Real-World 5G Security Challenges & Operational Strategies

Rémy Harel
Orange

Thanks for their contributions
Stéphane Gorse
Franck Vauthier

C&ESAR 2025 by DGA

32nd Computer & Electronics Security Application Rendezvous

19 - 20
Nov 2025

Rennes
France

5G is not « 4G+1 »

5G is not just a mobile network, it is a critical backbone for life use cases.
5G is not just an evolution of 4G (LTE) but a real revolution that will become the foundation of our economies and societies.

Business reality is clear: business and residential customers wants today to access their services “**anywhere anyway (device) and anyday**.” And with more demand for condientiality.

Direct consequence : attack surface widens
With billions of IoT, complex virtualized network with massive interconnections. The attack surface is expanding dramatically

5G didn't emerge alone. It's part of a **revolutionary ecosystem** that includes **AI**, **virtualization**, **Edge Computing**, and the automation revolution—all **transforming our digital landscape simultaneously**

5G was born into a **turbulent geopolitical era** and now faces cyber threats of **unprecedented scale** and **sophistication**

orange™

5G is transforming the very fabric of our digital lives.
Security isn't just important—it's the cornerstone of adoption, trust, and success.

Telco operators are targets

Image: www.freepik.com

Nord Net (24 février 2022)
(https://ec.europa.eu/newsroom/cipr/items/740427/en)
(Satellite solution) Flash of modem firmwares to kill them (not recoverable)
Several dozen of thousands devices to replace.

Vodafone Portugal (07 février 2022)
(https://www.vodafone.pt/en/press-releases/2022/2/cyberattack-on-vodafone-portugal.html)
Major compromission of the mobile network, with an interesting origin: social engineering
Major impact : 4.7M mobile subscribers without service, 1M landlines down, as well as SMS, TV, customer support…

AT&T, Verizon, Lumen, DoD (2021-2025)
(https://www.congress.gov/crs-product/IF12798)
Deep and major infiltration…but very stealthy and last years.
Spying and confidentiality breach, including lawful interception systems.

SKT télécom (découvert 18 avril 2025)
(https://www.koreaherald.com/article/10563945)
Authentication (HSS) solution compromised (by malware), with 23 million SIM cards to replace.
SKT was fined by the authorities for $97.2M. SKT lost 800,000 subscribers and estimated loss…in billions.

Telco operators and their networks are the direct – or indirect – targets of powerful forces motivated by spying, infiltration and disruption…

Europe, **a strict and evolving landscape**

In **Europe** 🇪🇺 the **NIS2 directive** significantly strengthens cybersecurity requirements for telecommunications operators, classified as essential entities.

The **Cyber Resilience Act** drastically reinforces requirements for vendors and system integrators.
There are many regulations to comply to in Europe, e.g. on personal data (GDPR), AI (IA act), …

In **France** 🇫🇷 **ANSSI** (National Agency for Information Systems Security) sets very high standards and conducts regular audits in Vendors or Operators premises.

The **L34-11 law**, known as the '5G law,' mandates extremely high security levels to operate 5G networks in France

orange™

The regulations in Europe set the expected level of security from Telco networks very high.
Companies and executives are accountable for the security of their networks

Virtualization : cornerstone for modern networks

Image: www.freepik.com

The « 5G+ » (5G SA) mobile network core is **entirely virtualized** (no physical NF: containers or VMs).

New radio network generations, like **Open RAN**, are also available as **virtualized** solutions.

Security wise, **virtualization** brings **opportunities** as well as **challenges**.

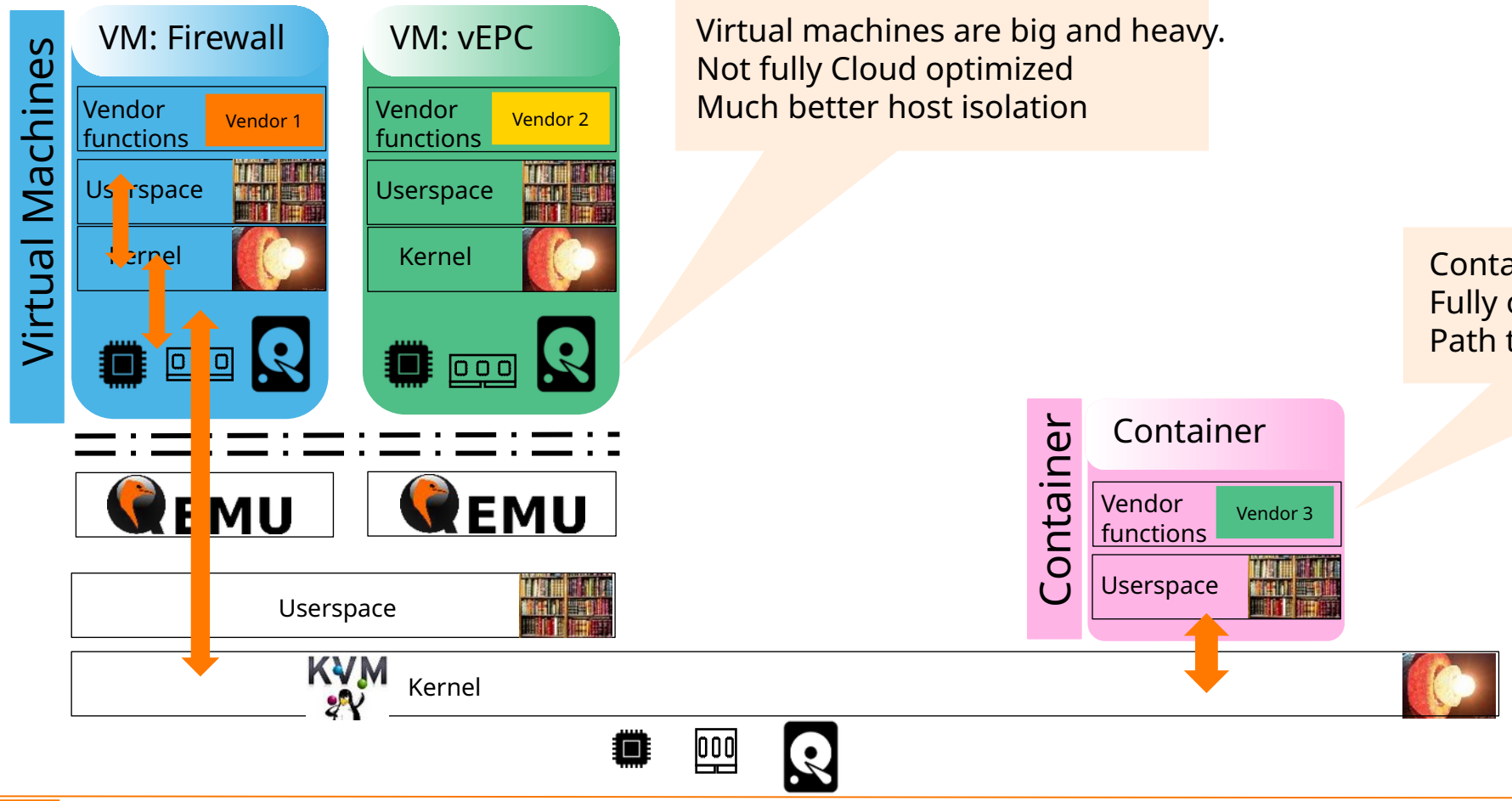
As opportunities, we can :

- increase the compute resources of the security functions
- We can instantiate new security functions on demand

Modern Telco networks are composed today of a mix of legacy physical functions, containers and virtual machines.
Telco operators have to ensure security of all virtualized technologies.

Architecture of containers vs VMs

Image: www.freepik.com



Virtual machines are big and heavy.
Not fully Cloud optimized
Much better host isolation

Containers are small and fast
Fully optimized for Cloud
Path to host is much more direct

Containers are smaller, lighter and faster...but require more attention, security wise. They are quite popular since they offer better performance and are Cloud Native (scaling, automation, ...)

Virtualization : cornerstone for modern networks

Image: www.freepik.com

A **container escape** or a **VM escape** can have major consequences (global shutdown) if the **mutualization** is too massive.

→ But the mutualization is what allows Operators to leverage the advantages of virtualization.

Isolation and **tight sealing** are crucial to avoid access to host.

Kubernetes security is achieved by deploying several configuration steps, such as:

- Use only secure image *(scanned & including supply chain checks)*
- **pods** configuration hardened and exclude root execution
- Strong **RBAC policy**; access rights and privileges is crucial
- Set-up strong **network policies** *(deny all, allow only what is needed)*
- Set-up **Log & Monitoring**
- Use a **Vault** or a secure storage to manage **keys**, **secrets** and **certificates**

orange™

As for 5G and 3GPP options, it is crucial to finely tune the configuration of virtualized networks to exploit their full potential without putting at risk the network.

Standards and evolutions from previous gen.

GSMA, NGMN, 3GPP, …

The whole industry (including Orange) started to work on 5G security since the conception of 5G (NGMN, GSMA, 3GPP, …).

5G is the **first mobile network generation actually Secured By Design**.

The weaknesses of previous generations have been fixed, and several new mechanisms emerged.

Among these mechanisms: **Strong & central mutual authentication** (*the network authenticates the device and the device also authenticates the network*), **Massive encryption** of communications, **User identity protection** (the famous SUCI)

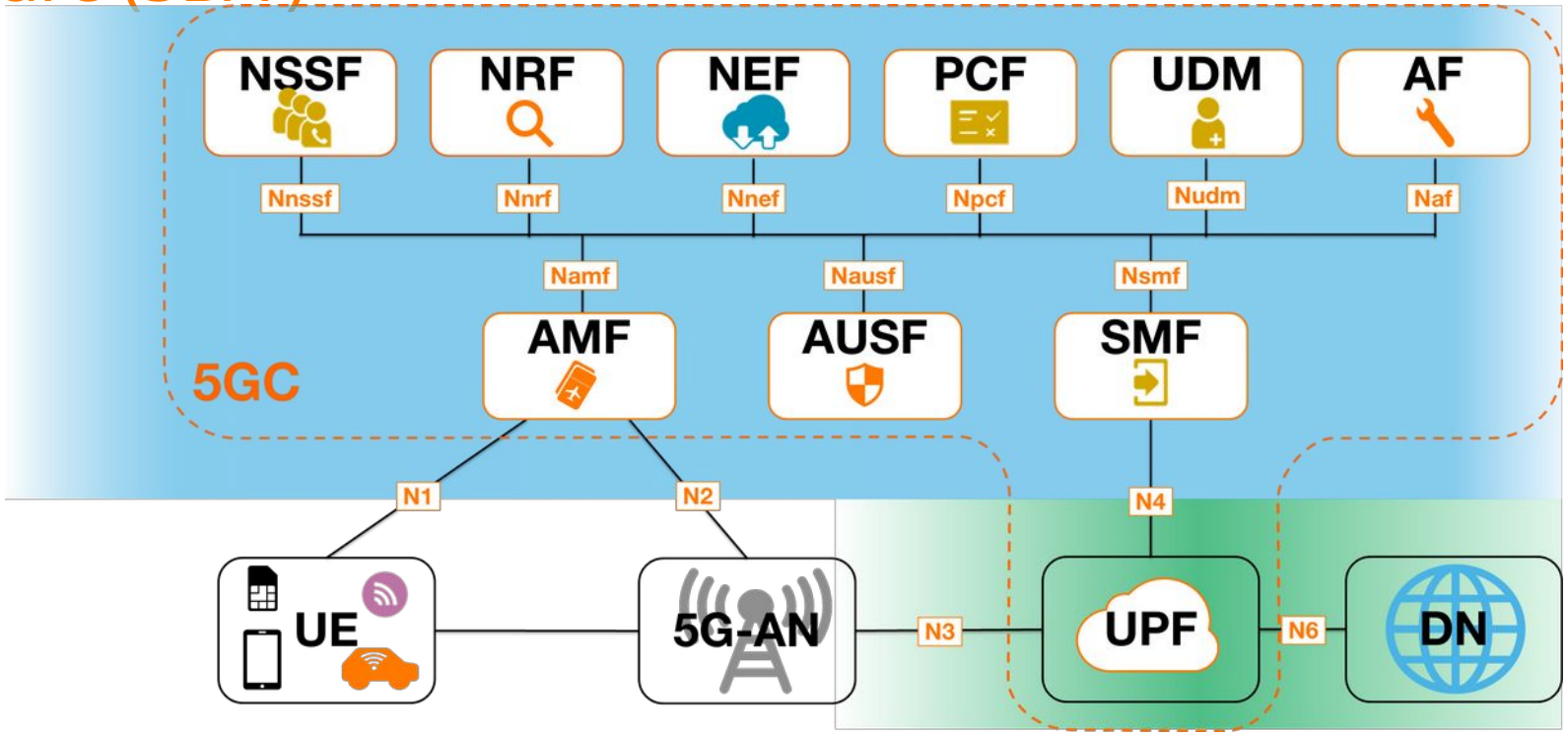
User plan integrity protection on the air interface is also a major step forward, as well as the Software Based Architecture.

With 5G, the security was at the heart of the conception of this new mobile network generation. It was a strong and collective effort from the Telco Industry

Software Base Architecture (SBA)

5G SA replaced Telco protocols (e.g. Diameter) for intra communications by **IT protocols**.

This architecture, called SBA, leverages multiple protocols to ensure the **security of internals communications**.

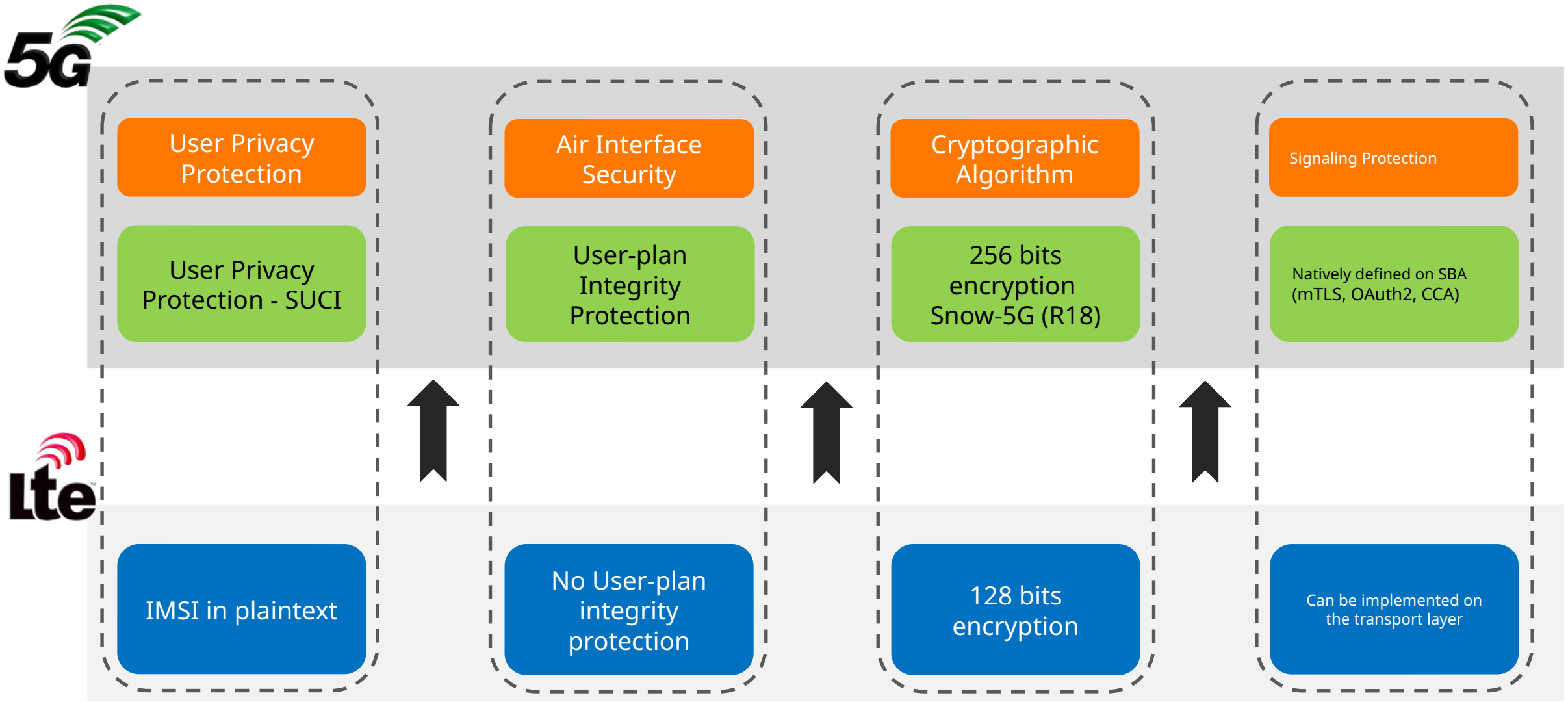


- API based with NF consumer and NF producer
- HTTP/2 with REST
- Authentication based on certificates X.509, optionally with Client Credentials Assertion (CCA)
- Confidentiality with TLS
- Authorization based on OAuth2

AF	Application Function
AMF	Access Management Function
AUSF	Authentication Server Function
DN	Data Network
NEF	Network Exposure Function
NRF	Network Repository Function
NSSF	Network Slice Selection Function
PCF	Policy Charging Function
RAN	Radio Access Network
SBA	Service Based Architecture
SMF	Session Management Function
UDM	Unified Data Management
UE	User Equipment
UPF	User-Plane Function

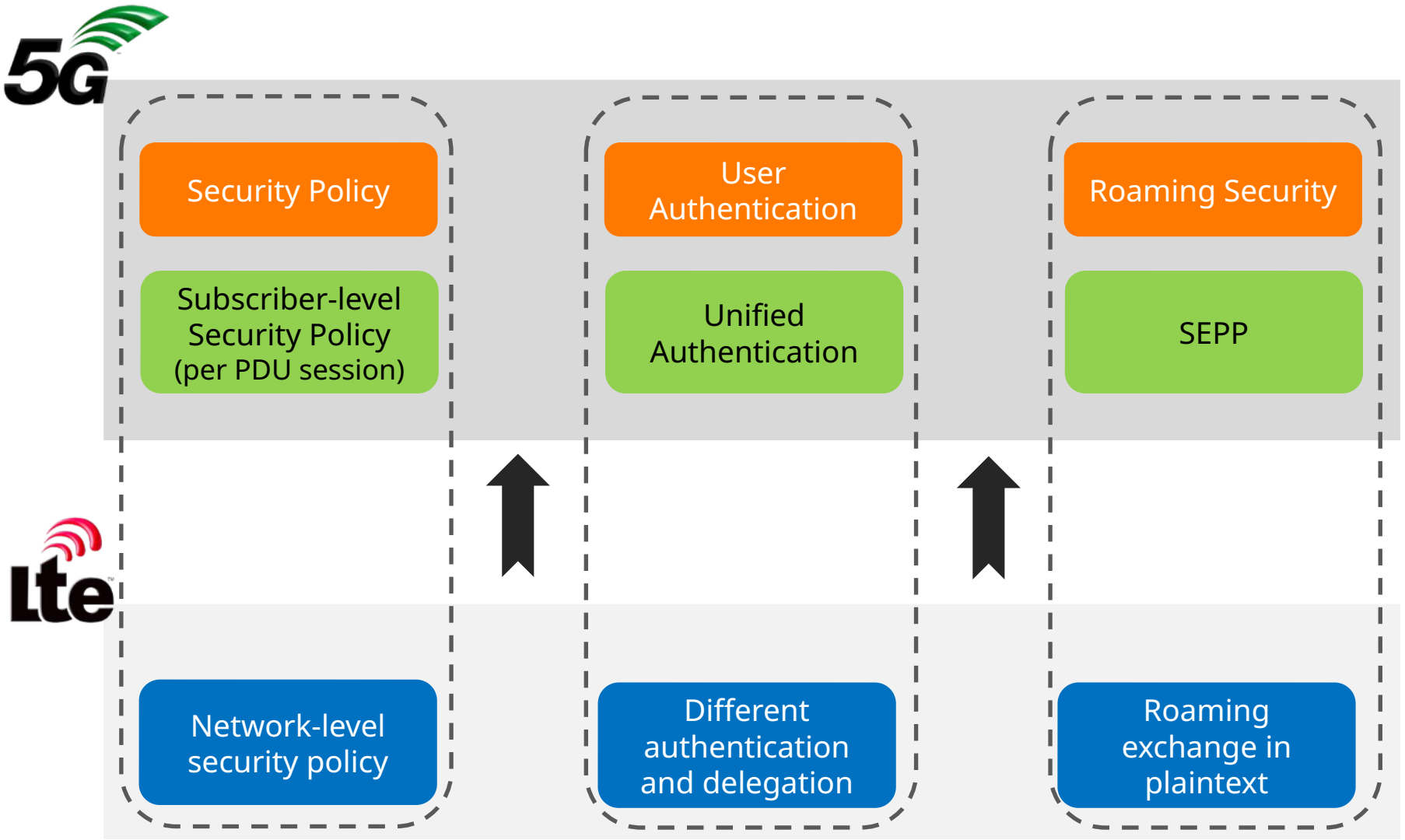
IMSI International Mobile Subscriber Identity
SUCI SUbscription Concealed Identity

Main 5G security improvements over LTE



PDU Packet Data Unit
SEPP Security Edge Protection Proxy

Main 5G security improvements over LTE



Classics still rule

If advanced security mechanisms and sophisticated attacks shine in discussions,
=> we tend to **overlook the basics!**

A lot of security problems today come from **weak passwords** or **uninstalled security patches**.

Hardening and **segregation** strongly limits the **lateralization** possibilities.

A **security in depth** approach reduces significantly the spreading of the attack…

…while **logs** and **monitoring** trigger **alarms** so security teams can react

Inventory is also not to be overlooked, especially to avoid **ghost servers**

orange™

Do not forget attackers will always take the easiest path!
It is pointless (and a waste of money) to deploy advanced security features if the basic security hygiene rules are not applied

The supply chain is a critical link

Image: www.freepik.com

A **supply chain attack** consists in hacking a third party of the target to reach this target, instead of targeting directly the main target.

These attacks often allow to reach **highly secured targets** by targeting **providers** with a **lower security level**

In some cases, these attacks can create **collateral damage** (e.g. SolarWinds attack)

To secure the supply chain, we use a combination of several actions:

- **Signature** of deliverables (e.g. images) and **strong authentication** of the supply source
- Deliverables are thoroughly analysed: **SBOM** generation, checking of signature, **vulnerability scanners**
- **Remediations plans** and **fixes** required for each problem detected
- **In critical case or doubt on the supply chain, refusal of the deliverables**

It is also interesting to note that the **GSMA NESAS** group worked on the security of the supply chain.
NIS2 directive and **CRA** make the security of the supply chain mandatory.

The attacks on the supply chain are more and more sophisticated and can be very difficult to counter or avoid.
Not only it requires a high level of security, it also requires very strict policies and processes.

Security is a choice

During sourcing of 5G solutions (vendors), security is a top priority in questions and vendor selection.
A lot of security features in 5G come as **options (3GPP)**, so it is important to **identify what we require**.

We also define a strong contractual framework **to commit and make accountable vendors on the security of their products (in the spirit of CRA and NIS2).**

When we receive the first deliverables, we start to generate SBOM, vulnerability scans, image signature checks…

The 5G solutions are then thoroughly checked in **Orange Innovation labs** prior to deployment

Regular exchanges with Vendor to discuss solution weaknesses, **Security reviews** are regularly held with main vendors. Major problems are **considered at exec level** to guarantee the best remediation path.

The Telco industry designed the **5G since the beginning with security in mind.**
To go even further, at Orange from picky vendor selection to intensive testing of software and hardware, each step is controlled and subject to verification.

Thorough validations in Labs

Upon delivery of a new version of a Network Function, **several tests are done** (following supply chain tests)

Hardening is checked: rights, unused software, unsecure protocols, …

Vulnerability scanners are triggered to ensure we do not have critical or major vulnerability in our networks

Secrets are also check, in binaries and plaintext files, to avoid for example **hardcoded password.**

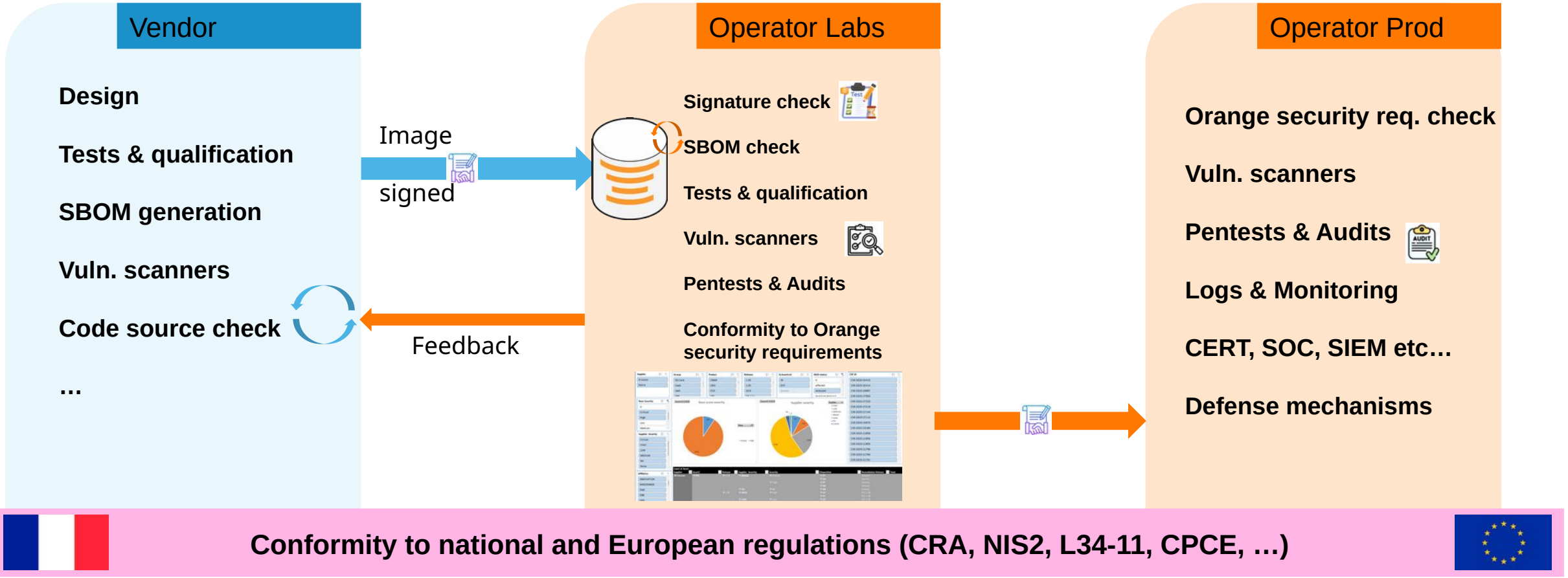
Functional tests (including security mechanisms) to ensure the NF behaves as expected

For each problem, we open **tickets** for support and request **remediation plans** (according to **SLA**)

For all risks we could not eliminate before deployment, the **security teams on field** are **notified of the risks** and mitigation actions are proposed.

The Labs (e.g. *Orange Innovation*) are a crucial step to ensure the security of networks. It acts as a filter: from strict selection of Vendors to security audits and controls, it allows to evaluate if the security level is good enough to go live.

Securing Telco networks



The Telco network and infrastructures security start with security from the Vendors.
A key and strategic step happens in Labs and preprods where security is thoroughly checked.
On the field, regular controls, audits and monitoring are crucial.

Secure does not mean simpler

In 5G, the **number of certificates exploded**. Encryption and Authentication is a great security addition….

…but the certificates management is a **nightmare**. **Automation is mandatory**.

A mishandling of a certificate can lead to a **denial of service** that would make hackers jealous ☺

The Telco Industry chose **CMPv2** to manage the certificates, since it was a well-known protocol on radio networks

Implementing CMPv2 in all functions of the **core networks** is clearly **not a walk in the park**

The content of **certificates changed in different 3GPP releases**, so there might be implementation discrepancies

Encryption between network functions make operators **rethink monitoring and troubleshooting**

orange™

Some security solutions like the massive encryption and authentication can bring some challenges for operational teams…but also for the Industry who needs to adapt.

Back on feet

In case of a successful attack, the time needed to restore the service is **money** (**loss**…and **fines**)

It is important to **understand what happened and how** it happened…so it won't happen again.

An increasing difficulty is the massive **number of logs** available.
It's a LOT (combination of several software layers)

Back-ups are really important, and so they must be secured and protected *(e.g. Vodafone PT attack)*

To process all these data, it is very important to have **clear and relevant logs**, with different levels.

AI-based tool are a fantastic **opportunity** to speed-up the process.
But it comes with several points of attention, notably **hallucination** & **sovereignty**.

New technologies such as AI can help a lot operational & security teams (as well as hackers…) but it introduces also new challenges to cope with.

Securing 5G in live networks

The first job: **training field teams** about security and good practices and **explaining why** it is not an option.

That includes **RETEX and cyberattack cold analysis** (e.g. SKT attack or Vodafone Portugal)

A **Security governance** is set up accord all entities and most critical subjects are followed at exec level (COMEX)

Security audits are performed by affiliates (**self control**), and **group governance** can trigger audits too.

A very **significant improvement** of **monitoring** and **reinforcement** of **SOC** teams 5G

It is also essential to invest in modern technologies that **are great enablers** for network security:
IA, automatization, advanced attack detection, EDR, big Data..

But it comes with its own challenges : IA or EDR examples

orange™

On the field, live network such as 5G need a constant operational vigilance to guarantee resilience and integrity of services.
Modern technologies can provide fantastic opportunities…but it comes with new challenges.

The importance of monitoring


Image: www.freepik.com

« A cyberattack is like a fire, the sooner you take care of it, the easier to neutralize it ».

Detecting **as soon as possible** the attack is crucial **to limit costs and impacts**

CERT, CSIRT and **PSIRT** are entities that communicate together about weaknesses, risks and attacks to better mitigate or avoid security attacks (security patches, countermeasures, …)

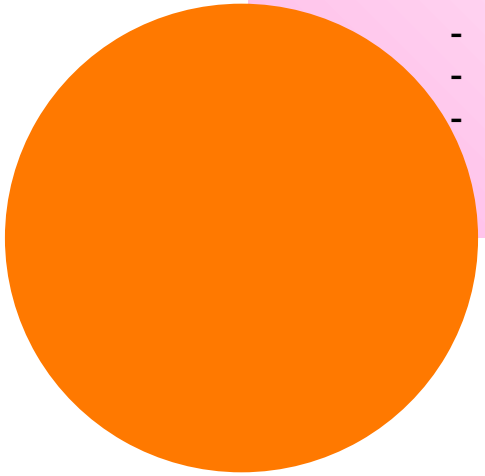
SOCs (Security Operation Center) are operational security supervision centers, running 24/7. Their mission is to detect, analyze and mitigate security incidents.

SOCs use **SIEM**, very powerful software that allows to trace, list, analyze and even ease the management of security incidents.

A **forensic job** and **reverse engineering** may be done to identify the **origin of the attack**.
The information from logs, SOC and SIEM is then essential to have a better understanding of the attack.

Detecting very early a cyberattack drastically reduce the impact of the attack
Investing in strong monitoring capacities (teams, tools, processes) is mandatory

Take aways 1/2



Hardening

- OS hardening
- Service hardening (ex: TLS, SIP…)
- Fuzzing & DDoS
- Weak passwords, passwords in plain text
- 3GPP SCAS tests
- CISCAT Assessor
- Pentests

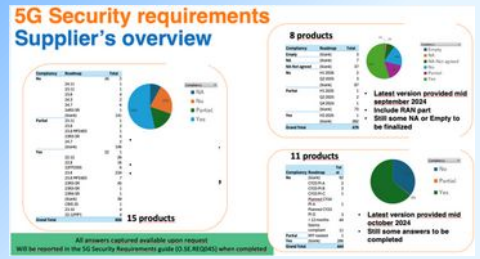
Take aways 1/2

Hardening

- OS hardening
- Service hardening (ex: TLS, SIP…)
- Fuzzing & DDoS
- Weak passwords, passwords in plain text
- 3GPP SCAS tests
- CISCAT Assessor
- Pentests

Security requirements

- Group requirements (official policy)
- Standards
- Best practices, RFP req.



Take aways 1/2

Hardening

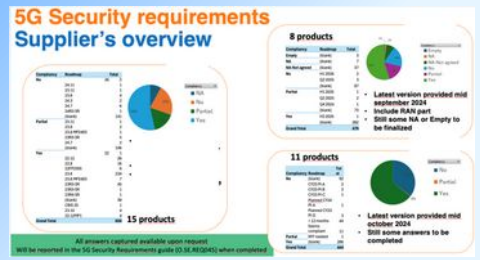
- OS hardening
- Service hardening (ex: TLS, SIP…)
- Fuzzing & DDoS
- Weak passwords, passwords in plain text
- 3GPP SCAS tests
- CISCAT Assessor
- Pentests

Vulns & SBOM

- Continuous process
- Inputs from vendors
- SBOM generators
- Vulnerability scans
- Vendors Remediation
- Patching Follow-up
- Specific analysis

Security requirements

- Group requirements (official policy)
- Standards
- Best practices, RFP req.



grype syft dependency track

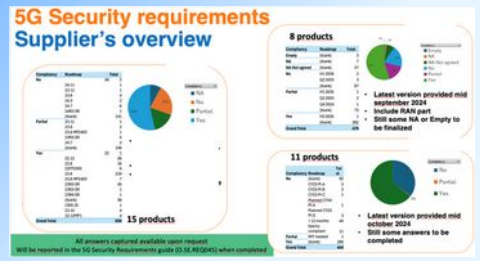
Take aways 1/2

Vendor Management
- Security Steercos
- Executive reviews
- NIS2 & CRA compliancy
- Contractual documents

Hardening
- OS hardening
- Service hardening (ex: TLS, SIP…)
- Fuzzing & DDoS
- Weak passwords, passwords in plain text
- 3GPP SCAS tests
- CISCAT Assessor
- Pentests

Vulns & SBOM
- Continuous process
- Inputs from vendors
- SBOM generators
- Vulnerability scans
- Vendors Remediation
- Patching Follow-up
- Specific analysis

Security requirements
- Group requirements (official policy)
- Standards
- Best practices, RFP req.



Take aways 2/2

5G is inherently **designed to be secure;** it's a fundamental requirement that has guided its conception and deployment through **standards**, **regulations**, and **architectural design**. However, operators have to carefully configure the options to leverage the best security features.

We've seen how 5G delivers major **security improvements** compared to previous mobile network generations: **enhanced encryption**, **secure service-based architecture**, and robust **subscriber identity protection**.

However, this must be **complemented** by strict **security measures** to ensure the quality of vendor-delivered solutions and proper network configuration.

Network **monitoring** and **rapid response capabilities** are equally critical to **detect attacks early** and significantly limit their impact.

Last but not least, implementing robust **recovery measures**—including high-quality backup protection—is essential to rapidly restore services after an attack and minimize business impact

orange™

THANK YOU!