SPARQ: A QoS-Aware Framework for Mitigating Cyber Risk in Self-Protecting IoT Systems

Alessandro Palma*, Houssam Hajj Hassan°, Georgios Bouloukakis°
Presented by Nikolaos Papadakis°

* Sapienza University of Rome
° SAMOVAR, Télécom SudParis

SEAMS 2025, Ottawa, Canada, April 29th

Self-Protection: Motivation

Act of taking measures to ensure one's own safety and well-being, through strategic actions to ***prevent*** harm or danger[Alicke].

Avoid going to the hospital periodically

SAVE TIME

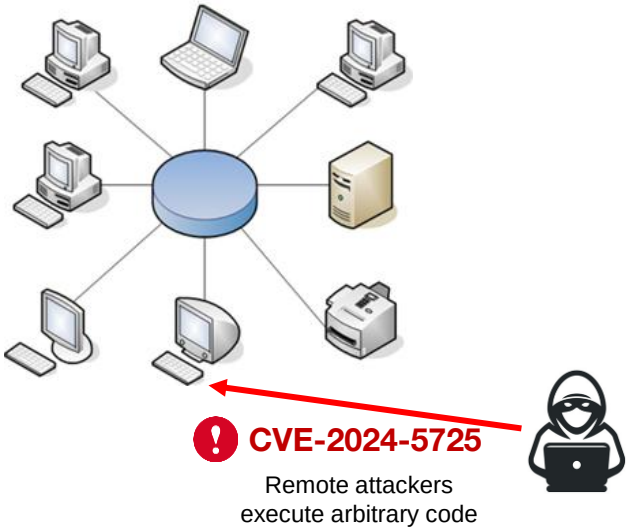
WHY?

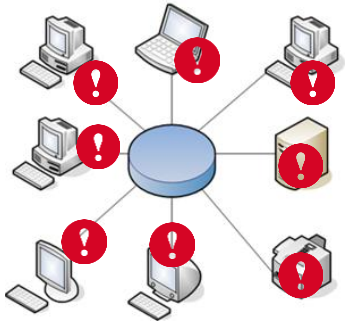
Defend against unexpected attacks

DEFEND/PREVENT ATTACKS

[1] Alicke, Mark D., and C. Sedikides. "Self-enhancement and self-protection: What they are and what they do." *European review of social psychology* 20.1 (2009): 1-48.

Self-Protection in IoT Networks

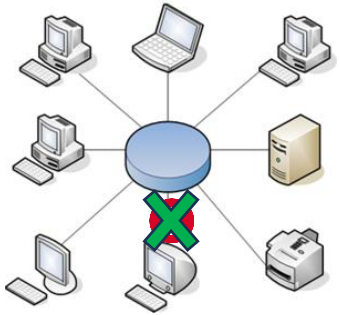




Wait for human operator

1. Analyze cyber risk
2. Take mitigation actions

In the meantime, network **attacked**



Self-protection

- Adapt the network to protect from exploits

Self-protection in IoT network: Issues and Challenges

- **drop-off links** to protect electrocardiogram
  - not worth interrupting services and leads to patients disappointment for low risk
  - can be patched by adjusting authorization controls
- **drop-off links** to protect X-ray machine
  - worth because vulnerability may cause unreliable measurements
  - requires **long** human intervention

NO single strategy for the different vulnerabilities

LOW RISK

CVE-2021-22722

Could cause unauthorized access

MEDIUM RISK

CVE-2023-49277

A remote user can execute arbitrary code

CRITICAL RISK

CVE-2021-22722

Could cause code injection when changing parameters.

Related Work

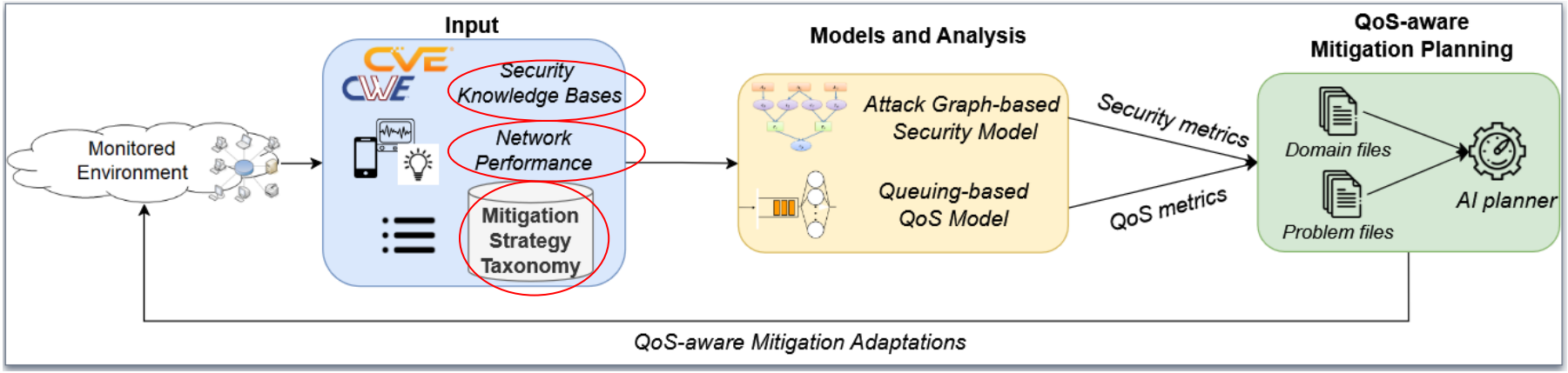
Existing self-protecting systems focus on workflow modeling[Yuan,Li]
To make them actionable a valuable solution is Attack Graphs, but it **overlooks the response planning**[Gonzalez]

Existing solutions for Attack Graph-based self-protection provide valuable proactive/reactive strategies to mitigate security[Zeller] without considering their **impact on QoS**[Bonomi]

Self-protection considering both QoS and security is crucial

[Yuan] Yuan, E., Malek, S., Schmerl, B., Garlan, D., Gennari, J.: Architecture-based self- protecting software systems. p. 33–42. QoSA '13, ACM (2013)
[Li] Li, N., Zhang, M., Li, J., Adepu, S., Kang, E., Jin, Z.: A Game-Theoretical Self-Adaptation Framework for Securing Software-Intensive Systems. ACM TAAS (2024)
[Gonzalez] Gonzalez-Granadillo, G., Dubus, S., Motzek, A., Garcia-Alfaro, J., Alvarez, E., Merialdo, M., Papillon, S., Debar, H.: Dynamic risk management response system to handle cyber threats. FGCS (2018)
[Zeller] Zeller, S., Khakpour, N., Weyns, D., & Deogun, D. (2020, June). Self-protection against business logic vulnerabilities. SEAMS (2020)
[Bonomi] Bonomi, S., Cuoci, M., Lenti, S., & Palma, A. (2024). Improving Attack Graph-based Self-Protecting Systems: A Computational Pipeline for Accuracy-Scalability Trade-off. CRiSIS (2024)

SPARQ: A QoS-Aware Framework for Mitigating Cyber Risk

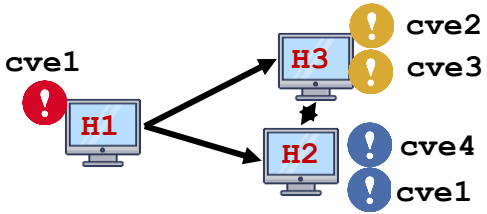


Model both security and QoS to take appropriate protection strategies

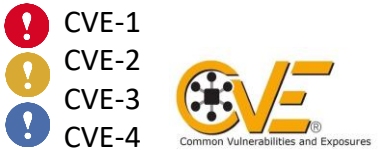
Automatically plan strategies informed by security and QoS models

SPARQ: Security Model

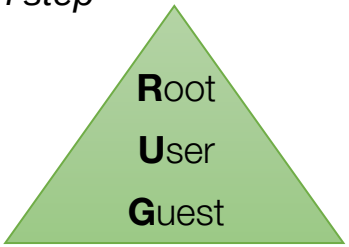
*An Attack Graph represents possible ways an attacker can intrude into the network by exploiting a **series of vulnerabilities** on network hosts based on certain **privileges** at each step*[Kaynar]



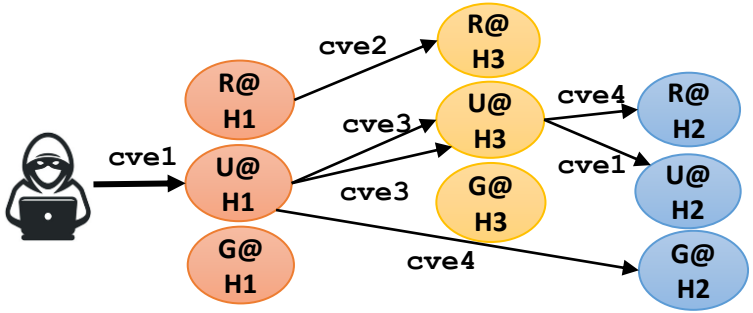
Reachability Network

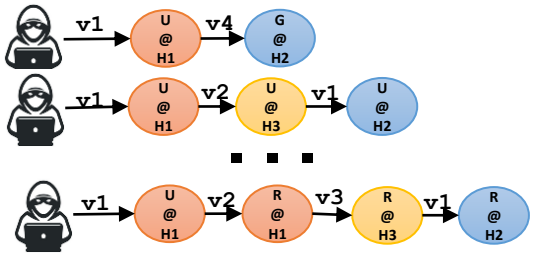


Vulnerability Inventory[CVE]



Attacker's privileges





Attack Graph simulation

CVSS

$risk(AP_1)$
$length(AP_1)$

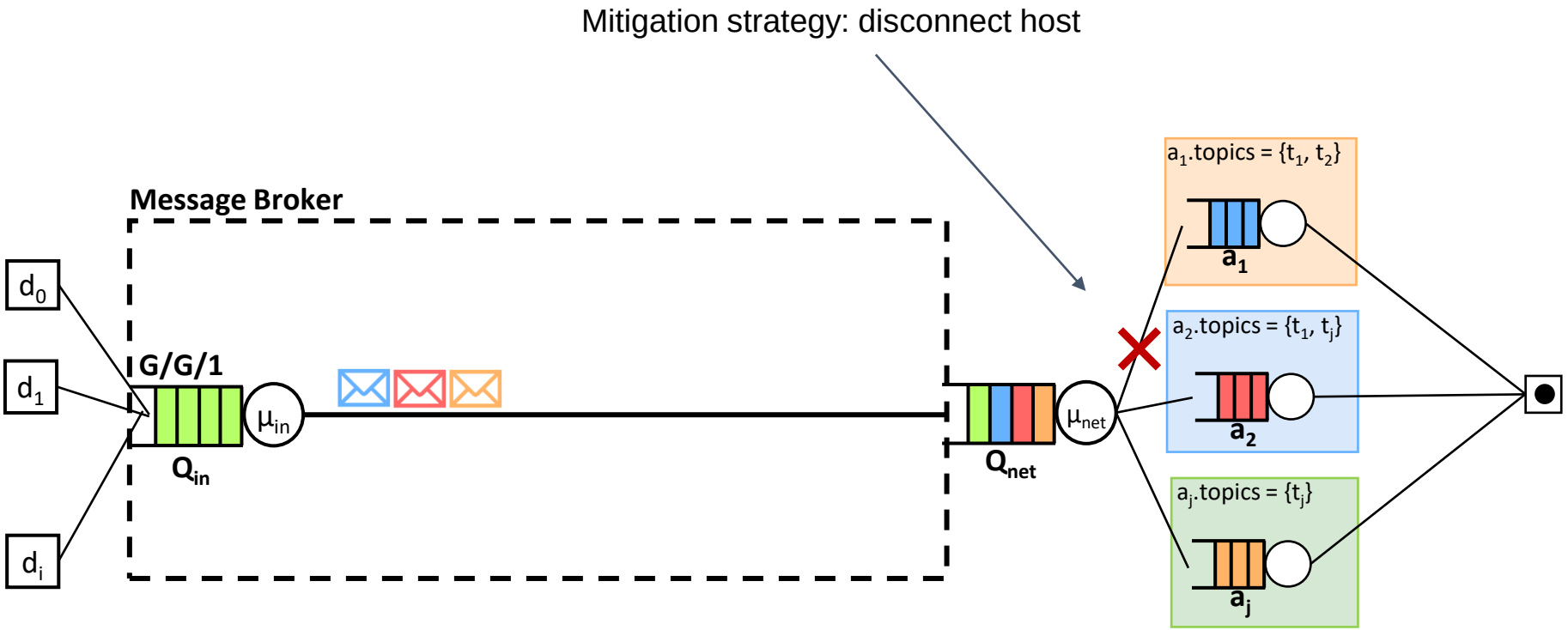
. . .

$risk(AP_N)$
$length(AP_N)$

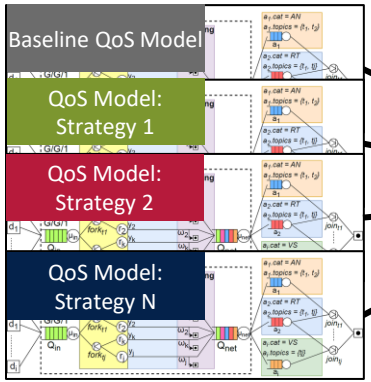
Security metrics

[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/

SPARQ: QoS Model



SPARQ QoS Model



simulate

Performance Metrics Dataset

App	Topic	Update Libraries	Change IP	...	Use Firewall	Input Validation	Restart device	...
app 1	smoke	0.2015	0.560679		0.4761	0.4651	0.498188	
app 1	temp	0.515479	0.13125		0.5193	0.4950	0.131307	
app 3	temp	0.633439	0.5532327		0.4624	0.3168	0.23485	
app j	occupancy	0.134651	0.345628		0.2156	0.5138	0.154152	

Response times per data flow

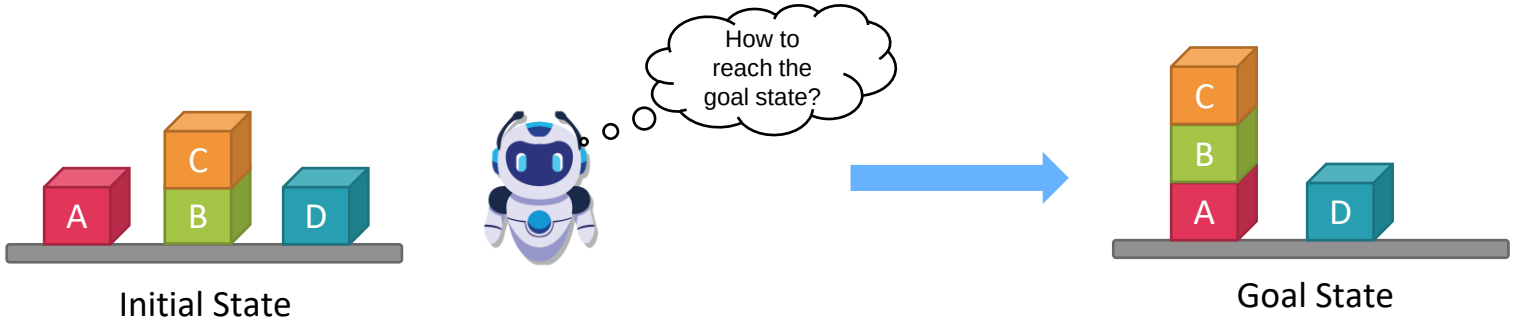
App	Topic	Update Libraries	Change IP		Use Firewall	Input Validation	Restart device	...
app 1	smoke	452.141	262.432		450.14	363.43	479.532	
..	...	...	...		...	...	...	

Throughput per data flow

App	Topic	Update Libraries	Change IP	...	Use Firewall	Input Validation	Restart device	...
app 1	smoke	0.00	0.008243		0.0014	0.000	0.000	
..	...	...	...		...	...	...	

Drop rate per data flow

SPARQ: QoS-aware Mitigation Planning



Automated Planning is an area of artificial intelligence where the task is to **choose** and arrange **actions** in order **to achieve some goal**.

Application Domains

- Robotics [1]
- Web services composition [2], [3]
- Orchestration of IoT applications [4]

[1] A. Kattepur, B. Purushothaman. Cognitive Computation and Systems. 2020.
[2] S. Qi, X. Tang, D. Chen. IEEE CGC. 2012
[3] G. Zou, Y. Chen, Y. Yang, R. Huang, Y. Xu. Intl. Conf.on Cloud Computing and Virtualization.
[4] U. Bellur, N. Narendra, and S. Mohalik.IEEE Services. 2017

SPARQ: QoS-aware Mitigation Planning

A Planning Domain **Σ** is a state transition system that contains**:**

- A finite set of states of the system (S)
- A set of actions α to be performed by an agent (e.g., SPARQ)
- A state transition function γ: S x A → S
- A cost function C: S x A → [0, ∞)

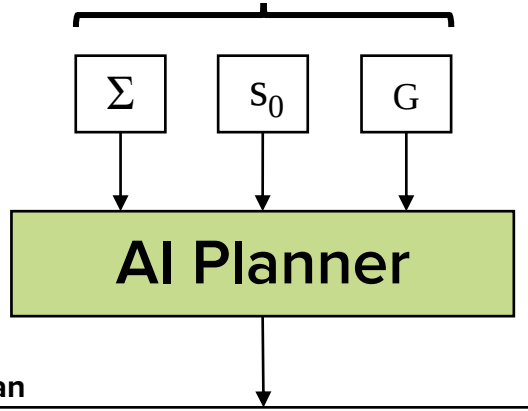
Initial State

- No mitigation action is applied
- Current security metrics (e.g, average risk, number of attack paths, etc.)

Goal State

- $R < R_{max}$
- $L < L_{max}$
- $\Delta_{app} < \Delta_{max}$
- $\Theta_{app} > \Theta_{min}$
- $\Xi_{app} < \Xi_{max}$

Planning Problem: $P = (\Sigma, s_0, G)$



Plan

π

$\pi = <\alpha_1, \alpha_2, \alpha_3, \ldots>$

α_1: m(app_1)

α_2: m(app_2)

α_3: m(app_3)

A solution for a planning problem P is a plan π such that

$\gamma(s_0, \alpha_1) \ldots (s_m, \alpha_\pi)$ satisfies G.

SPARQ: QoS-aware Mitigation Planning

A Planning Domain **Σ** is a state transition system that contains:
- A finite set of states of the system (S)
- A set of actions α to be performed by an agent (e.g., SPARQ)
- A state transition function γ: S x A → S
- A cost function C: S x A → [0, ∞)

Initial State

- No mitigation action is applied
- Current security metrics (e.g, average risk, number of attack paths, etc.)

Goal State

- $R < R_{max}$
- $\Delta_{app} < \Delta_{max}$
- $\Theta_{app} > \Theta_{min}$
- $\Xi_{app} < \Xi_{max}$

Planning problems are expressed using the Planning Domain Definition Language (PDDL), an action centered language that provides a standard syntax to describe actions by their parameters, preconditions, and effects.

Domain file

```
(:action update-libraries
   :parameters (?d -device ?app -application)
   :precondition (and (not (mitigation-applied ?d)))
   :effect (and (increase (avg_risk) 0.720)
                (decrease (avg_len) 1.889)
                (increase (avg_latency) 0.487)
                ….
                (mitigation-applied ?app))
```

Problem file

```
(:objects
   device1 device2 … -device
   app1 app2 app3 app4 … -application)
(:init
      (not (mitigation-applied app1))
      (= (avg_risk) 0)
      (= (avg_len) 0)
      …
      (= (avg_latency) 0)
(:goal (and  (mitigation-applied app1))
(:metric minimize (+ (+ (+
      (* 1 (avg_risk)))
      (* 1 (avg_len)))
      (* 1 (avg_latency)))
```

SPARQ: QoS-aware Mitigation Planning

Mitigation adaptation	QoS effects	Category
Update software libraries	Increased delay	Security
Avoid dynamic refactoring	Human intervention	Security
Double-Check the used programming language	Human intervention	Security
Check compilers correctness	Human intervention	Security
Environmental variables hardening	Human intervention	Security
Isolate code running from other processes	Human intervention	Security
Separate code and data and limit their interaction	Human intervention	Security
Separation of privilege: only necessary messages to necessary destinations	Reduced message size + Reachability adaptation	Security
Specify output encoding in messages	N/A	Security
Input validation	Increased delay	Security
Quarantining system files of a device	N/A	Security
Use an application firewall	Reachability adaptation	Architectural
Traffic redirection	Reachability adaptation	Architectural
Attack surface reduction: block untrusted sources	Reachability adaptation	Architectural
Limit resource utilization	Reduced message rate	Architectural
Change IP address	Reachability adaptation	Architectural
Restart a device	Increased delay + Shutdown period	Architectural
Packet dropping: drop all the packets to vulnerable destination	Reduced message rate + Reachability adaptation	Architectural
Disconnect the device from the Internet	Reachability adaptation	Architectural
Terminate one or more services in a device	Reduced message rate + Shutdown period	Architectural
Block one or more ports of a device	Reduced message rate	Architectural
Terminate all services in a device	Shutdown period	Architectural

Security strategies from security standards[CWE]

Architectural strategies modify infrastructure

- Most of the strategies can be immediately executed
  - QoS can be simulated
- … some require human intervention

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

Evaluation

2 IoT networks:

- ➢ Healthcare network (13 devices, 216 vulnerabilities)
- ➢ Smart home network (20 devices, 512 vulnerabilities)

Human intervention simulated with 3 strategies:

1. retain risk
2. patch all device vulnerabilities
3. patch a single vulnerability

Comparison with:

- No adaptation
- Only security adaptations
- Only architectural adaptations

Implementation details:

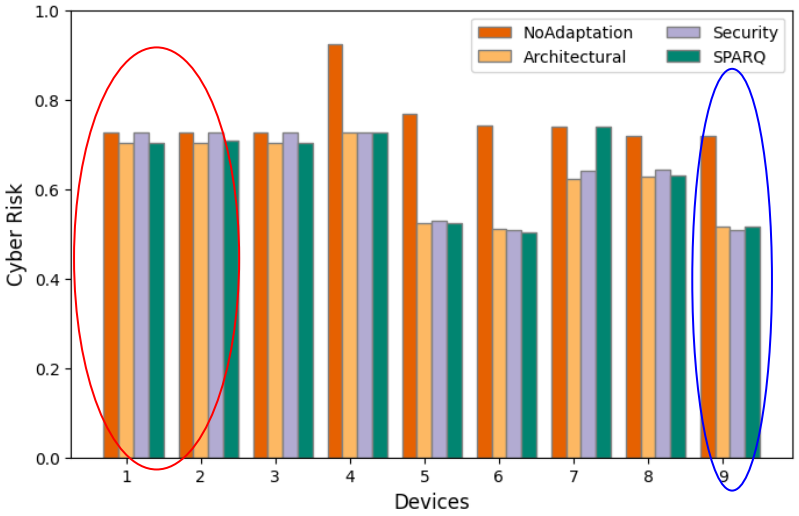
- Security model in Python*[Palma]*
- QoS model in JMT*[JMT]*
- Metric-FF for PDDL planner*[MetricFF]*

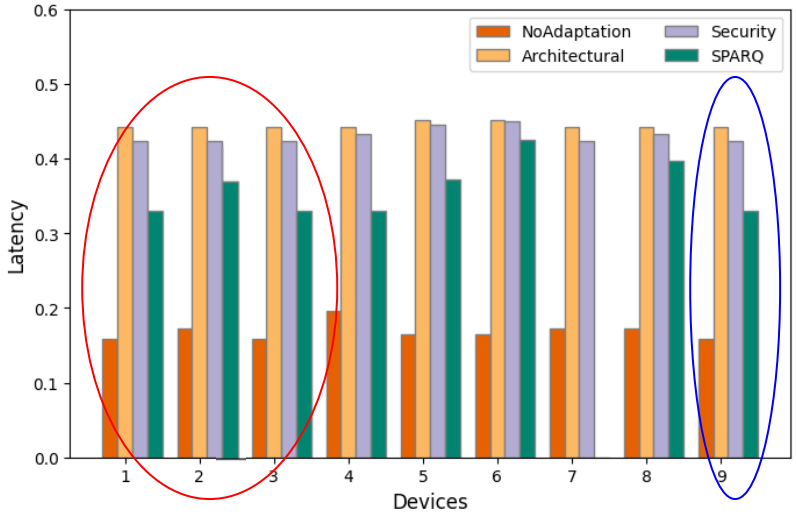
Research Questions (RQ):

1. To what extent is considering both architectural and security adaptations beneficial for **security**?
2. To what extent is considering both architectural and security adaptations beneficial for **QoS**?
3. What is the **security-QoS trade-off?**

[Palma] Palma, A., & Angelini, M. It is Time To Steer: A Scalable Framework for Analysis-Driven Attack Graph Generation. ESORICS 2024
[JMT] https://jmt.sourceforge.net/
[MetricFF] https://fai.cs.uni-saarland.de/hoffmann/metric-ff.html

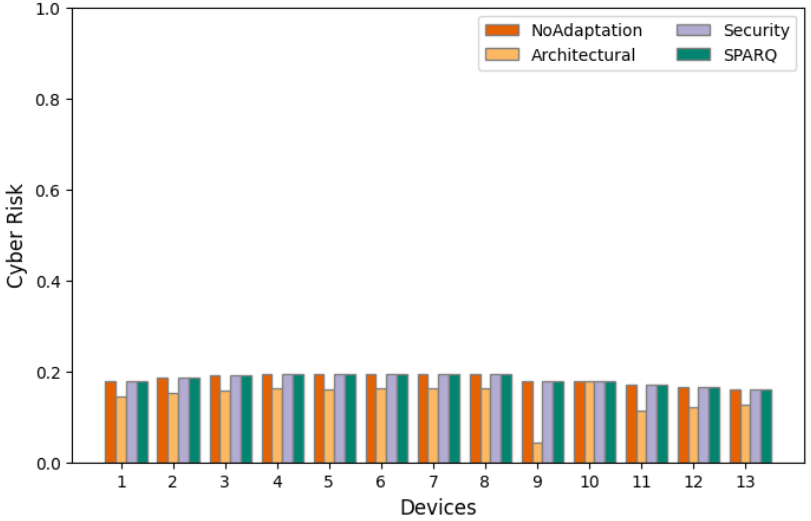
Evaluation: Smart Home Setting

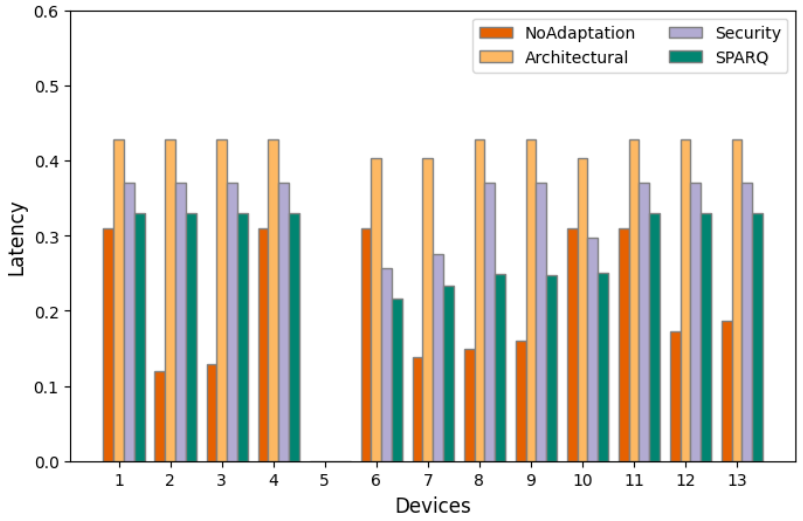




- SPARQ identifies the architectural adaptations in the **most risky situations**
- SPARQ correctly identify adaptations **worth applying or not**
  - if the cyber risk is low it may not be worth changing the network infrastructure
- Avg latency of **0.27** seconds in the smart home network (acceptable wrt QoS)

Evaluation: Healthcare Setting

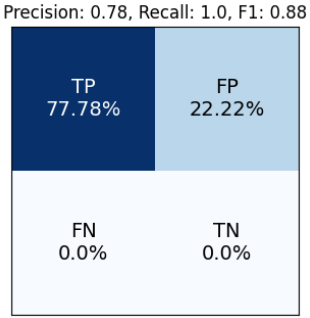




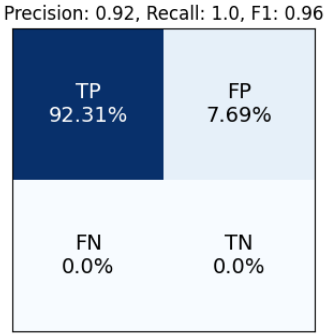
- Similar observations of Smart Home settings, but more risky devices
- In very risky scenarios (Healthcare), behaviour **comparable to ideal conditions**
  - SPARQ does not sacrifice QoS in critical infrastructures
- Avg latency of **0.26** seconds (acceptable wrt QoS)

Evaluation: QoS-aware Mitigation Planning (RQ3)

SMART HOME



HEALTHCARE



TP: correct strategies from CWE

FP: strategies not expected by CWE

FN: strategies expected by CWE

TN: strategies not in SPARQ nor in CWE

- Existing solutions that apply only architectural adaptations degrade the performance of the QoS due to the **drastic actions** that are put in place even when not necessary
- Applying only security adaptations provides very specific mitigation actions, but **disregards QoS** and the possibility of employing them autonomously
- SPARQ balances security and QoS for mitigation plans
  - in terms of QoS it **outperforms existing solutions**
  - in terms of security it shows an avg **0.85 accuracy**

Conclusion

SPARQ as a framework for self-protection integrating **QoS scenarios** beyond security

Security modeled through **Attack Graphs**, QoS modeled through **Queueing Networks**

Results show **good trade-off** of security and QoS, identifying suitable mitigation actions

Future Works

- Investigate the impact of human actions in SPARQ
  - Extend SPARQ as a human-in-loop system
- Enhance context-awareness with additional environment parameters

SPARQ: A QoS-Aware Framework for Mitigating Cyber Risk in Self-Protecting IoT Systems

Presented by Nikolaos Papadakis

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

Houssam Hajj Hassan
Télécom SudParis
houssam.hajj_hassan@telecom-sudparis.eu

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

Prototype and all materials available: