SHIELD: Assessing Security-by-Design in Federated Data Spaces Using Attack Graphs

Alessandro Palma*, Nikolaos Papadakis[+], Georgios Bouloukakis[+], Joaquin Garcia-Alfaro[+], Mattia Sospetti[-], Kostas Magoutis[°]

*Sapienza University of Rome, Italy

[+]Samovar, Télécom SudParis, France

[-]GrottiniLab S.r.L, Italy

[°]University of Crete, Greece

SAC 2025, Catania, Italy, April 1st 2025

Supported by the Horizon Europe projects DI-Hydro (Grant n. 101122311)

Federated Data Space

***Collaborative** environments where multiple organizations **share and access** data across different domains*

collect consumption data

collect charging data

adapt controls

collect data for analytics

Transportation COMMUNITY

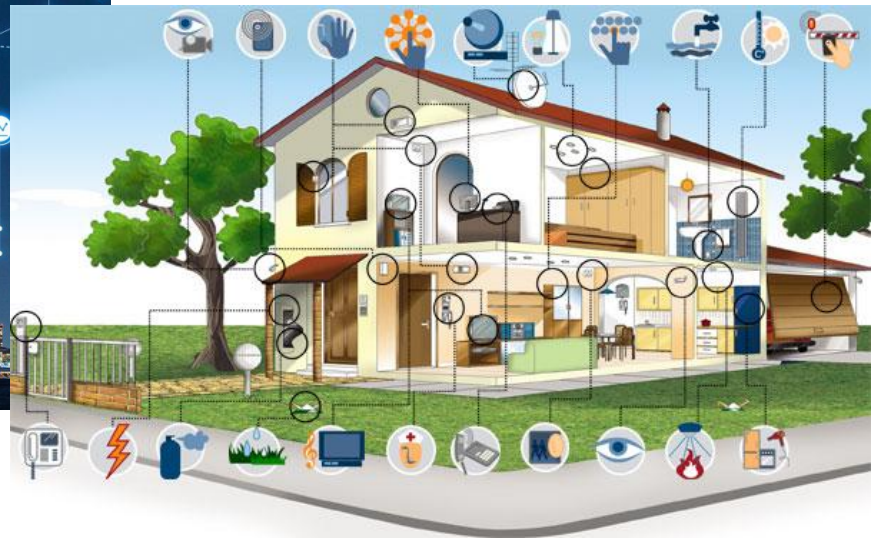
Charging Station COMMUNITY

Management COMMUNITY

Federated Data Space

***Collaborative** environments where multiple organizations **share and access** data across different domains*

Smart Cities



Smart Homes

… in a modern version of Hogwarts

Federated Data Space: security issues

Transportation COM

CVE-2021-22722

Could cause code injection when changing station parameters.

How to make federated data spaces **SECURE-BY-DESIGN** ?

Management COMMUNITY

Force separation of code and data

CVE-2023-49277

A remote user can execute arbitrary code, leading to unauthorized access

No interference with third-party companies

Update firmware

Too downtime service

Current security of federated data spaces

Security-by-design

- Anomaly detection based on traffic[Vajpayee]
- Anomaly detection based on cyber-physical functionalities[Bhardwaj]

Do not consider **existing** vulnerabilities

Secure messaging

- Message encryption[Razouk]
- Message tampering and authentication[Malina]

Mainly for **confidentiality** and **integrity**

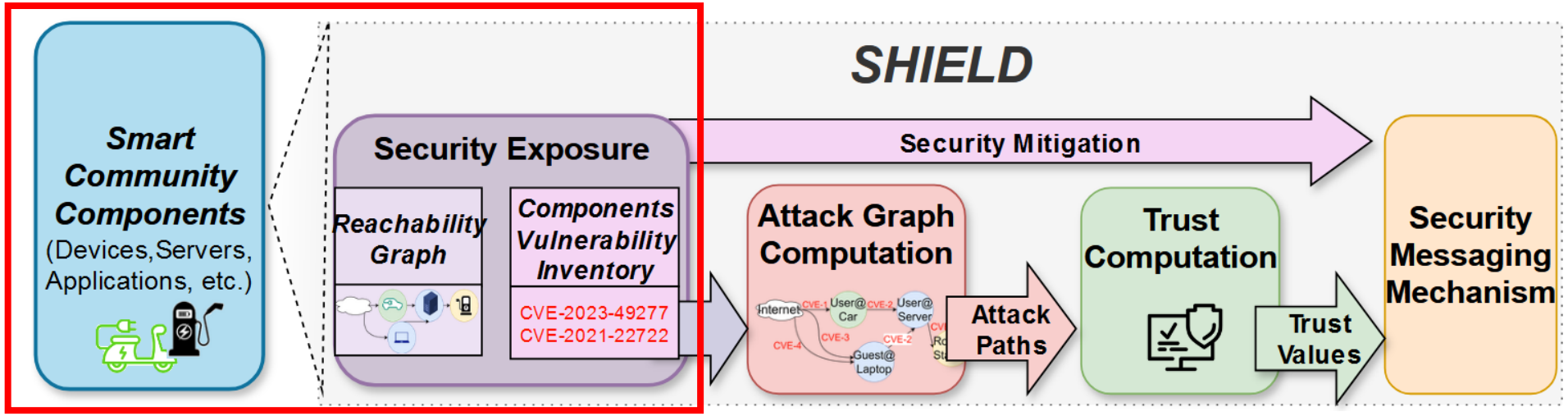
Trust management

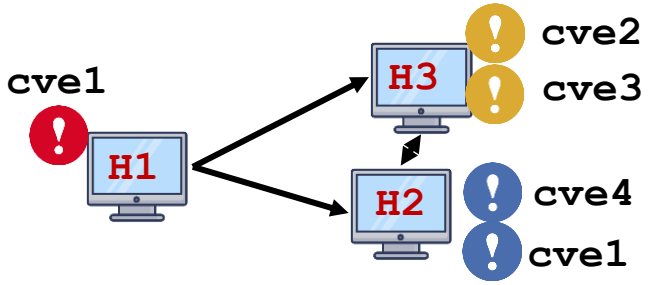
- TEE (Trusted Execution Environment)[Pascoal]
- QoS-based trust[Khan]

Lack of combination of **cyber risks** and **federated architecture**

[Vajpayee] P. Vajpayee and G. Hossain. 2024. Risk Assessment of Cybersecurity IoT Anomalies Through Cyber Value at Risk. (AIIoT).
[Bhardawaj] S. Bhardwaj and M. Dave. 2024. Attack detection and mitigation using Intelligent attack graph model for Forensic in IoT Networks. Telecom. Sys. 85, 4 (2024).
[Razouk] W. Razouk, D. Sgandurra, and K. Sakurai. 2017. A new security middleware architecture based on fog computing and cloud to support IoT constrained devices. (IoT-ML)
[Malina] L. Malina, G. Srivastava, P. Dzurenda, J. Hajny, and R. Fujdiak. 2019. A Secure Publish/Subscribe Protocol for Internet of Things. (ARES '19).
[Pascoal] T. Pascoal, J. Decouchant, and M. Völp. 2022. Secure and distributed assessment of privacy-preserving GWAS releases. (MIDDLEWARE)
[Khan] Z. A. Khan and P. Herrmann. 2017. A Trust Based Distributed Intrusion Detection Mechanism for Internet of Things. (AINA)

Proposed solution: SHIELD





Reachability Graph

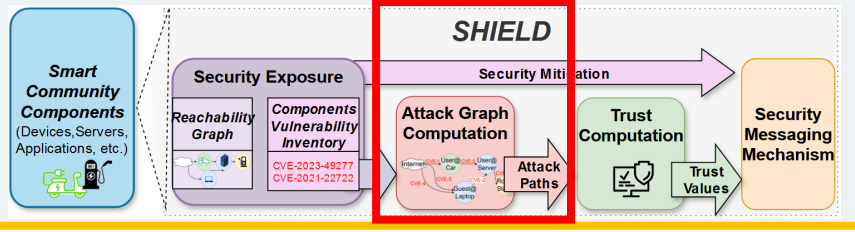
Vulnerability Inventory[CVE]

Network administrator has full view of reachability

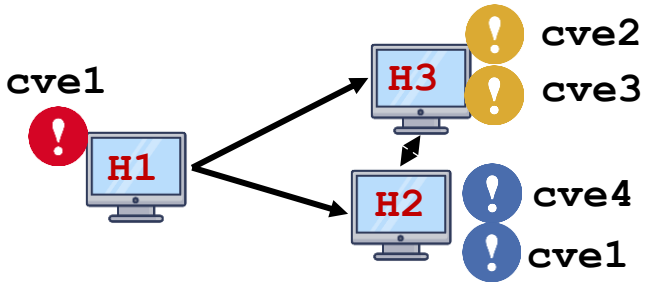
No adversarial attacks during trust computation

[CVE] https://cve.mitre.org/

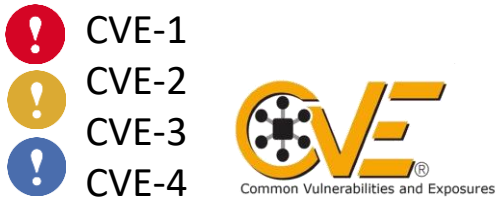
Attack Graph



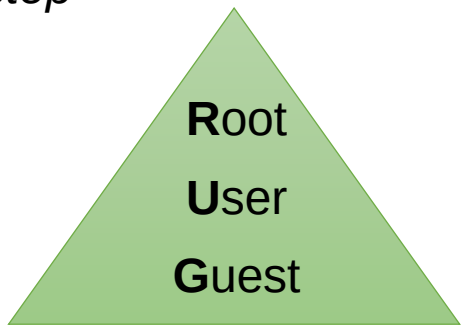
*An Attack Graph represents possible ways an attacker can intrude into the network by exploiting a **series of vulnerabilities** on network hosts based on certain **privileges** at each step*[Kaynar]



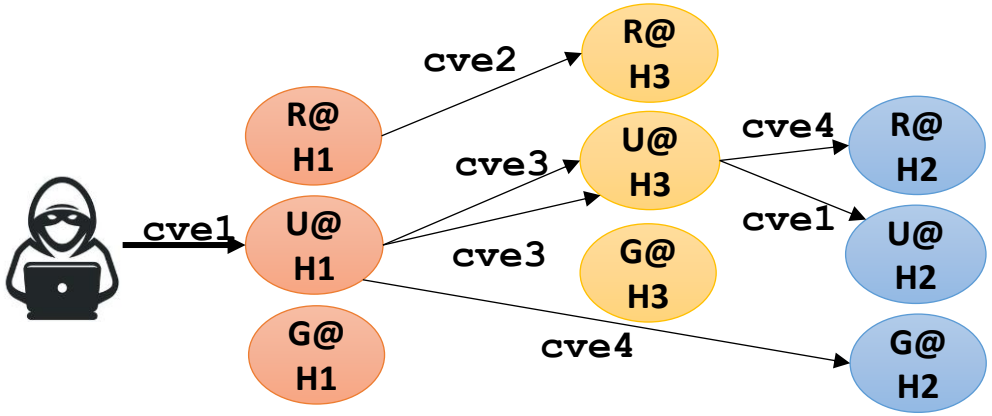
Reachability Network

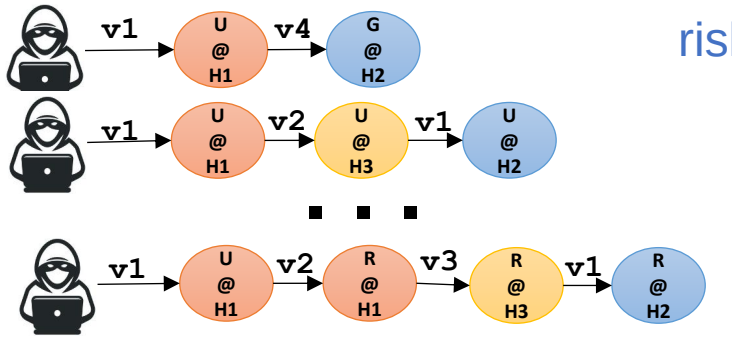


Vulnerability Inventory[CVE]



Attacker's privileges





Attack Graph generation

$risk(AP_1)$ = likelihood * impact

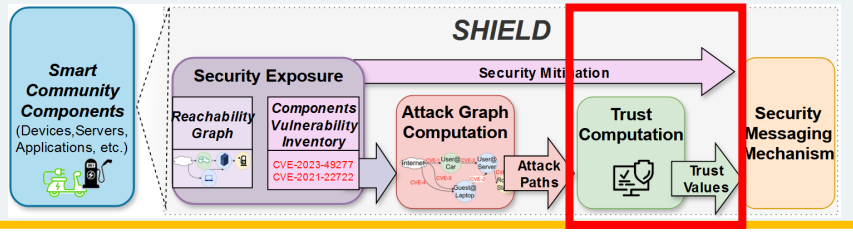
. . .

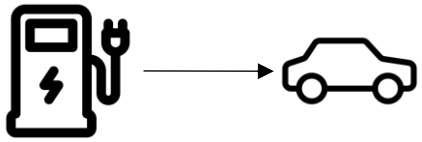
$risk(AP_N)$

Attack Path analysis

[Kaynar] Kaynar, K. A taxonomy for attack graph generation and usage in network security. *Journal of Information Security and Applications*, *2016*.
[CVSS] https://www.first.org/cvss/

Trust Computation





source device d_s target device d_t

- R: **Risk** of being attacked from d_s
- L: Avg attack path **length** from d_s to d_t
- O: **belonging** to same community
- C: num. traversed **communities**

$$P_{dsdt} = [R, L, O, C]$$

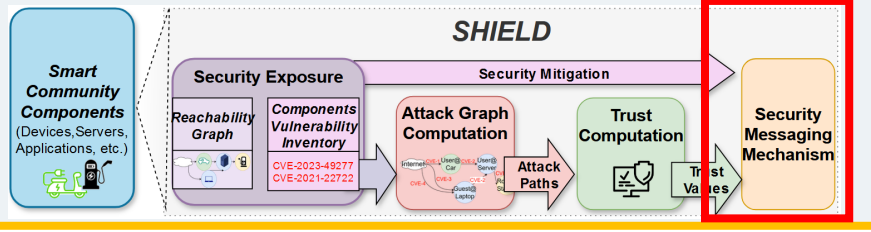
weights $W_{dsdt} \in [0,1]$
s.t. $\sum_i w_i = 1 \; \forall i$

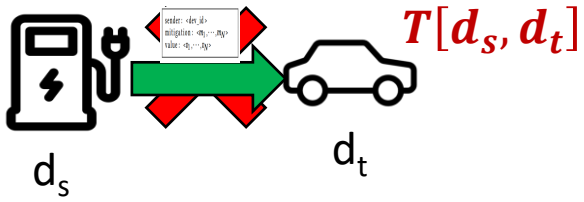
Aggregation function

$$F = \begin{cases} 0, & if\ w_R R \geq r\_max \\ 1, & if\ w_R R \leq r\_min \\ round\left(\sum_{p \in \{L,C,O\}} (w_p p + w_R(1-R))\right), & otherwise \end{cases}$$

Trust computation
$\boldsymbol{T[d_s, d_t] = [P_{dsdt}, W_{dsdt}, F]}$

Security Messaging Mechanism





Security mitigation

$$m(u, d_t) = [id, phase, strategy, cost, \boldsymbol{applied}]$$

From CWE[CWE]

- Strategies may impact other devices (e.g., resource limitation) → $C_{between}$
- Local strategies (e.g., isolate running code from data) → C_{within}

d_s is a risky source — d_t $opt-out$ d_s $if\ T[d_s, d_t] = 0$

d_s is a trusted source — d_t $receives\ from$ d_s $if\ T[d_s, d_t] = 1$

d_s is a trusted source and d_t has mitigation affecting d_s — d_t $sends$ $\boldsymbol{mitigationMSG}$ $if\ T[d_s, d_t] = 1 \wedge m(u, d_t) \in C_{between}$

d_s **patches** a vulnerability — d_t $recomputes\ trust$

$\boldsymbol{mitigationMSG}$

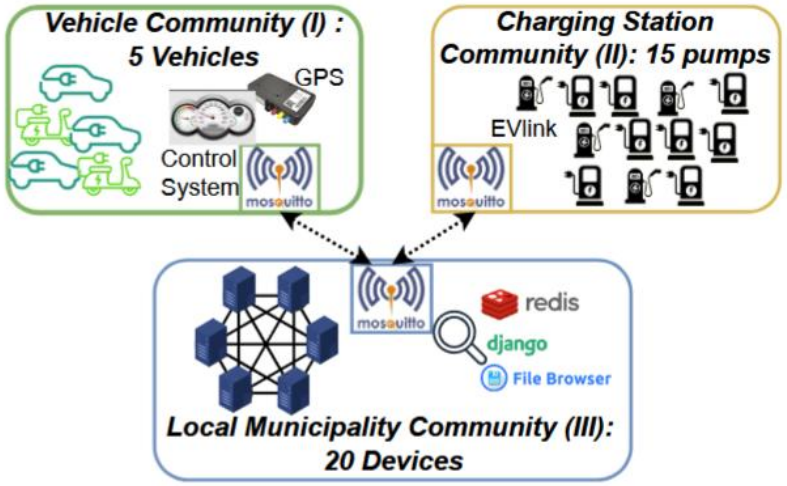
sender: <dev_id>
mitigation: $<m_1, \cdots, m_N>$
value: $<v_1, \cdots, v_N>$

$\boldsymbol{patchingMSG}$

sender: <dev_id>
patched: $<u_1, \cdots, u_N>$

[CWE] https://cwe.mitre.org/

Evaluation: setup



Community	Service
(I) Vehicle	SourceCodester Vehicle Control System v1.0
(I) Vehicle	HQT-401 GPS
(II) Local Municipality	Redis v6.2.6
(II) Local Municipality	Django v3.2
(II) Local Municipality	Filebrowser v2.22
(III) Charging station	EVlink City v3.4.0.1
(III) Charging station	EVlink Smart Wallbox v3.4.0.1
(III) Charging station	EVlink Load Management v4.0.0.13
	Mosquitto Broker with MQTT v5.0

SHIELD prototype using:

- pub/sub for communication
- State-of-the-Art Attack Graph generation[Palma]
- Python for trust model implementation

Compare with:

- Naïve pub/sub (no security)
- Protocol-based security pub/sub[Park]

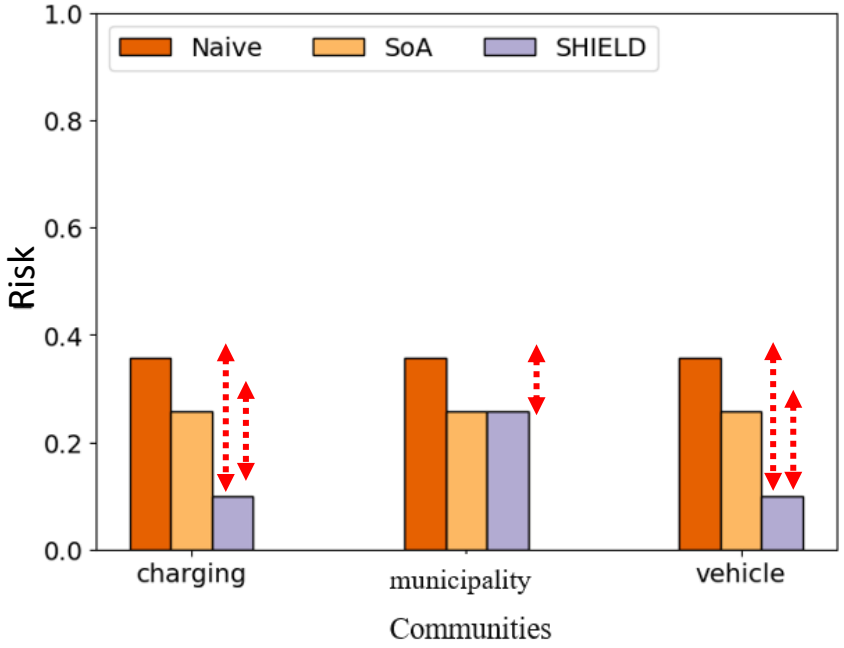
Evaluate:

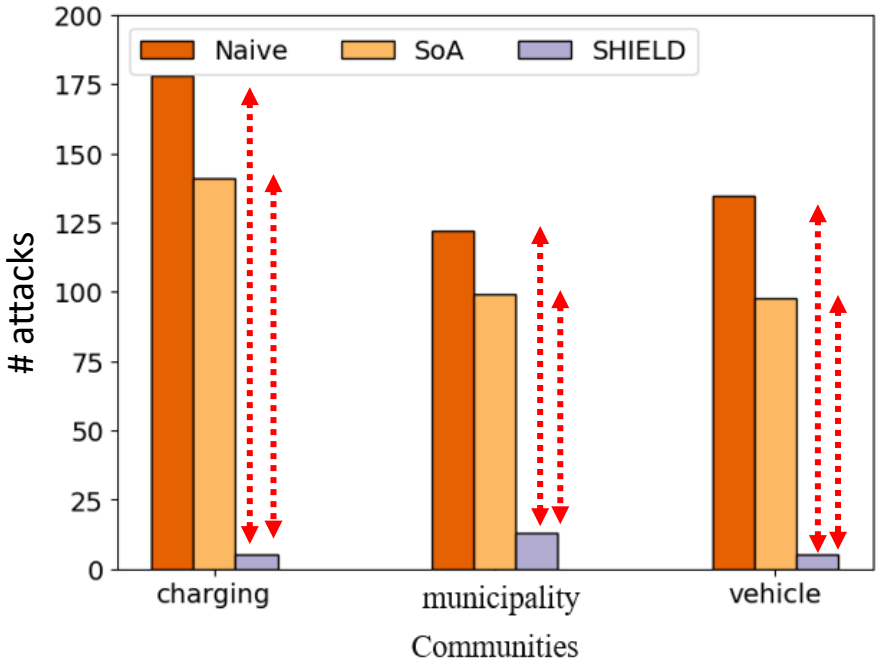
- Security (cyber risk assessment and attack surface reduction)
- Overhead (response time and message loss)

Applied to a real scenario from Hellenic energy provider (PPC)[Dalamagkas]

[Palma] Palma A., Angelini M. 2024. It Is Time to Steer: A Scalable Framework for Analysis-driven Attack Graph Generation. ESORICS (2024).
[Park] C.-S. Park and H.-M. Nam. 2020. Security Architecture and Protocols for Secure MQTT-SN. IEEE Access 8 (2020).
[Dalamagkas] C. Dalamagkas, A. Georgakis, K. Hrissagis-Chrysagis, and G. Papadakis. 2024. The Open V2X Management Platform. In Web Engineering. https://www.ppcgroup.com/en/ppc/

Evaluation: security

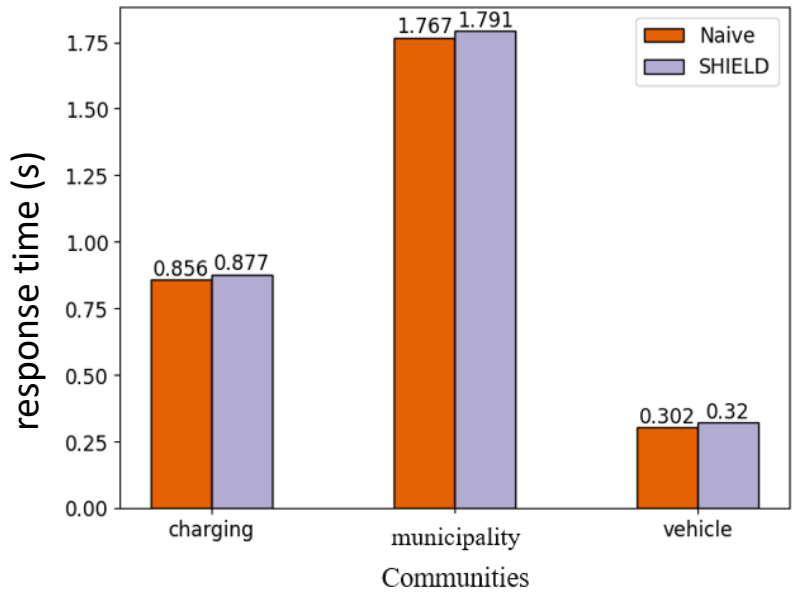




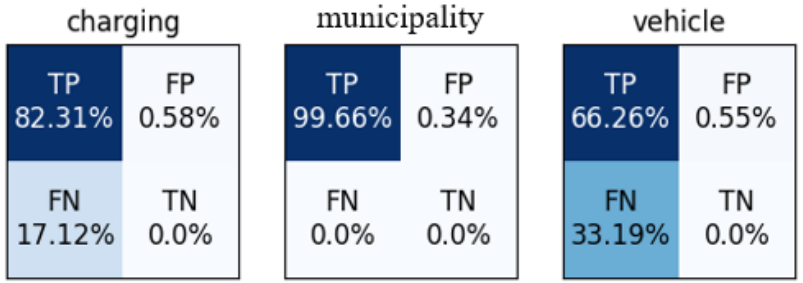
- Risk reduced by **60%** compared to Naïve
- Risk reduced by **35%** compared to SoA
- Best effects on charging stations

- Attack surface reduced by **85%** compared to Naïve
- Risk reduced by **65%** compared to SoA
- Best effects on peripheral communities

Evaluation: Quality-of-Service



- TP: messages correctly delivered
- FP: messages lost
- FN: non-operational messages
- TN: messages correctly NOT



Quality of Service (QoS)

- Response time **increased by 1.5%**
- Accuracy 0.82 → **18% lost messages**

Security-QoS Trade-off
Price to pay to have risk-aware secure messaging

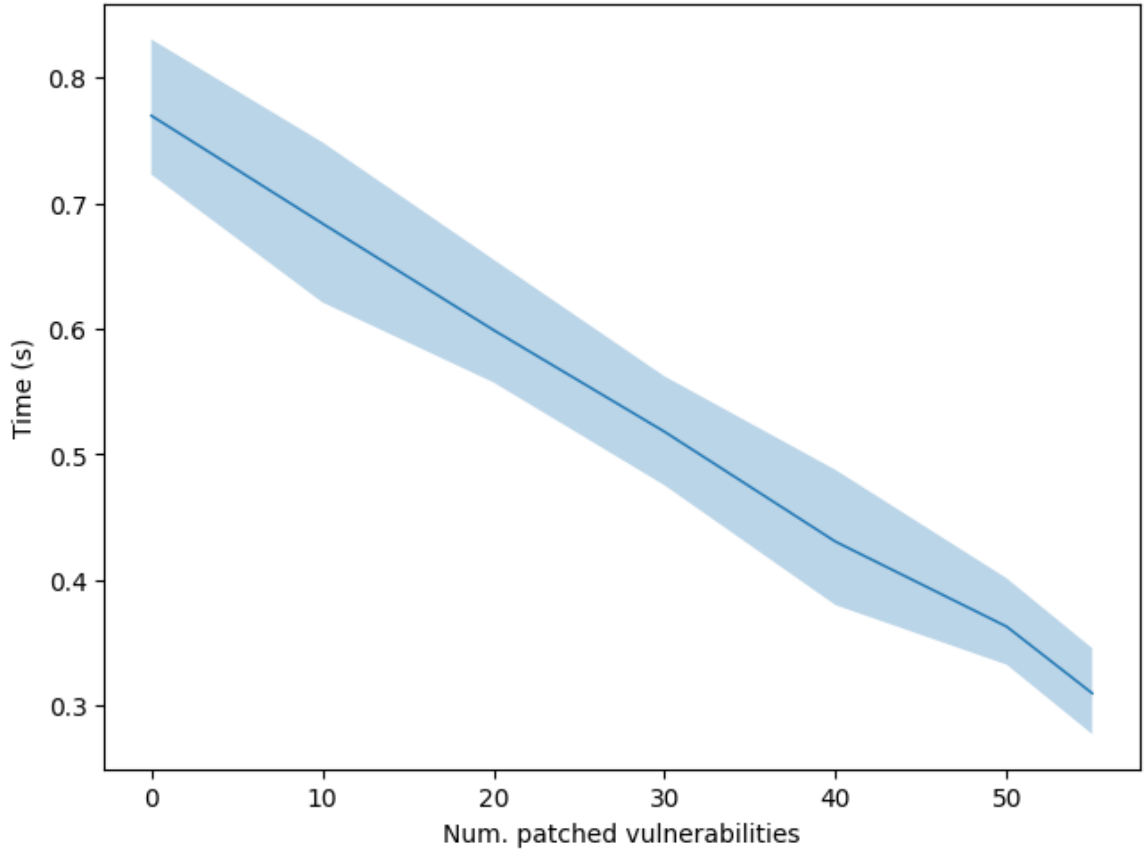
Evaluation: Changes in the network

Simulation of vulnerability patching during the computation

- Step of (up to 10) vulnerabilities per time
- 100 simulations per scenario

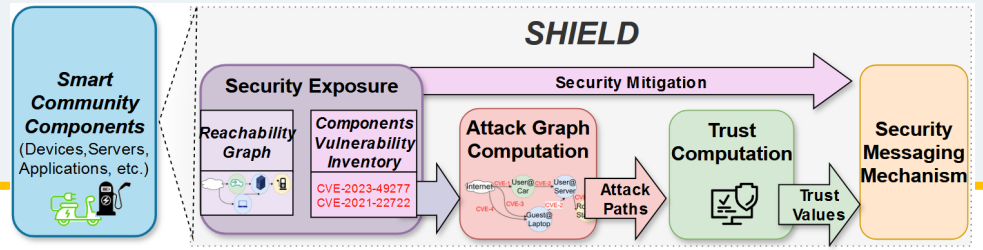
Results

- Decreasing computation time by patched vulnerabilities.
- In the worst-case scenario the computation time is relatively small.
  - Reasonable for federated data spaces[Lim]



[Lim] K. L. Lim, J. Whitehead, D. Jia, and Z. Zheng. 2021. State of data platforms for connected vehicles and infrastructures. Comm. in transportation res. 1 (2021).

Conclusions



SHIELD: an architectural framework to assess cyber risks in federated data spaces

- Combine federated architecture with risk assessment → security-by-design

Risk reduction up to 60% and attack surface up to 85%

Slight degradation on the QoS (response time increased by 1.5% and 18% message lost)

FUTURE WORKS

- ➢ Define a sophisticated model to analyze and react to QoS degradation (e.g., replicas)
- ➢ Remove assumption of safe computation (e.g., modeling Byzantines scenarios)

Supported by the Horizon Europe projects DI-Hydro (Grant n. 101122311)

SHIELD: Assessing Security-by-Design in Federated Data Spaces Using Attack Graphs

Alessandro Palma
Sapienza University of Rome
palma@diag.uniroma1.it

Nikolaos Papadakis
Samovar, Télécom SudParis
nikolaos.papadakis@telecom-sudparis.eu

Georgios Bouloukakis
Samovar, Télécom SudParis
georgios.bouloukakis@telecom-sudparis.eu

Joaquin Garcia-Alfaro
Samovar, Télécom SudParis
joaquin.garcia_alfaro@telecom-sudparis.eu

Mattia Sospetti
GrottiniLab S.r.L
mattia.sospetti@grottinilab.com

Kostas Magoutis
University of Crete
magoutis@ics.forth.gr

All materials available at: