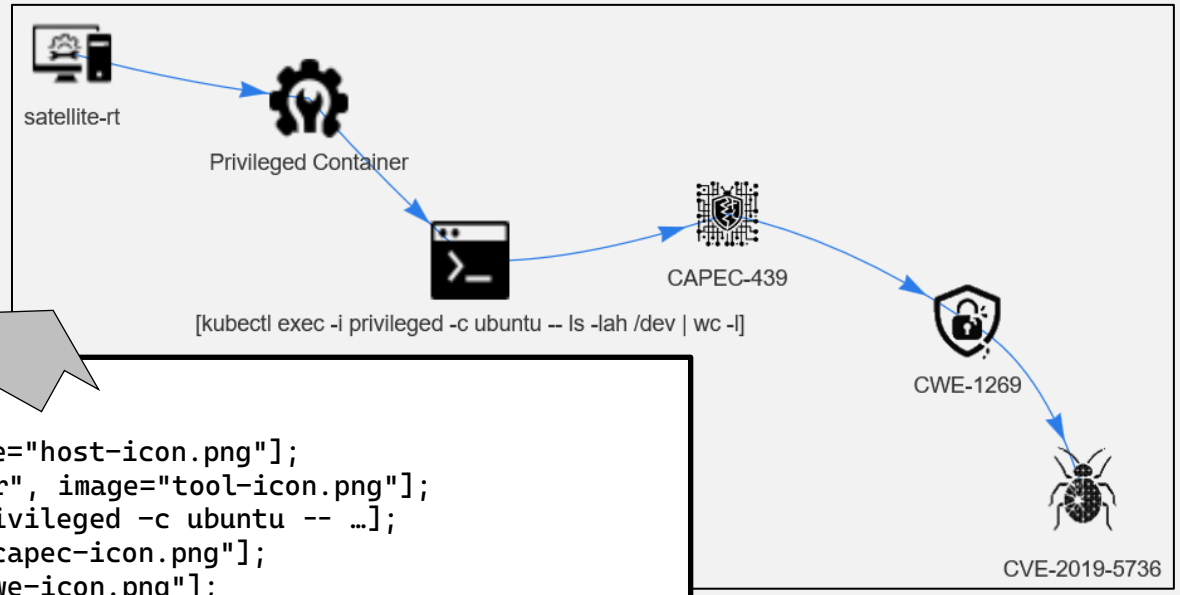
Visualisierung des Angriffspfads

Mithilfe von

- DOT
- Vis.js

```
{
  "hostname": "satellite-rt",
  "ip": "192.168.40.22",
  "tool_name": "Privileged Container",
  "command": [
    "kubectl exec -i privileged -c ubuntu -- …"
  ],
  "mitre": {
    "TA0004": [
      "MS-TA9018"
    ]
  },
    "cve": [
      "CVE-2019-5736"
  ]
}
```

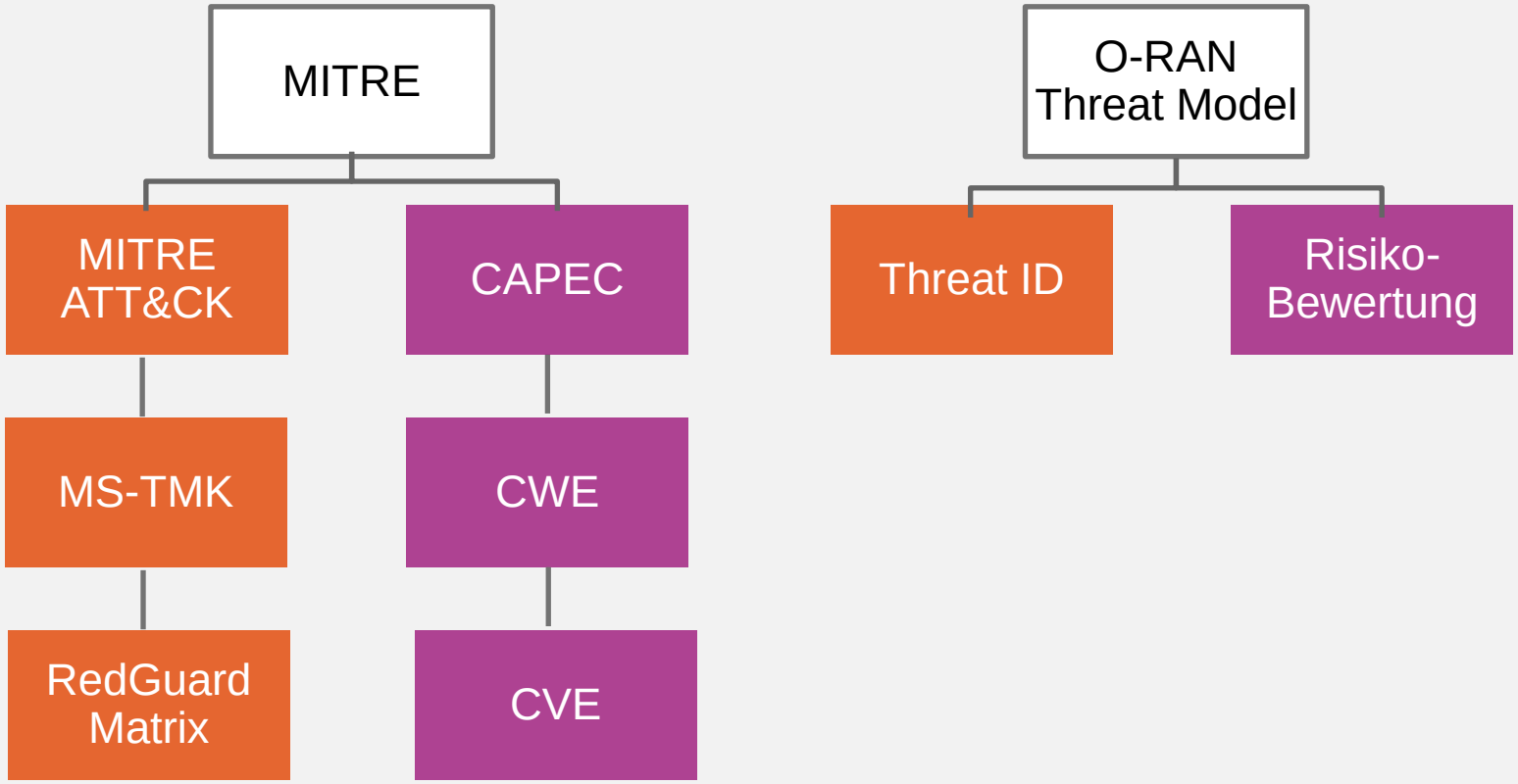
```
digraph attack {
      node [shape=square];
      n1 [label="satellite-rt", image="host-icon.png"];
      n2 [label="Privileged Container", image="tool-icon.png"];
      n3 [label="[kubectl exec -i privileged -c ubuntu -- …];
      n4 [label="CAPEC-439", image="capec-icon.png"];
      n5 [label="CWE-1269", image="cwe-icon.png"];
      n6 [label="CVE-2019-5736\n", image="cve-icon.png"];
      n1 -> n2 -> n3 -> n4 -> n5 -> n6;
}
```



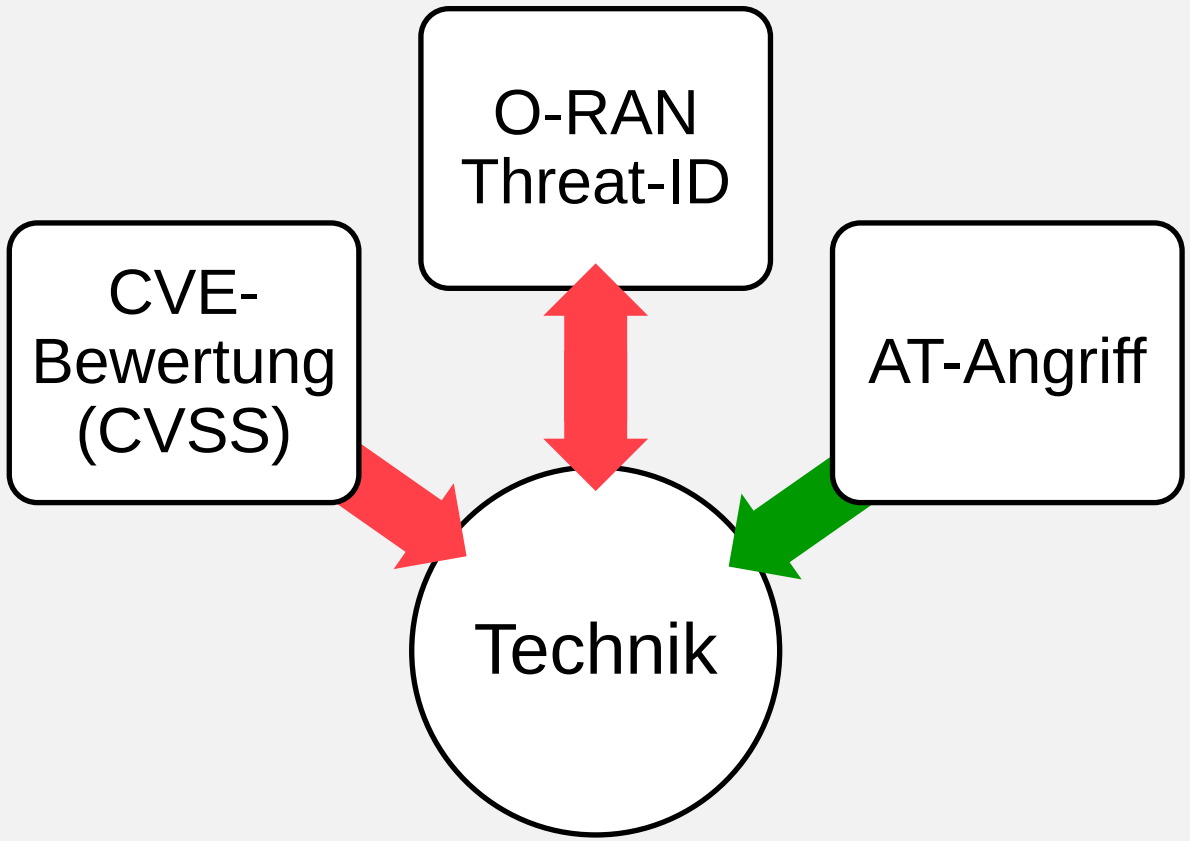
Rework der Matrix

Kategorisierung

Klassifizierung



Verknüpfung der Systeme



MS-TA9002
Compromised image In registry

T1525,T1195.002
Implant Internal Image with malicious code

T-IMG-01
VM/Container images tampering

MS-TA9040
Denial of Service

T1498,T1499
Endpoint/Network Denial of Service

T-ADMIN-01
Denial of service against NFO/FOCOM

5G-FORAN
DFIR IN OPEN RAN

Technology
Arts Sciences
TH Köln

ACEMA O-RAN

A Comprehensive Empirical Method to Analyze Threats in O-RAN Environments

- Felix Klement
  - E-Mail: felix.klement@uni-passau.de

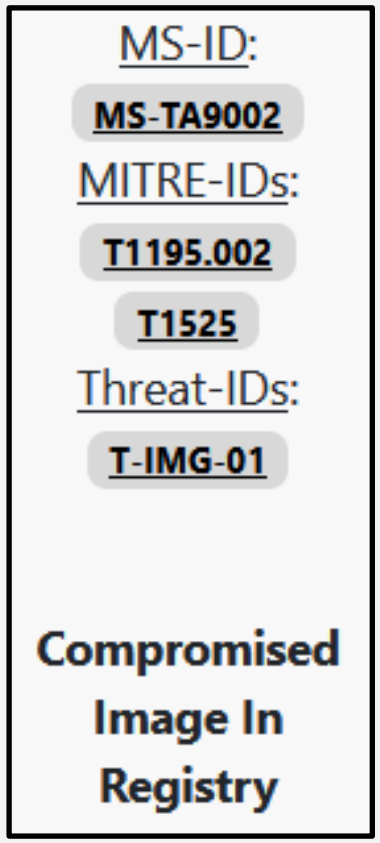
F. Klement, W. Liu, and S. Katzenbeisser, “Toward Securing the 6G Transition: A Comprehensive Empirical Method to Analyze Threats in O-RAN Environments Available: https://ieeexplore.ieee.org/document/10339923/

ACEMA O-RAN: Input

Mapping von MITRE-Technik zu O-RAN-Threat-ID

- Basis: MS-*Threat Matrix for Kubernetes*
- 66 Mappings

```
ThreatID;  Name;                          MITREID;  Tactic
T-IMG-01;  Compromised Image In Registry;T1195.002;initial-access
T-IMG-01;  Compromised Image In Registry;T1525;    initial-access
T-ADMIN-01;Denial of service;             T1498;    impact
T-ADMIN-01;Denial of service;             T1499;    impact
...
```



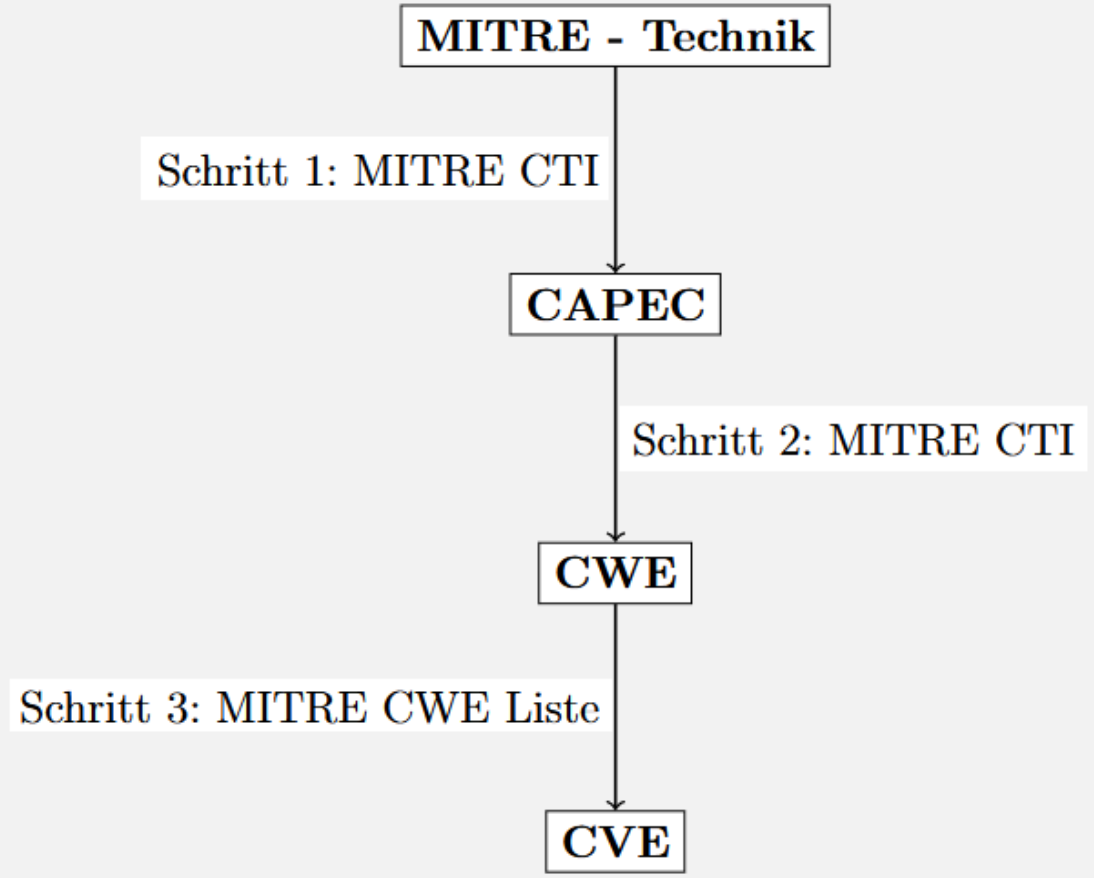
5G-FORAN
DFIR IN OPEN RAN

Technology Arts Sciences TH Köln

ACEMA O-RAN: Gathering

Mapping von MITRE-Technik zu CVE

- Schritt 1 & 2
  - mitreattack.attackToExcel.stixToDf .techniquesToDf(data, "enterprise-attack")
- Schritt 3
  - cwe2.Database().get(…)
- Weitere Infos über CVEs
  - nvdlib.searchCVE(…)

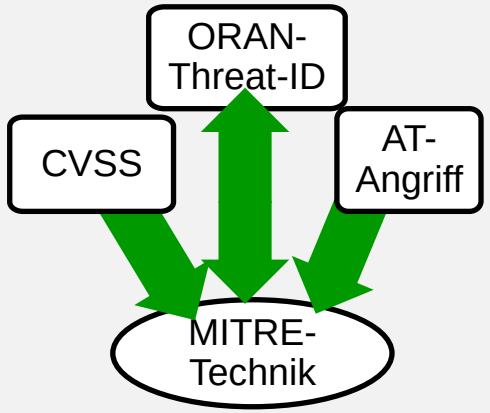


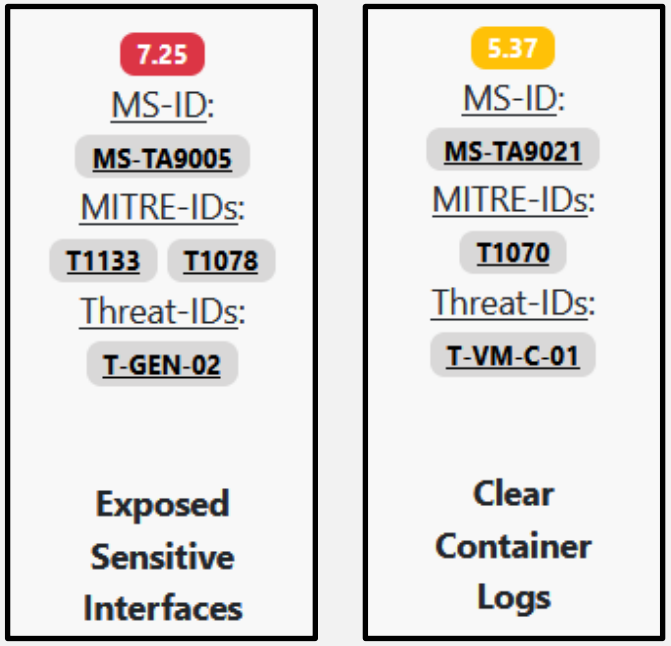
5G-FORAN
DFIR IN OPEN RAN

Technology
Arts Sciences
TH Köln

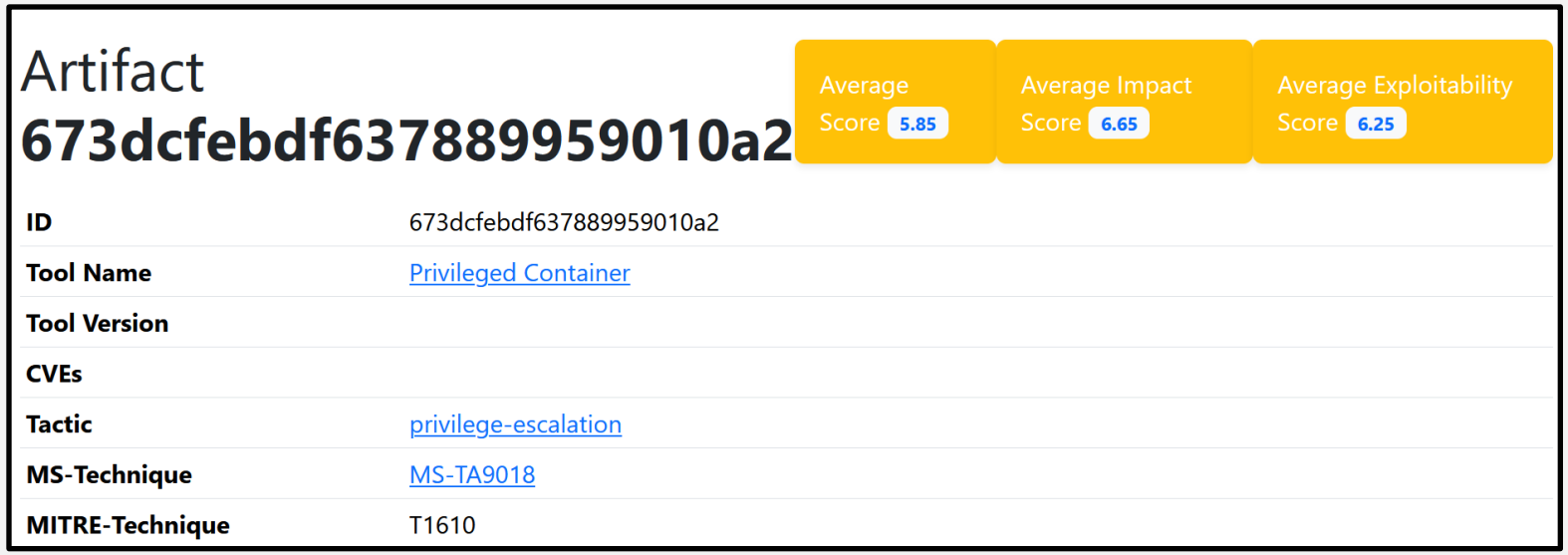
ACEMA O-RAN: Analysis

Anwendung im Dashboard





Anwendung in der Matrix



Anwendung in der Detailansicht eines Artefakts

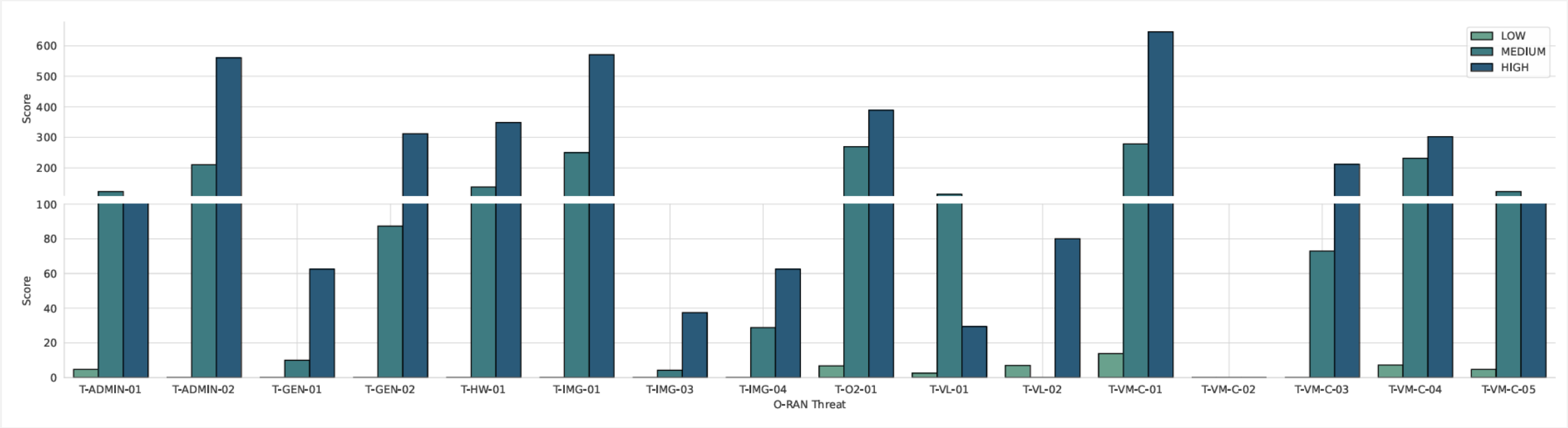
5G-FORAN
DFIR IN OPEN RAN

Technology
Arts Sciences
TH Köln

ACEMA O-RAN: Analysis

Wissenschaftliche Erkenntnisse #1

O-RAN Threats, denen CVEs mit hohem CVSS zugeordnet werden



ACEMA O-RAN: Analysis

Wissenschaftliche Erkenntnisse #2

Analyse der CVSS Vektoren

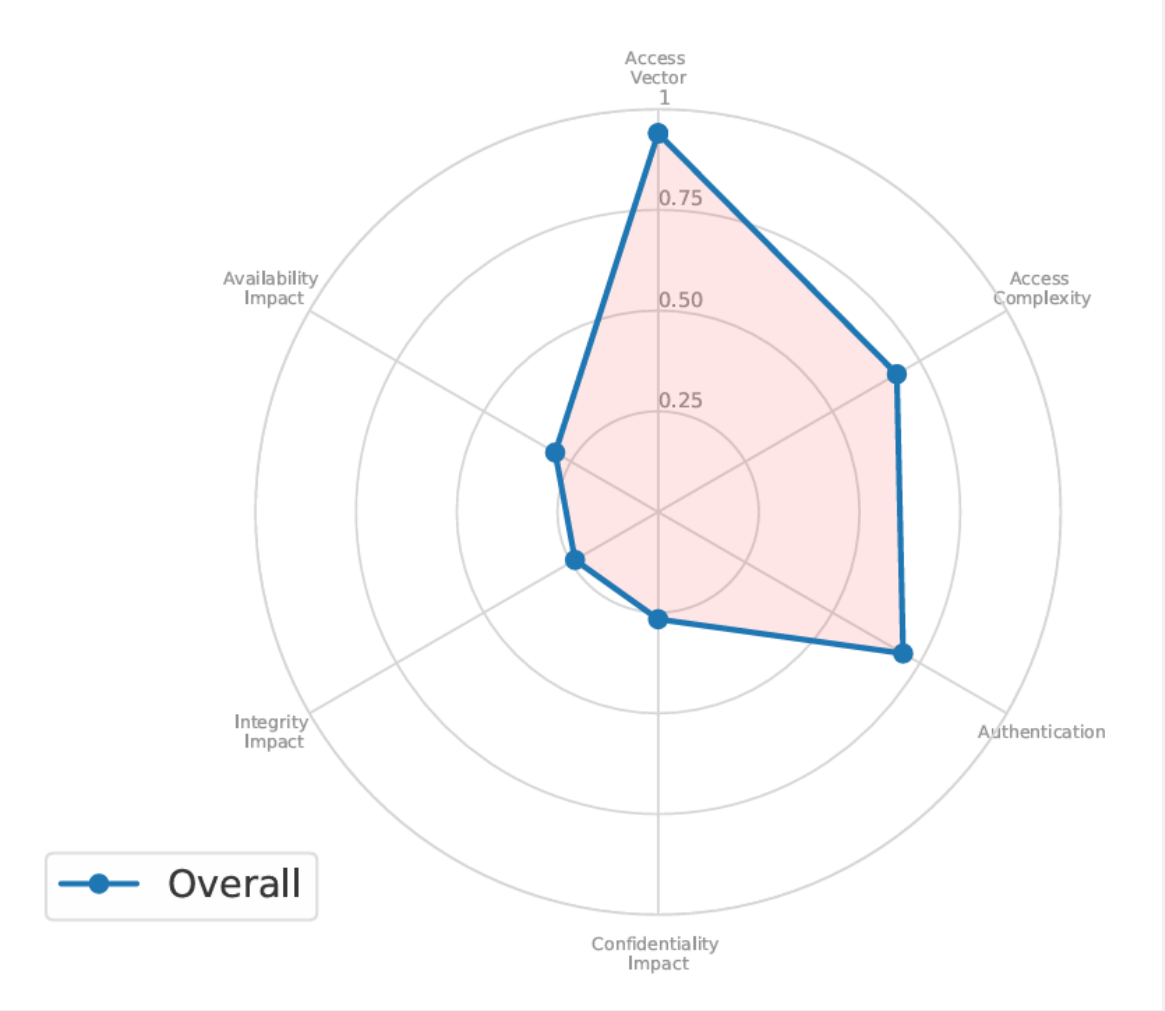
```
AccessVector =
      local access: 0.395
      adjacent network accessible: 0.646
      network accessible: 1.0

AccessComplexity =
      high: 0.35
      medium: 0.61
      low: 0.71

Authentication =
      requires multiple instances of authentication: 0.45
      requires single instance of authentication: 0.56
      requires no authentication: 0.704

* Impact =
      none: 0.0
      partial: 0.275
      complete: 0.66
```

[2]



[2] “CVSS v2 Complete Documentation,” Available: https://www.first.org/cvss/v2/guide

Wo gibt’s was & Fragen

Das Dashboard läuft unter
database-attack.foran.lab

ACEMA Quellcode mit allen Daten und Diagrammen
github.com/dumpeldown/acema_oran

Arbeit & Präsentation
github.com/dumpeldown/foran-ba