Reti radiomobili 5/6G - sfide e opportunità per la sicurezza

April 07, 2025

Giuseppe Bianchi

Professor, University of Roma Tor Vergata
Director, National CNIT Network Assurance & Monitoring LAB

CNIT

➔ **CNIT = Consorzio Nazionale Interuniversitario per le Telecomunicazioni**

- ⇨ Non-profit
- ⇨ from 1995
- ⇨ Legal Entity recognized by MIUR and supervised by MEF

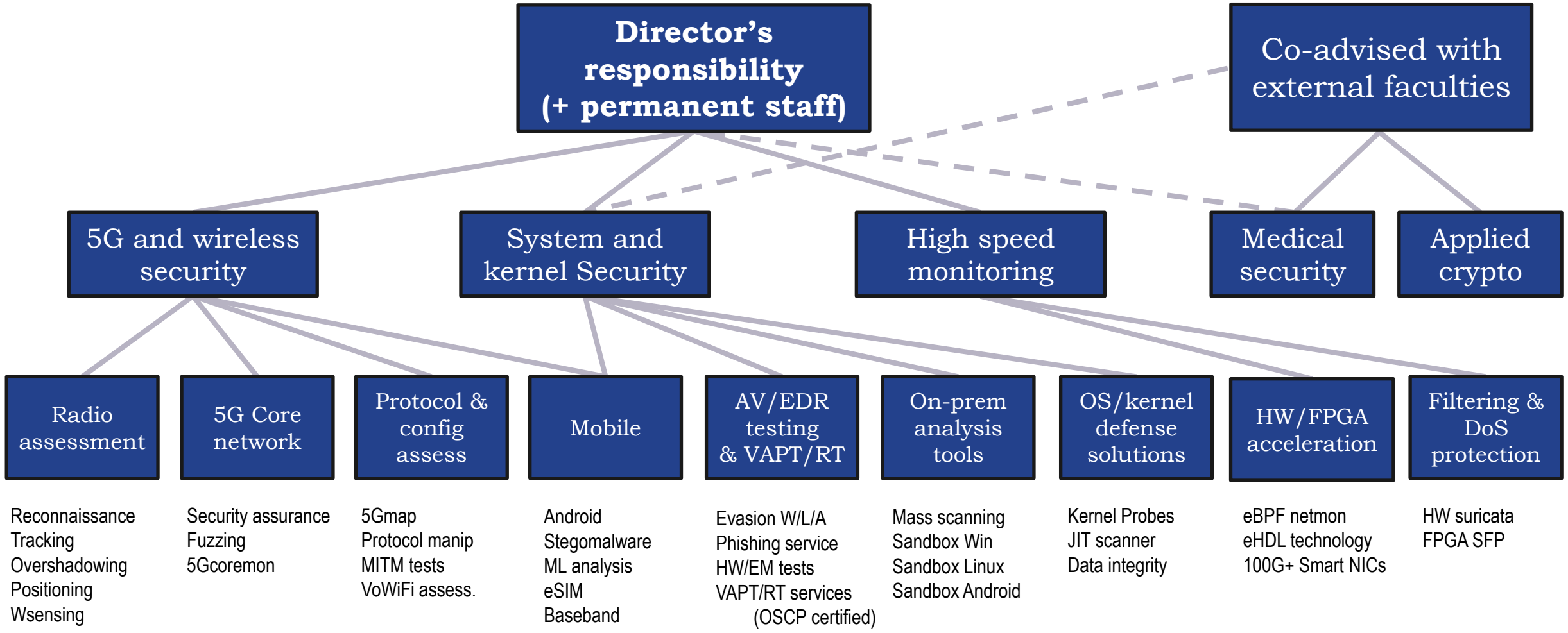
➔ **49 research units (41 universities + 8 CNR institutes)**

- ⇨ **1300+ affiliates**, **100+ employees**
- ⇨ 8 national labs (GE, BO, PIx2, AQ, NA, RM2, CT+PA)

➔ **Natl LAB on Network Assurance and Monitoring**

- ⇨ **Launched on nov 2022, current site in Tor Vergata**
- ⇨ **About 30 collaborators (6 of which permanent)**
- ⇨ **Charter: <u>security of networked systems</u>**

Areas


Director's responsibility (+ permanent staff)
Co-advised with external faculties
5G and wireless security
System and kernel Security
High speed monitoring
Medical security
Applied crypto
Radio assessment
5G Core network
Protocol & config assess
Mobile
AV/EDR testing & VAPT/RT
On-prem analysis tools
OS/kernel defense solutions
HW/FPGA acceleration
Filtering & DoS protection
Reconnaissance
Tracking
Overshadowing
Positioning
Wsensing
Security assurance
Fuzzing
5Gcoremon
5Gmap
Protocol manip
MITM tests
VoWiFi assess.
Android
Stegomalware
ML analysis
eSIM
Baseband
Evasion W/L/A
Phishing service
HW/EM tests
VAPT/RT services
(OSCP certified)
Mass scanning
Sandbox Win
Sandbox Linux
Sandbox Android
Kernel Probes
JIT scanner
Data integrity
eBPF netmon
eHDL technology
100G+ Smart NICs
HW suricata
FPGA SFP

5G+ networks are VERY complex

Improved mgmt of Network Access Security (AMF vs SEAF)

Security & Access control for interconnection traffic

Auth home control; User Identity deconcealment

Careful credential mgmt

non3GPP access

N3IWF

L2 integrity

AMF

SEAF

SEPP

SEPP

AUSF

SIDF

ARPF

UDM

UDR

DU

CU

gNB

Serving network

Security Assurance for NFV

Home network

Improved key derivation → several different levels of trust (trust domains)

DU Distributed Unit
CU Central Unit

N3IWF Non 3GPP Inter Working Function

AMF Access Management Function
SEAF SEcurity Anchor Function

SEPP Security Edge Protection Proxy

AUSF AUthentication Server Function
SIDF Subscription Identifier Deconcealment Fct
ARPF Auth credential Repository & Processing Fct
UDM Unified Data Management
UDR Unified Data Repository

5G+ networks are VERY complex

Improved mgmt of Network Access Security (AMF vs SEAF)

Auth home control; User Identity deconcealment

Careful credential mgmt

non3GPP access

N3IWF

ARPF

UDR

gNB

5G+ security solution design: a necessary (but largely insufficient) pre-condition!

Many issues still to face ☹

DU Distributed Unit
CU Central Unit

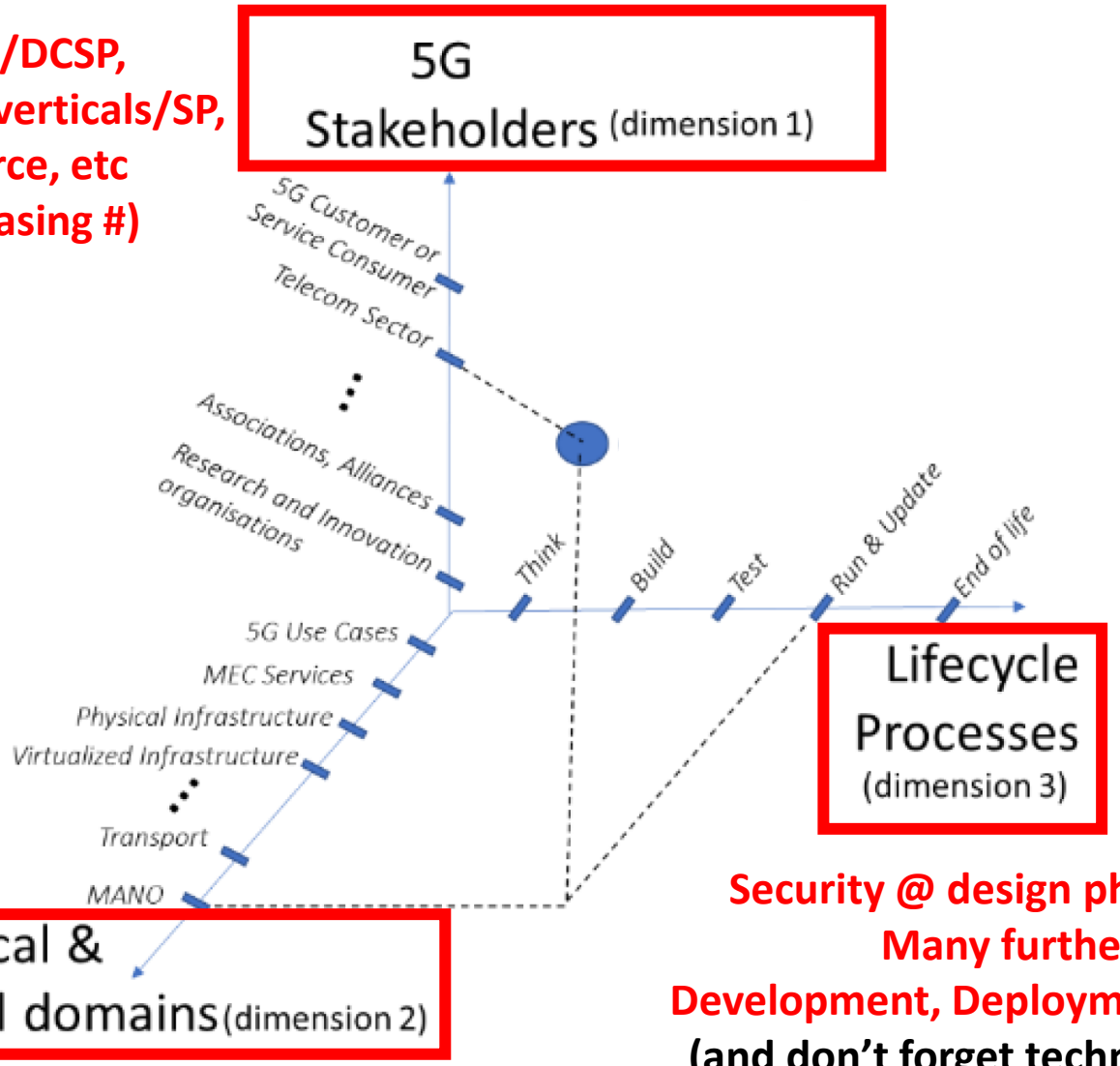
Access Management Function
SEAF SEcurity Anchor Function

N3IWF Non 3GPP Inter Working Function
SEPP Security Edge Protection Proxy

rver Function
fier Deconcealment Fct
ository & Processing Fct
UDM Unified Data Management
UDR Unified Data Repository

Issue #1: Increased threat surface!

TLC, cloud/DCSP,
policy makers, verticals/SP,
open source, etc
(Ever increasing #)



Heterogeneous technologies
Increased threat surface
Decentralization / edge computing

Security @ design phase not nearly enough;
Many further crucial phases:
Development, Deployment, Integration & testing…
(and don't forget technology decommissioning!)

Issue #2: broad range of risks

Technical

Geo-political

societal

Cascade effects

	Risk categories
Risk scenarios related to insufficient security measures	R1: Misconfiguration of networks R2: Lack of access controls
Risk scenarios related to 5G supply chain	R3: Low product quality R4: Dependency on any single supplier within individual networks or lack of diversity on nation-wide basis
Risk scenarios related to modus operandi of main threat actors	R5: State interference through 5G supply chain R6: Exploitation of 5G networks by organised crime or Organised crime group targeting end-users
Risk scenarios related to interdependencies between 5G networks and other critical systems	R7: Significant disruption of critical infrastructures or services R8: Massive failure of networks due to interruption of electricity supply or other support systems
Risk scenarios related to end user devices	R9: IoT (Internet of Things) exploitation

Issue #3: Too early implementations?

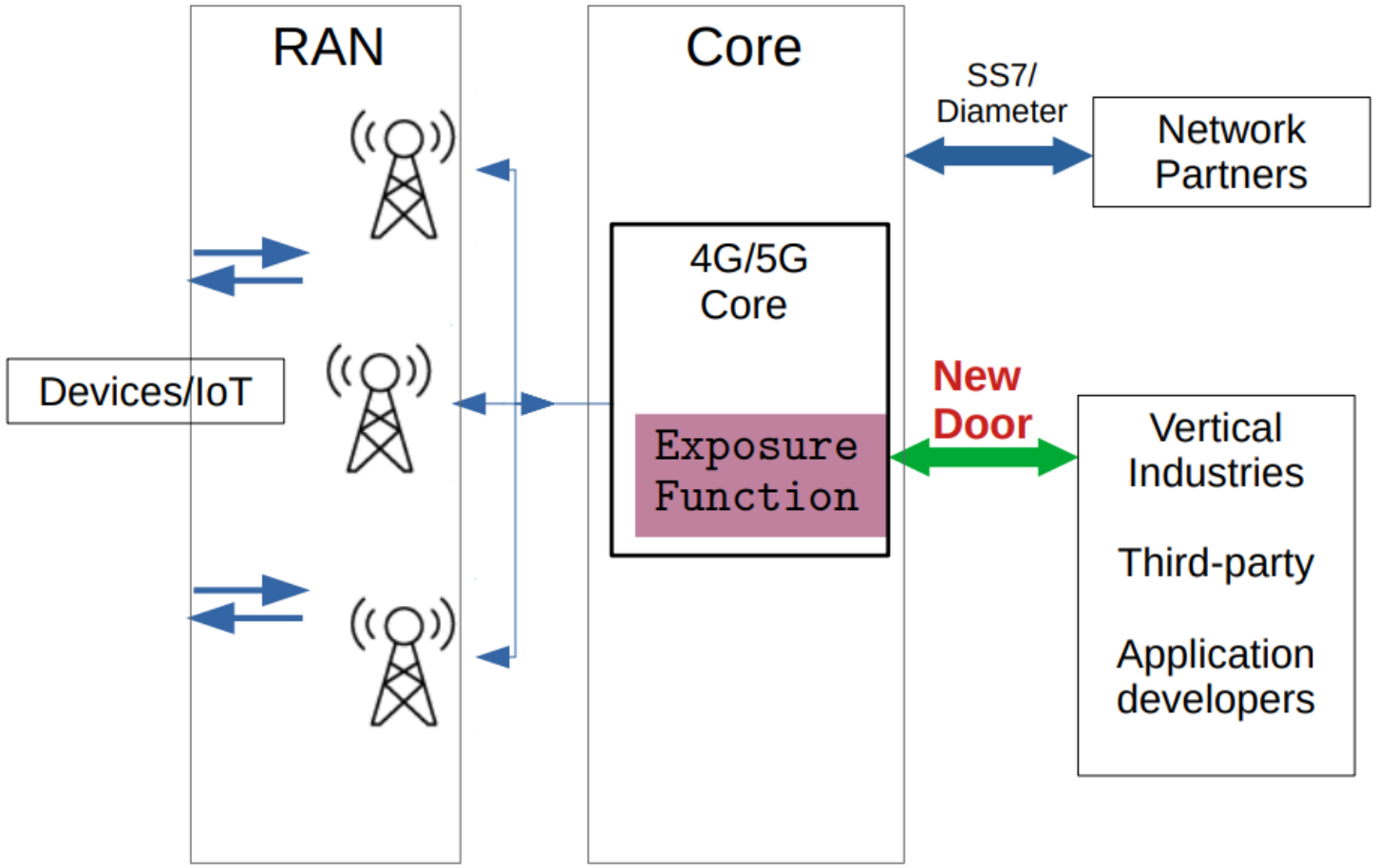
Attacks from a New Front Door
in 4G & 5G
mobile networks

Dr. Altaf Shaik & Shinjo Park

TU Berlin
& FastIoT

Blackhat USA 2022

New front door: exposure function



Issue #3: too early implementations?

Summary of security analysis

- Oauth and TLS is used in majority of platform (5/9) but not all of them.
- Only 2 out of 9 IoT platforms are not affected with serious vulnerabilities and API risks
- IMSI is exposed outside of 3GPP network, same practice may apply for 5G IMSI (SUPI)
- Lack of rate-limits, strong password policies
- Internal software information and core network IP addresses are exposed
- Authorization vulnerability can destroy the IoT devices and the network
- Script/code injection vulnerability found in many platforms, and is missed when a internal pen-testing
- SMS and IP content inspection is not present in mobile and IoT networks
- Attacker can easily obtain access to IoT service platforms and service APIs with forged identity

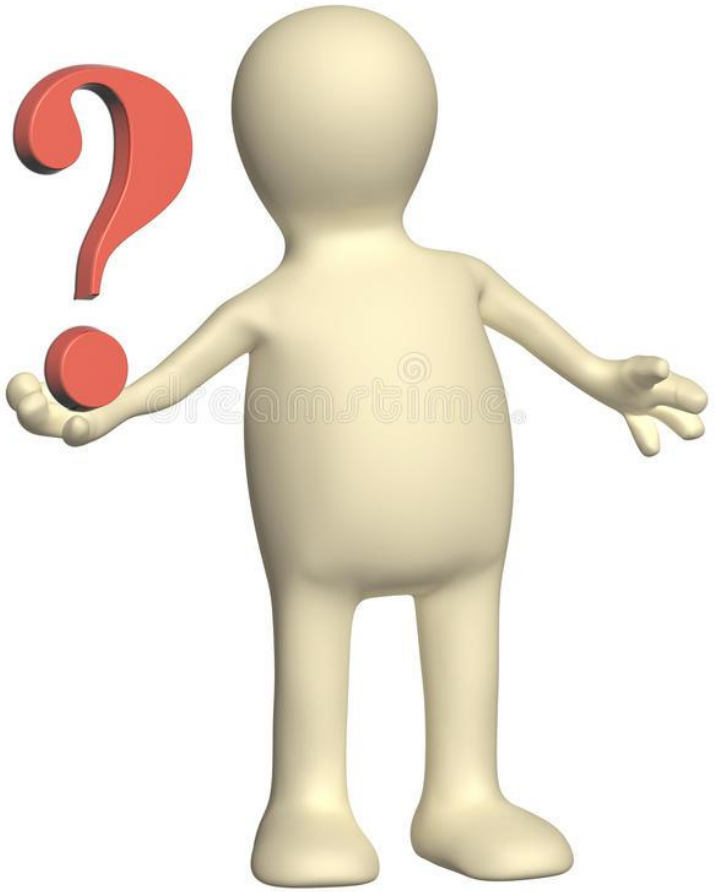
We're talking about PRODUCTION platforms!

Issue #4: configuration «options»

- **Is IMSI/SUPI protection ON?**
- **Is Integrity ON?**
  - **Just on control plane or also on data?**
- **Is certificate enrolment (TS 33.310) supported by gNB? Secure boot? …**
- *… very long list follows…*

To what extent? An example…

- **Requirement**: "The gNB **shall support confidentiality, integrity and replay protection** on the gNB DU-CU F1-U interface for user plane".
- Then **a NOTE** (!) says: "The above requirements allow to have F1-U **protected differently (including turning integrity and/or encryption off or on for F1-U)** from all other traffic on the CU-DU (e.g. the traffic over F1-C)".



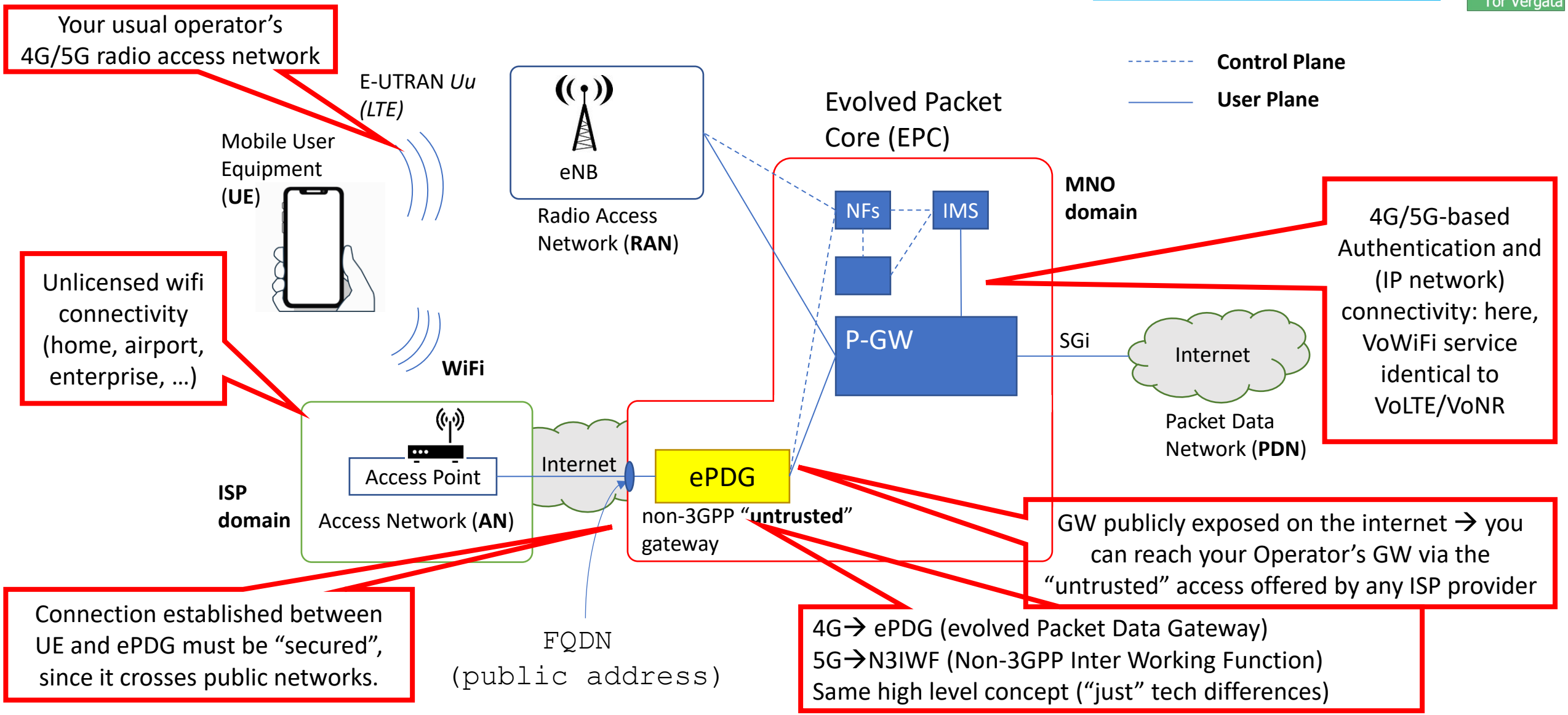
Any compelling evidence of (blatant) real world misconfiguration?

Yes, let's peek at two of our recent experiments:

1. VoWiFi security checking in real world networks
2. 5Gmap: Encryption/integrity checking in real world networks

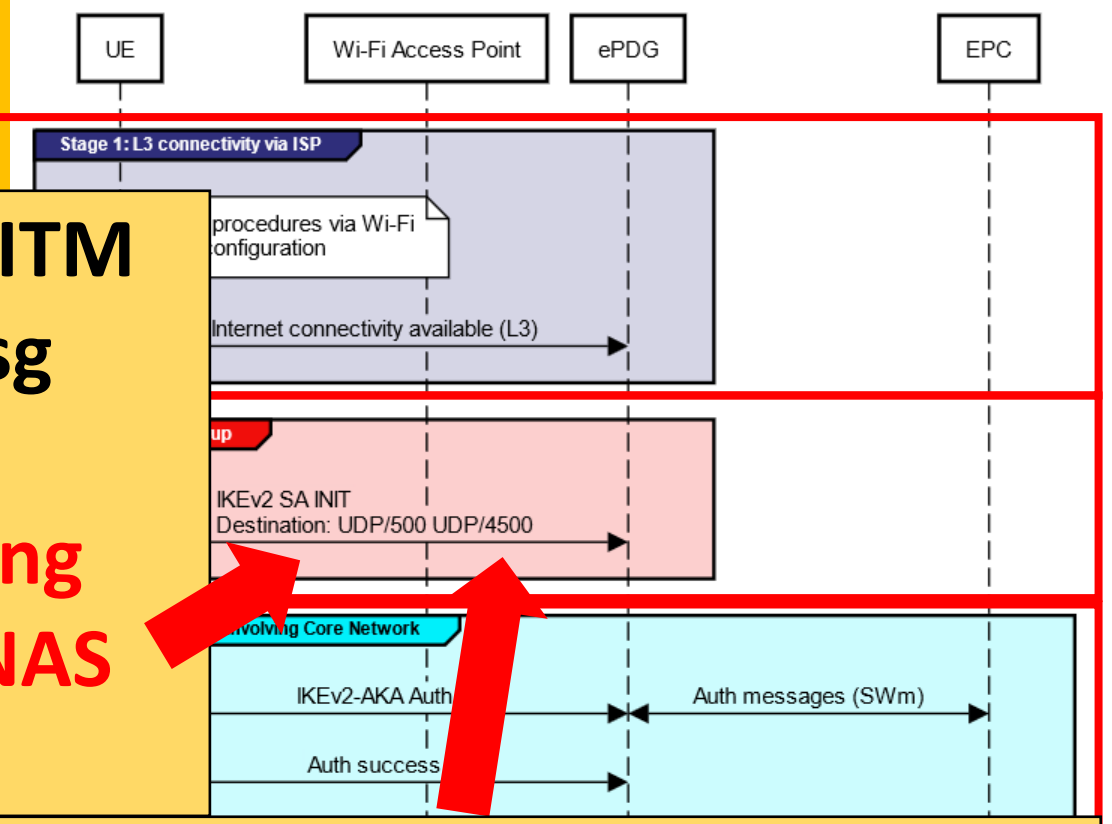
Both with an end user perspective – no access to network internals!

WoWiFi – how does it work?



Giuseppe Bianchi - Professor, Networking & Network Security, Univ. Roma «Tor Vergata» - **Director, CNIT Network Assurance and Monitoring National LAB**

VoWiFi/4G procedures at a glance



Our Result #2 (in progress): obvious MITM on anonDH → access to pre-auth msg

Massive IMSI catching

Potential for DoS, downgrade, spoofing attacks, eavesdropping unencrypted NAS (see next slide!)

USIM/eSIM secr

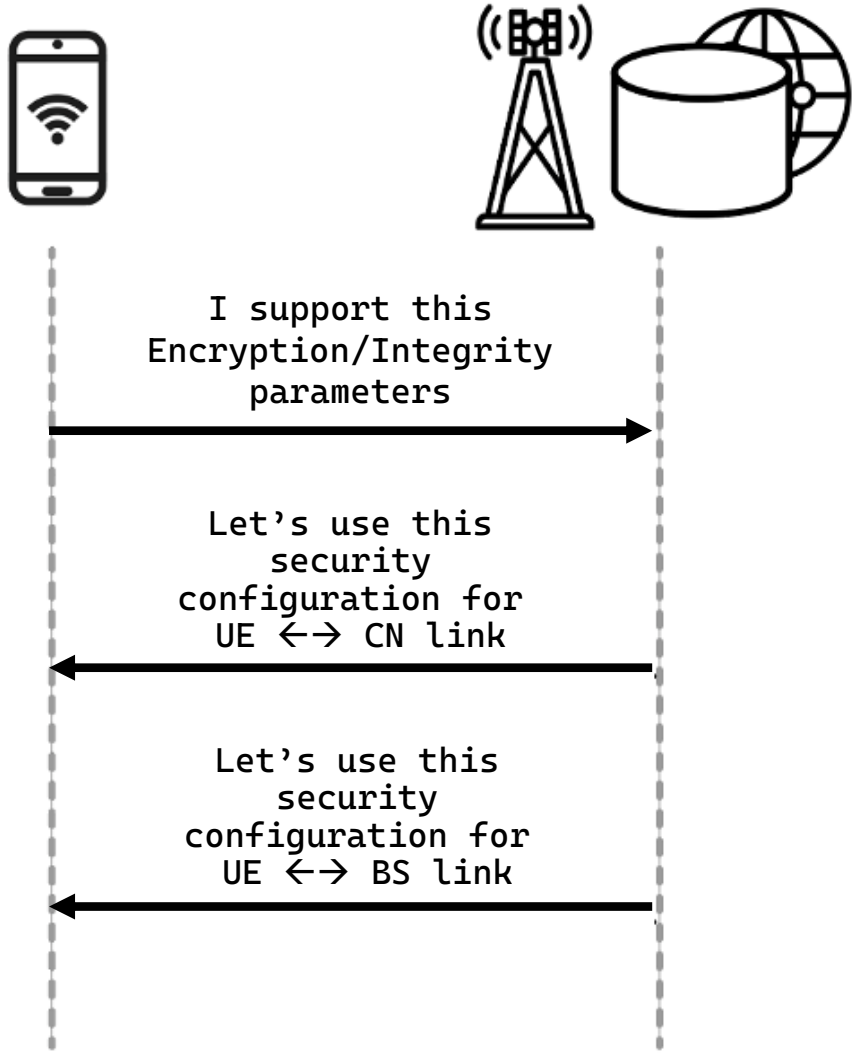
- Stage 4: IPSec tur
  - Only at this stag
    "3GPP-authenti
- Stage 5: use valid
  - VoWiFi (vendor

Our Result #1: tests in the wild on 2523 MNOs

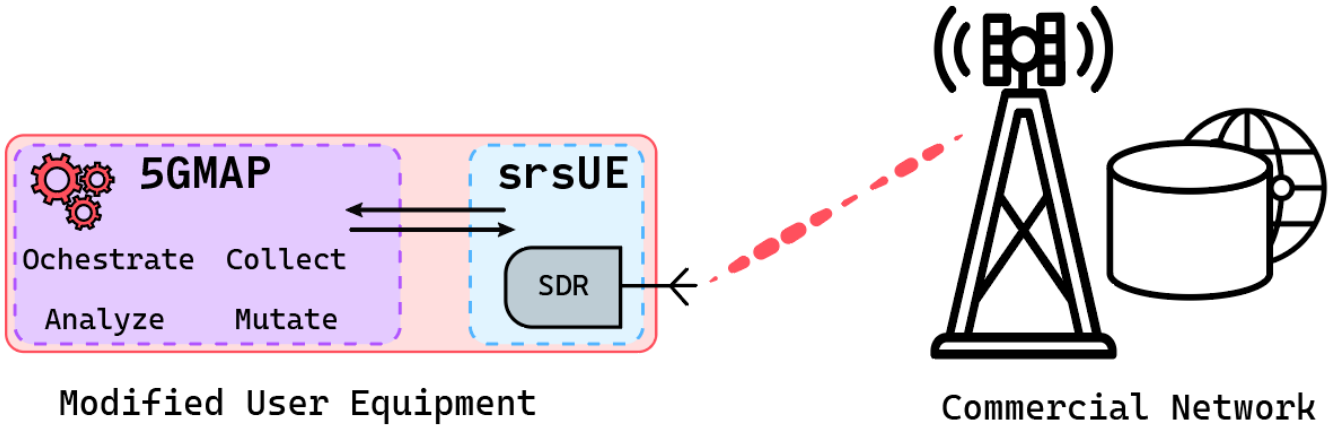
detailed crypto configuration profiling of 340 responding ePDGs → weak algorithms' support!

- **DH groups** →more than 30% accept DH groups smaller than 2048 bits
- **Symmetric enc** → DES and 3-DES encryption in almost 20% ePDGs (DES=7%)
- **Integrity, PRF** → HMAC-MD5 in almost 20% ePDGs
- **Cookie defense** → only in 8 ePDGs (out of 695)

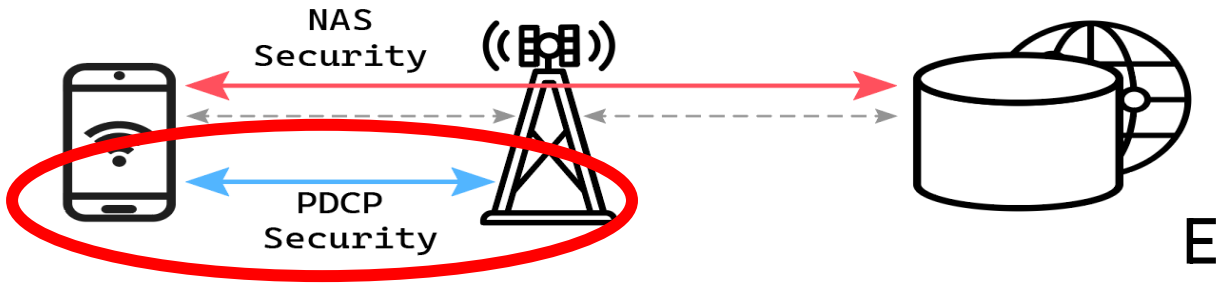
5Gmap: empower end users with means to test MNO protection configs



- **Methodology:**
  - Propose ONE config at a time
  - By iterating on all possible configs, we profile the operator's encryption & integrity configuration



Result #1: potential for downgrade!



BS (PDCP) Algorithms

Encryption Algorithms

	NONE	EEA1	EEA2	EEA3
Operator 1	✓	✓	✓	
Operator 2	✓	✓	✓	
Operator 3		✓	✓	

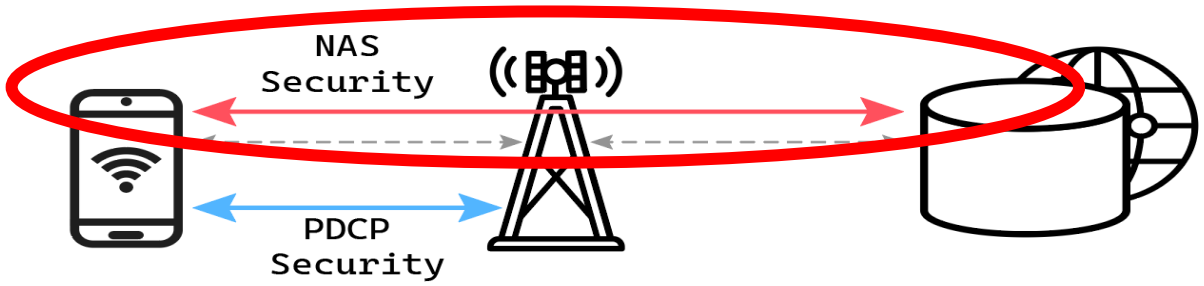
Integrity Algorithms

	NONE	EIA1	EIA2	EIA3
Operator 1		✓	✓	
Operator 2		✓	✓	
Operator 3		✓	✓	

Legend

- ○ Preferred Algorithms
- ✓ Supported algorithm

Result #2: some «forgot» NAS encryption!!



Core network (NAS) Algorithms

Encryption Algorithms

	NONE	EEA1	EEA2	EEA3
Operator 1	✓			
Operator 2	✓			
Operator 3		✓	✓	

Integrity Algorithms

	NONE	EIA1	EIA2	EIA3
Operator 1		✓	✓	
Operator 2		✓	✓	
Operator 3		✓	✓	

Legend

- ○ Preferred Algorithms
- ✓ Supported algorithm

Giuseppe Bianchi - Professor, Networking & Network Security, Univ. Roma «Tor Vergata» - **Director, CNIT Network Assurance and Monitoring National LAB**

Updated results

CRITICAL! NO ENCRYPTION ON PDCP

Table 2: **AS supported algorithms (Attach with IMSI).**

	Algo	Mno1	Mno2	Mno3	Mno4	Mvno1	Mvno2	Mvno3
eNB Cipher Algo	EEA0			✓	✓		✓	
	EEA1	✓✓	✓	✓	✓✓	✓	✓✓	✓✓
	EEA2	✓	✓✓	✓✓	✓	✓✓	✓	✓
	EEA3							
eNB Integ Algo	EIA0							
	EIA1	✓✓	✓	✓	✓	✓	✓	✓✓
	EIA2	✓	✓✓	✓✓	✓✓	✓✓	✓✓	✓
	EIA3							
gNB Cipher Algo	NEA0			✓			*	
	NEA1	✓✓	✓	✓	✓	✓	*	✓✓
	NEA2	✓	✓✓	✓✓	✓✓	✓✓	*	✓
	NEA3						*	
gNB Integ Algo	NIA0	✓✓		✓✓	✓✓		*	✓✓
	NIA1		✓			✓	*	
	NIA2		✓✓			✓✓	*	
	NIA3						*	

Supported ✓, Preferred ✓✓

* 5G not available.

CRITICAL! STILL NO ENCRYPTION Even With 5G

Updated results

One operator has fixed the issue after disclosure

EVEN MORE CRITICAL!
NO ENCRYPTION EVEN POSSIBLE
ON NAS

Table 4: **NAS supported algorithms.**

	Algo	Mno1	Mno2	Mno3	Mno4	Mvno1	Mvno2	Mvno3
EPC Cipher Algo	EEA0			✓	✓		✓	
	EEA1	✓	✓			✓		✓
	EEA2	✓	✓		✓	✓		✓
	EEA3							
EPC Integ Algo	EIA0							
	EIA1	✓	✓	✓	✓	✓	✓	✓
	EIA2	✓	✓	✓	✓	✓	✓	✓
	EIA3							

Supported ✓, Preferred ✓

So, what should we mostly focus on?

- 6G security standardization? Yes, though starting point already very good
  - But worth to underline:
    - PHY sensing → privacy! Need for more compelling solutions here
    - migration to Post Quantum Crypto → mainly operational but… will be an issue!!

- Configuration Security & Visibility Gaps
  - **Main concern in today's talk!** Operators/Vendors may struggle with configuration intricacies.

- API attacks surging (Telcos often lack expertise in API security, see Exposure Function ☹)

- Supply chain security concerns (and nation-state threats)
  - **Dependence on Foreign Tech**
  - **open source risks** (see XZ-Utils backdoor as a trailblazing example)
  - **Plenty of old code in TLC** (Java applets in eSIM: were you aware?)
  - **inherited vulnerabilities via SW dependencies**…
    - Current official O-RAN RIC implementation: 792 vulnerabilities (of which 16 critical) [netsoft 2024]

Thank you!

Giuseppe.Bianchi@uniroma2.it

Giuseppe Bianchi
CNIT NAM Lab, director
Professor of Networking & Network Security
University of Roma «Tor Vergata»