

PoC#4 – MitM: AI and Models for 5G/6G Networks

Judit Cerdà Izquierdo

jut.cerda@upc.edu

UPC

PoC Objective

The objective of this Proof of Concept (PoC) is to demonstrate and validate the behavior of the proposed Security Plane within a Beyond 5G (B5G) infrastructure. The PoC aims to provide a clear visualization of the Security Plane's operational workflow and its response mechanisms under adverse conditions. To assess its effectiveness and resilience, the Security Plane is evaluated through the execution of a Man-in-the-Middle (MitM) attack scenario.



**UNIVERSITAT POLITÈCNICA
DE CATALUNYA
BARCELONATECH**

CRAAXLab

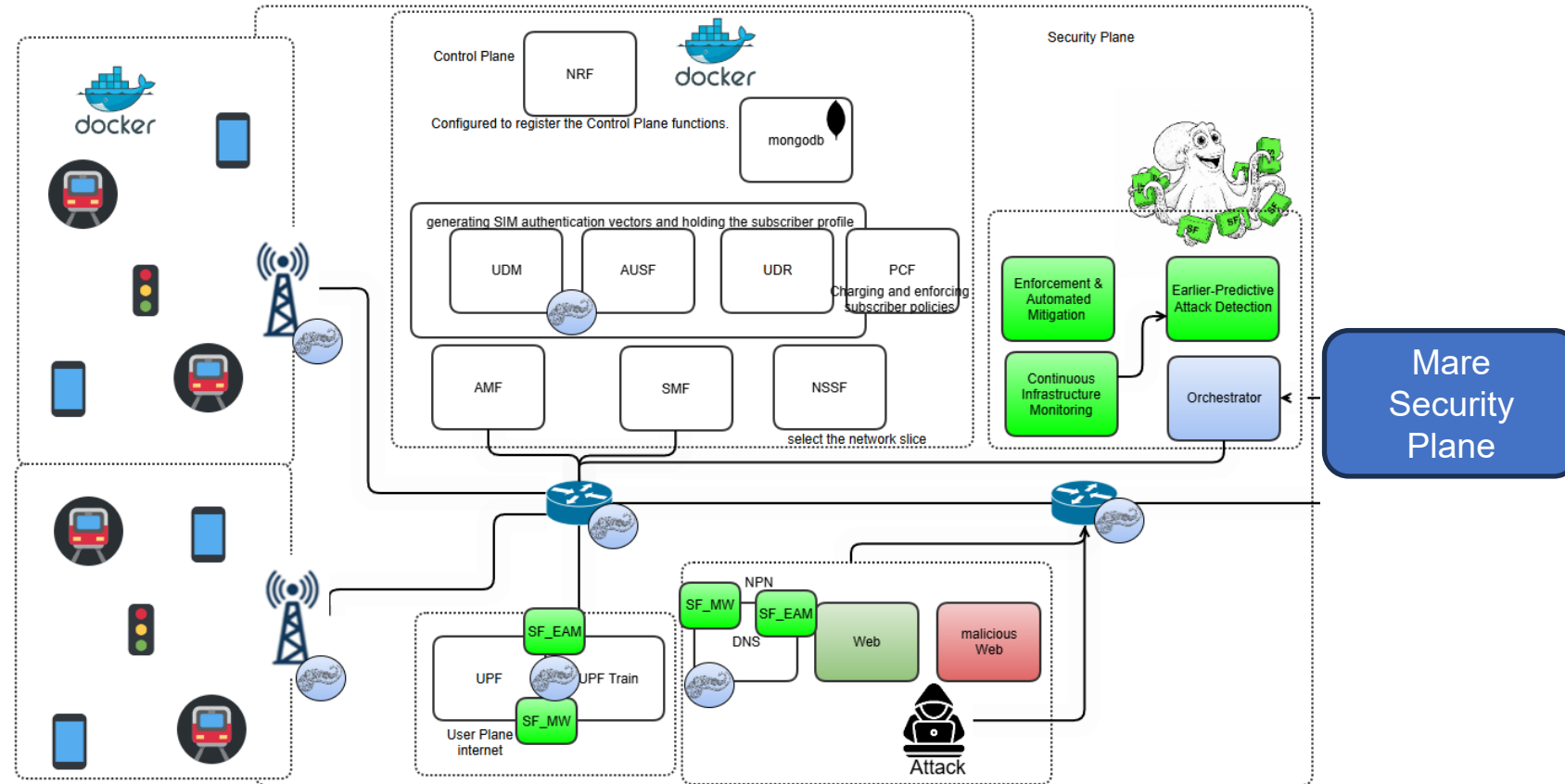
UPC - BARCELONATECH

Advanced Network Architectures Lab

Selected scenarios and Testbed

5G Testbed Overview

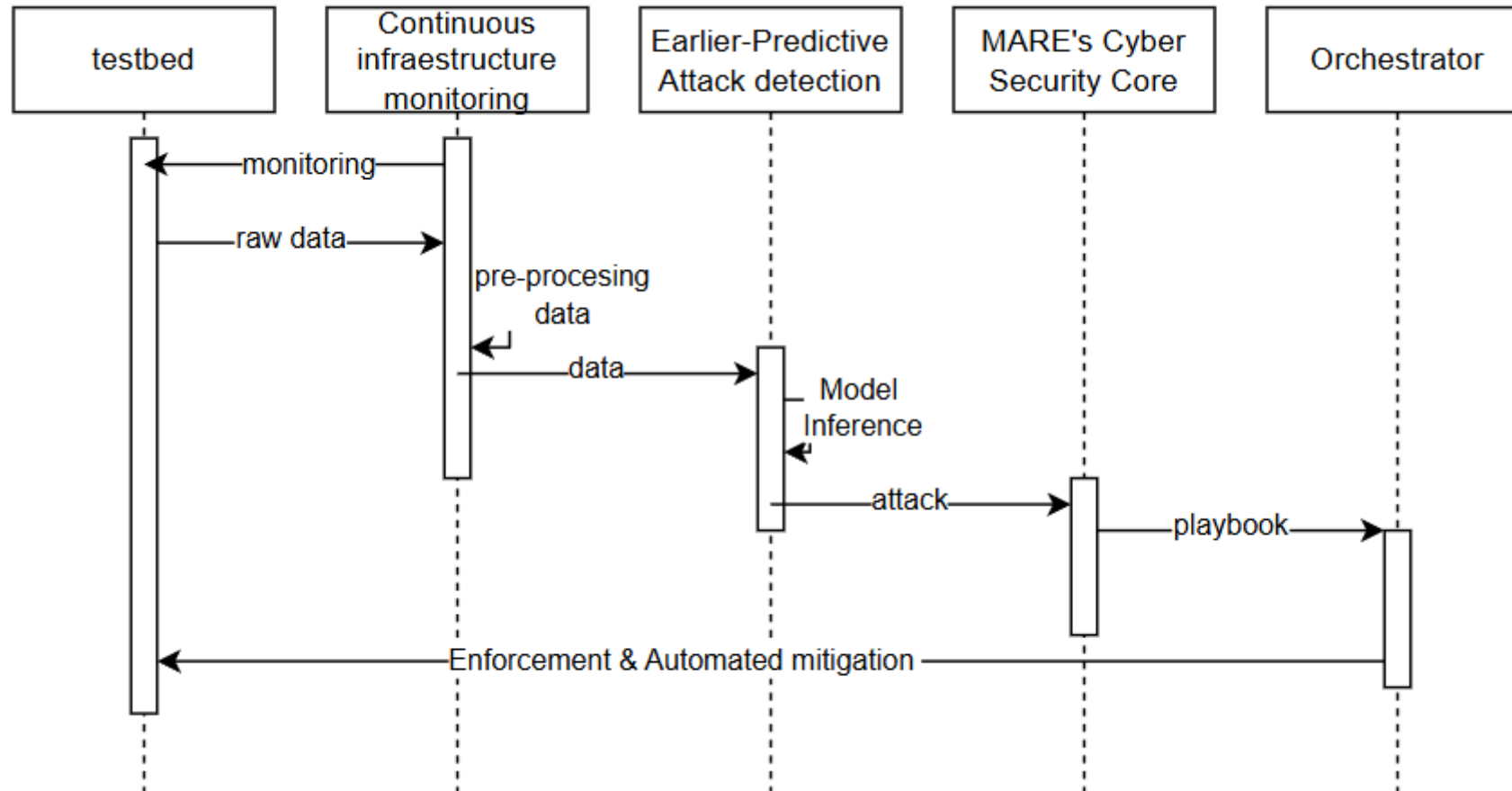
- Multiple UEs, two radio nodes, User Plane, Control Plane, and Security Plane.
- NPN hosting network services.
- PoC focus:
 - DNS Server (attack target)
 - Benign Web Server
 - Malicious Web Server
- Security Plane:
 - Security Functionalities
 - Security Orchestrator
 - Integration with the MARE architecture



Security Functions and DOTs

Security Functions	DoTs
Continuous Infrastructure Monitoring	Packet capture DOT (tcpdump)
	Flow feature extraction DOT (Tshark)
	network and system metrics DOT (Cadvisor + Prometheus)
	Telemetry aggregation & normalisation DOT
Earlier-Predictive Attack Detection	Supervised classification DOT (Random Forest)
Enforcement & Automated Mitigation	Mitigation recommendation DOT (Smart Recommender)
	Firewall enforcement DOT (arp/ iptables / netfilter).
	Pre-assessment & SLA validation DOT

Workflow



Validation strategy (KPIs)

Anomaly Detection Rate

Percentage of tampered or spoofed DNS traffic correctly classified as anomalous by the AI-based detection Security Function.

-**Target Value:** $\geq 85\%$

-**Success Threshold:** $\geq 80\%$

-**Measurement Method:** Comparison between labelled attack datasets and model outputs using confusion matrix analysis.

Mean Detection Time

Average time required to detect an ongoing MitM DNS spoofing attack after its initiation.

-**Target Value:** < 1 minute

-**Success Threshold:** < 2 minutes

- **Measurement Method:** Time elapsed between attack injection and alert generation.

Mitigation Deployment Time

Time required to activate the Enforcement Security Function after attack detection.

-**Target Value:** < 30 seconds

-**Success Threshold:** < 1 minute

-**Measurement Method:** Time elapsed between alert generation and enforcement activation.

Additional KPIs addressed by this PoC

- KPI-4: False Positive Rate: $\leq 5\%$
- KPI-5 False Negative Rate: $\leq 2\%$
- KPI-6: Attack Mitigation Success Rate: $\geq 95\%$
- KPI-7 – Service Continuity: $\geq 95\%$
- KPI-8 – Monitoring Coverage: 100% of relevant infrastructure and traffic flows monitored.

Future Work

The following steps to implement are:

- Create an ML model capable of predicting the attack.
- Verify the effectiveness of the SFs through PASTE.
- Improve the detection model KPIs.
- Incorporate intelligence into the ASPO models to support decision-making.

Thank you

Follow us

#MARE6G_EU



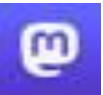
@MARE_EUProject



@MARE_EUProject



@MARE_EUProject



@MARE_EUProject@eupolicy.social