TOR VERGATA
UNIVERSITÀ DEGLI STUDI DI ROMA

Seminario
ISCOM - Scuola Superiore di Specializzazione in Telecomunicazioni (SSSTLC)
MIMIT (Ministero delle Imprese e del Made in Italy)
Roma, 29 marzo 2023

5G: architettura, servizi, protocolli e soluzioni innovative per la sicurezza

Prof. **Franco Mazzenga**

Dipartimento di Ingegneria dell'Impresa ''Mario Lucertini''

Università di Roma Tor Vergata

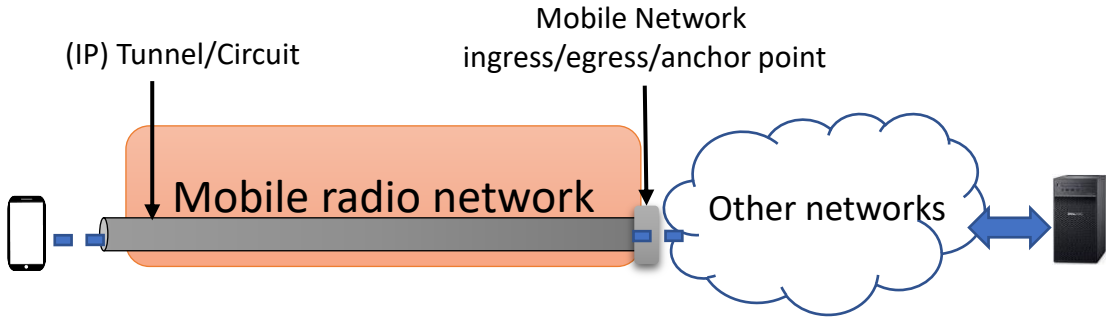
email: mazzenga@ing.uniroma2.it

Sommario

- Il sistema 5G
  - Architettura: rete di accesso e core network
  - Opensource softwarization
  - Network slicing e MEC
- Sicurezza per il 5G
  - Concetto di Trust e sua evoluzione verso il 5G
  - Perimetro per la sicurezza del 5G
  - Stakeholders, Minacce, Responsabili e bersagli della rete 5G
  - Vulnerabilità già identificate
- Soluzioni di sicurezza nel 5G
  - Attività di standardizzazione
  - La specifica 3GPP TS 33.501
  - La sicurezza di livello PHY (PSL)
- Conclusioni

Servizio offerto da un sistema radiomobile

- Dal punto di vista dell'utente, un sistema radiomobile:
  - Offre un servizio di rete per la **connettività end-to-end** tra utenti o gruppi di utenti a distanza e può spostarsi nell'area coperta dal servizio
  - Il requisito della mobilità implica l'uso ''*obbligatorio*'' delle tecnologie radio per la connessione con il sistema radiomobile
  - Il servizio di rete per la connettività è utilizzato per il trasferimento della voce/dati associati ai servizi di comunicazione e alle applicazioni utente
  - Le applicazioni in esecuzione sul terminale utente utilizzano i servizi di connettività offerti dal sistema radiomobile per svolgere le proprie funzioni e quindi offrire servizi al proprietario del terminale
- **Tipi di utenti:** Utenti (o gruppi) entrambi in movimento, Utenti in movimento e un (gruppo) utenti fissi che accedono da rete fissa



2G: creazione di un circuito nella rete mobile che collega il terminale mobile al punto di ingresso/uscita della rete mobile

3G: creazione di un tunnel a circuito e/o pacchetto (IP) nella rete mobile che collega il terminale mobile al punto di ingresso/uscita della rete mobile

4G: creazione di un **EPS bearer** basato su IP nella rete mobile che collega il terminale mobile al punto di ingresso/uscita della rete mobile

5G: creazione di una **sessione PDU (PDU SESSION)** basata su IP nella rete mobile che collega il terminale mobile al punto di ingresso/uscita della rete mobile

La rete mobile offre il servizio di connettività utilizzando circuiti (2G) o (molto) più in generale tunnel (>2G)

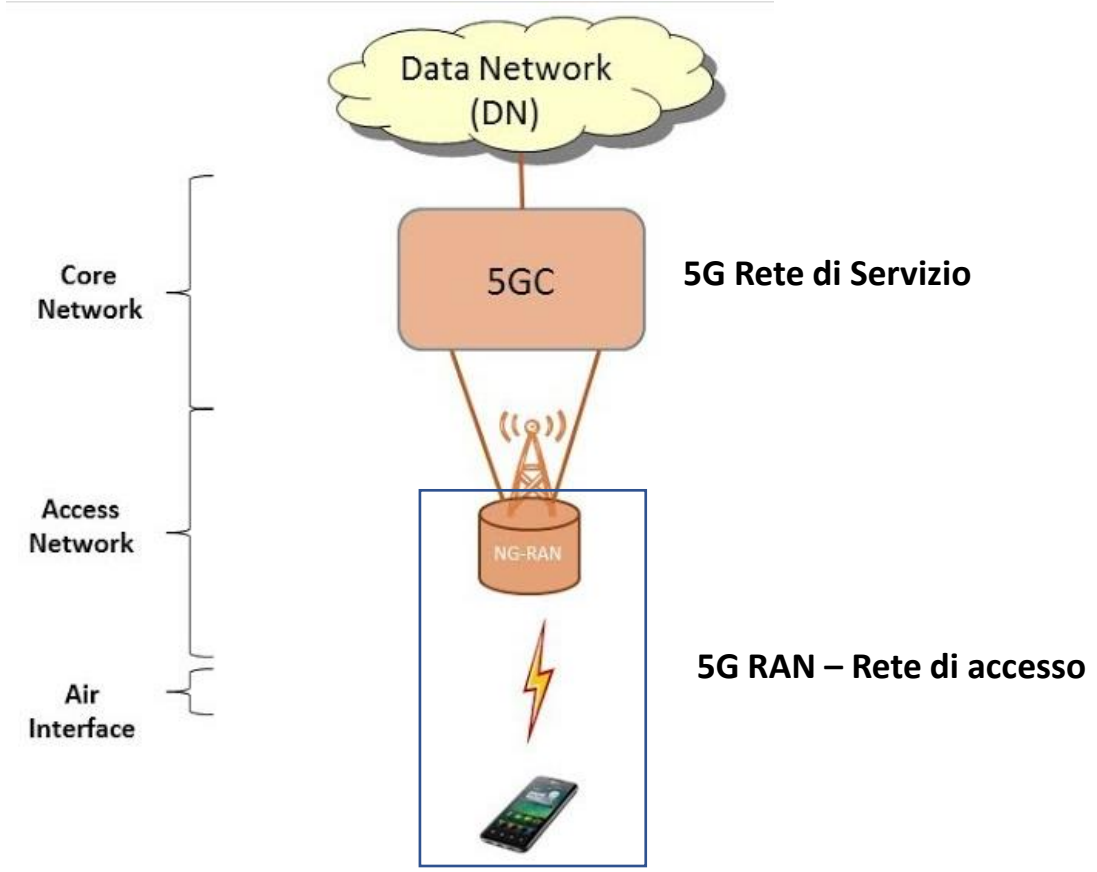
Architettura di base del 5G

Rete di accesso basata sulla:

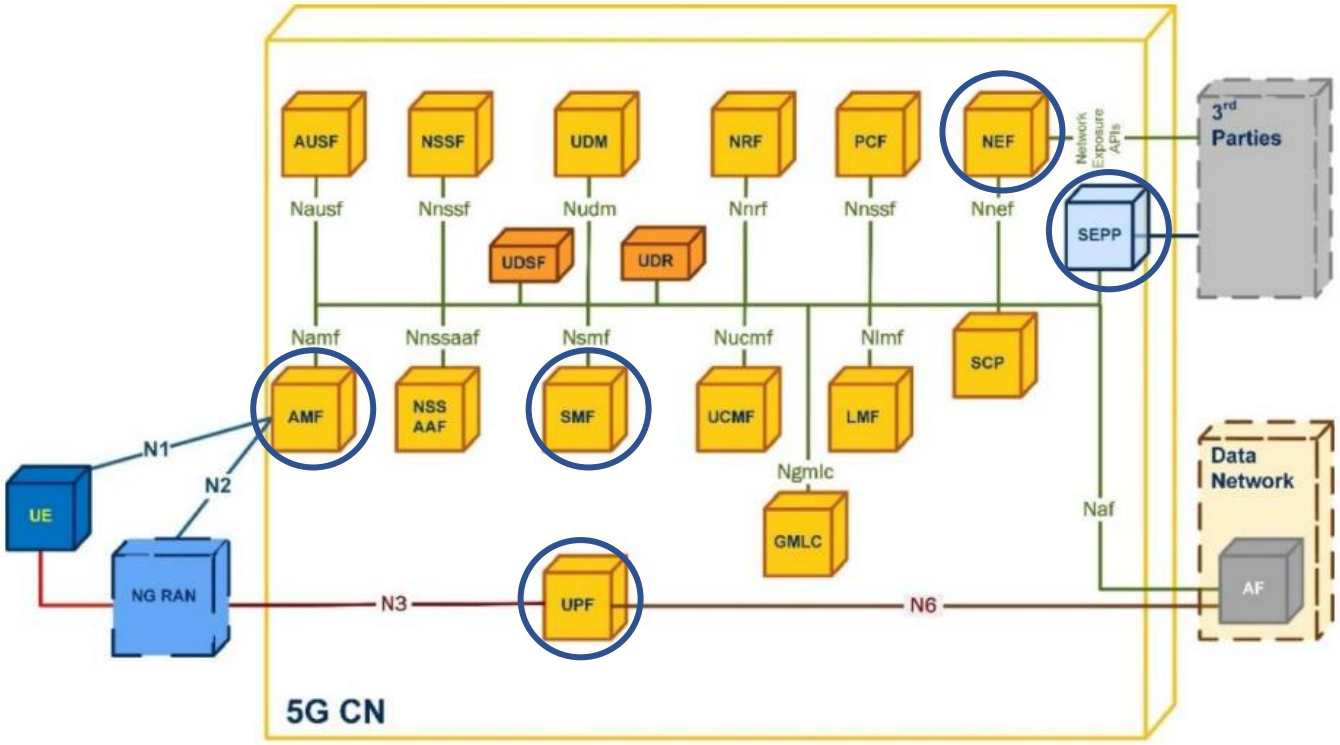
- ***5G New Radio, 5G NR:***
  - 5G new radio nome della **5G radio access network e della interfaccia radio**.
  - Comprende i punti di accesso denominati gNB.
  - E' in grado di accogliere traffico offerto dagli utenti molto variabile (da kbps (nodo IoT) a Gbps).

Rete di servizio: funzionalità descritte nel

- ***5G NextGen Core Network (5GC):***
  - Nella fase iniziale del dispiegamento del 5G, si utilizza la rete di servizio (Core Network) del 4G (Non Stand Alone);
  - Comprende due piani: **il piano di utente** per il trattamento e il trasferimento dei flussi; **il piano di controllo** per la gestione dell'operatività della rete.
  - Lo sviluppo e il dispiegamento della 5G core network consente al 5G di raggiungere la sua massima potenzialità sia in termini di capacità di trasferimento dati, flessibilità e requisiti di latenza (Stand Alone).



Core network architecture del 5G



Some of the security NFs in the 5G Core network
AUSF: AUthentication Server Function;
ARPF: Authentication credential Repository and Processing Function;
SEAF: SEcurity Anchor Function.
SEPP: Security Edge Protection Proxy

5G architecture: complete virtualization of the Core network (5G CN).

The 'softwarisation' of network functions will enable easier portability and higher flexibility of networking systems and services (Control-User Plane Separation, CUPS).

The Software Defined Network (SDN) abstracts low-level network functionalities to simplify network management.

Network Function Virtualisation (NFV) provides the enabling technology for placing various network functions in different network components on the basis of performance needs/requirements; and eliminates the need for function-or service-specific hardware.

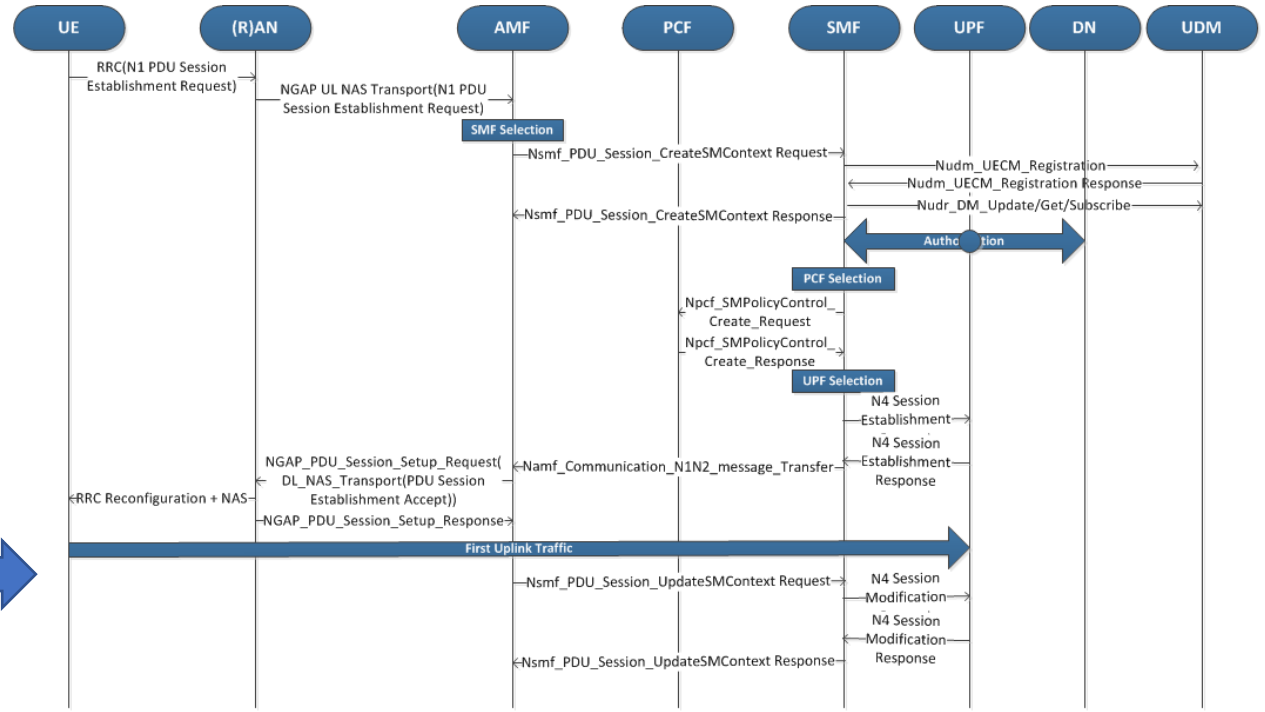
SDN and NFV, complementing each other, improve the network elasticity, simplify network control and management, break the barrier of vendor-specific or proprietary solutions, and are thus considered as highly important for future networks.

These novel network technologies and concepts that rely heavily on 'softwarisation' and virtualisation of network functions will introduce new and complex threats for security (see after).

Esempio: funzionalità nella rete di servizio del 5G -> **PDU Session Establishment**

- I **servizi di rete** deputati alla realizzazione del servizio di connettività offerto dall'operatore e che sono specifici della rete di servizio (ad esempio del 5G) sono realizzati (*nascono dalla ''combinazione''*) derivante dalla **interazione tra le entità che realizzano le funzioni di rete (NF)**
- L'interazione avviene mediante scambio di messaggi e dei dati di utente attraverso le interfacce (N1,N2,N3,… nel caso 5G)
- In generale una funzionalità ''*complicata*'' specifica della rete di servizio viene tipicamente decomposta/ripartita in piu NF elementari ciascuna di queste realizzate dalle entità ''specializzate'' come AMF, SMF (piano di controllo) e UPF (piano di utente).
  - **Esempio: PDU session establishment nel 5G**

5G PDU Session Establishment



Source: 5G PDU Session Establishment, by prasanna sahu in 5G Core

Open-source Softwarization della rete 5G: la SBA

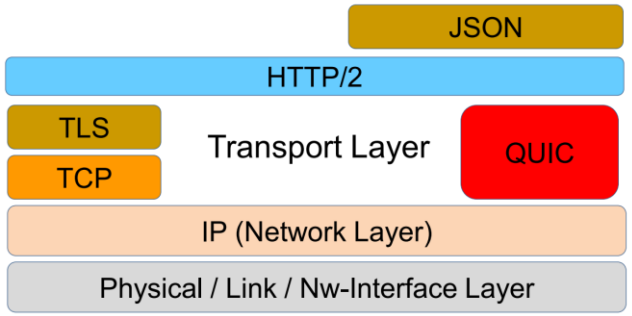
- 5GS standardization **is largely implemented by open-source software alliances** along with many proprietary vendor-specific implementations. Small-scale implementations often opt for open-source software implementation to keep costs low. The advantage of using an open-source software suite is that anybody from the community can review the codes and flag potential bugs. Many reviewers can report those bugs so that the vulnerabilities can be detected early for patching.

Essentially, all NFs can communicate with each other using either a request/response or subscribe/notify interactions between NF service consumers and producers.

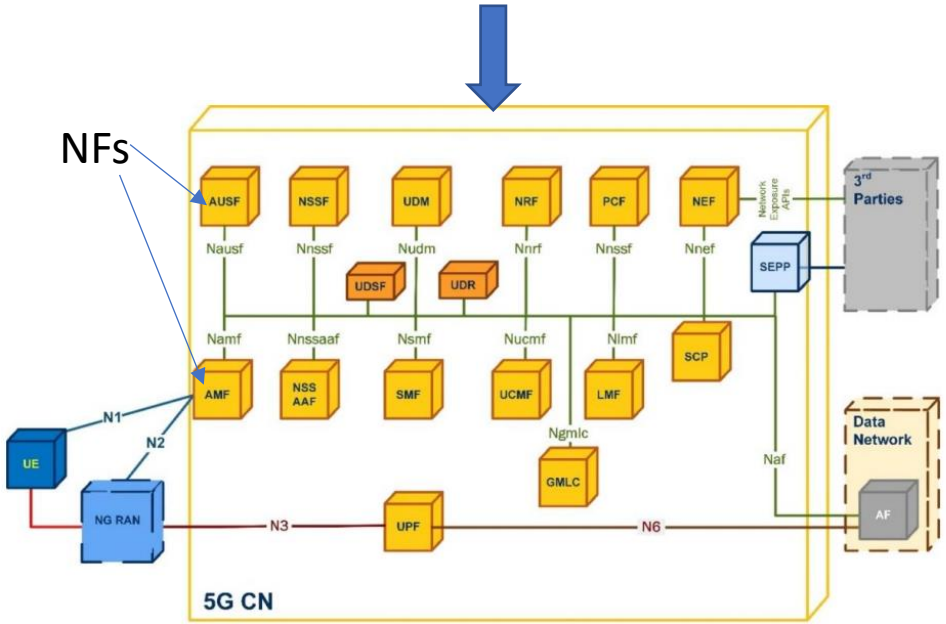
5G Service Based (Core Network) Architecture adopts **IETF protocols**

IT concept of Service Based Architecture (SBA) has been imported in the 5G core network design

- HTTP/2 adopted as the **application layer protocol** for the service based interfaces
- **TCP adopted as the transport layer protocol**;
  - Use of QUIC, binary encoding (e.g. CBOR) and other aspects are left for possible support in future releases
- JSON adopted as the serialization protocol;
- **REST-style service design** whenever possible and custom (RPC based) methods otherwise.



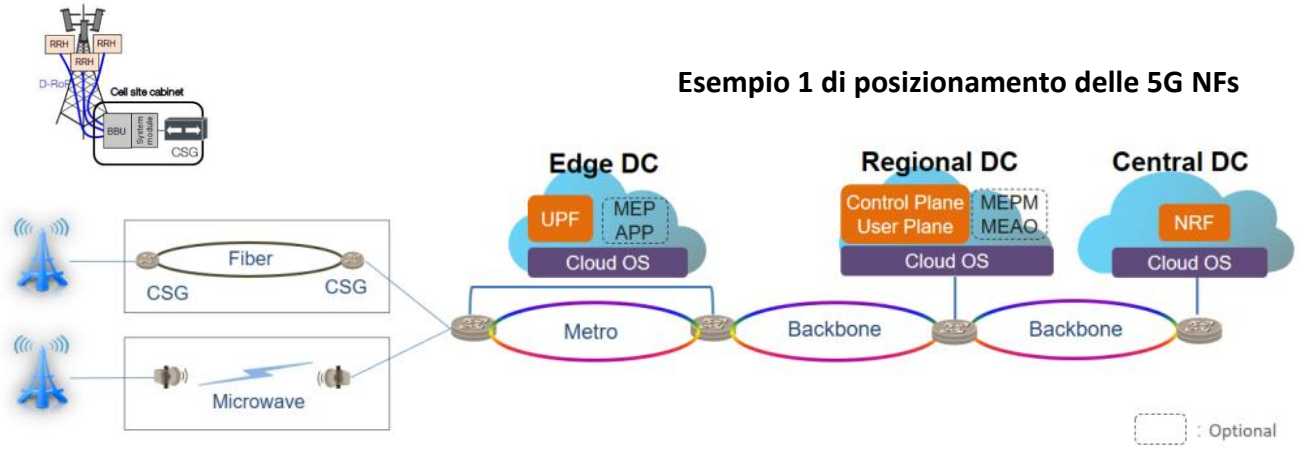
Service Based Architecture (SBA)



Domanda: le NF del 5G dove sono posizionate all'interno della rete dell'operatore ?

- Dipende dalle scelte di pianificazione della rete da parte del Telco e dai requisiti di prestazione desiderati
- La rete di servizio del 5G contiene ''entità di rete'' come AMF, SMF (piano controllo) e UPF (piano di utente) che implementano una o più specifiche funzionalità di rete (NF).
- Le entità (AMF, SMF, UPF etc.) **sono tipicamente ''distribuite''** nella rete dell'operatore e sono implementate in apparati HW/SW specializzati (vecchio approccio) oppure come macchine virtuali che realizzano funzioni di rete virtuali (NFV) che girano su hardware general purpose
- Il loro posizionamento all'interno della rete dell'operatore è importante per garantire il soddisfacimento dei requisiti di TH legati al problema della latenza sulle connessioni.

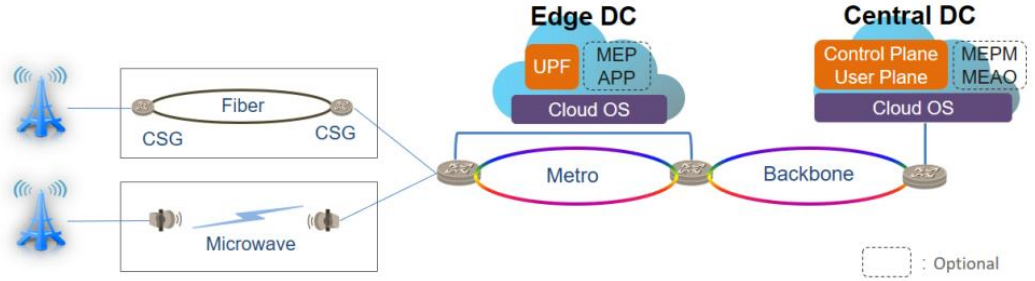
Esempio 1 di posizionamento delle 5G NFs



Legend:

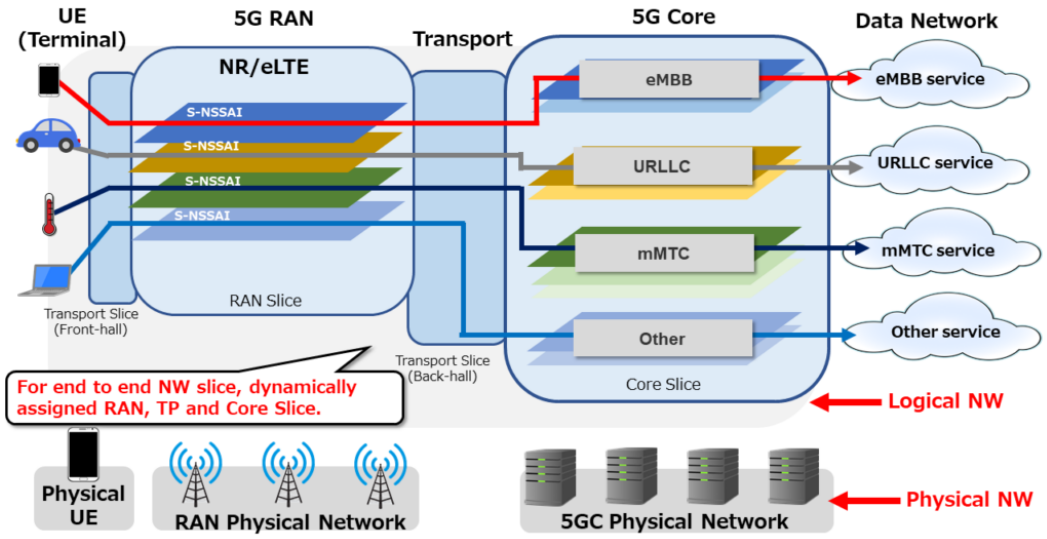
- MEPM: MEC Platform Management
- MEP: MEC platform
- MEAO: MEC Application Orchestrator
- CSG: Cell Site Gateway – solitamente installato nei CO
- UPF: user plane function

Esempio 2 di posizionamento delle 5G NFs



5G: Network slicing e MEC

- La softwarizzazione della rete abilita il network slicing: creazione di reti logiche sulla stessa infrastruttura fisica

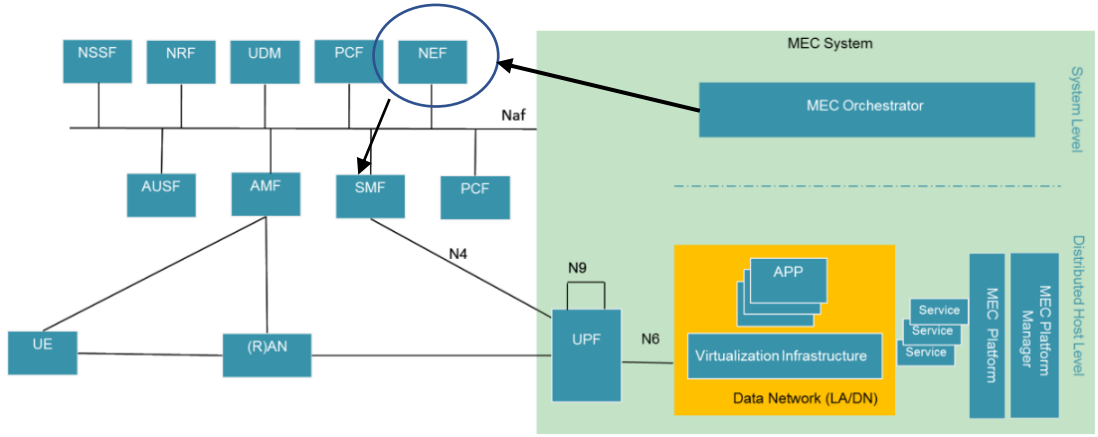


Fig, End to End Network Slicing Overview

by T.Nagumo

Network slices are used to deploy services **at the multi-access edge across a distributed cloud infrastructure**. Network slices can be configured based upon the service-type (eMBB, mMTC, URLLC), customer, and application to provide the required latency, bandwidth, QoS, and security.

- 5G supporta il MEC -> nuovo elemento da considerare nella analisi delle vulnerabilità
- **Con il MEC la rete 5G si apre verso l'esterno**



Motivazioni per l'impiego del Multi Access Edge Computing (MEC)

MEC provides a new ecosystem and value chain. **Operators can open their Radio Access Network (RAN) edge to authorized third-parties, allowing them to flexibly and rapidly deploy innovative applications and services towards mobile subscribers, enterprises and vertical segments.**
Multi-access Edge Computing **will enable new vertical business segments and services for consumers and enterprise customers**.

Sicurezza per il 5G

Terminologia

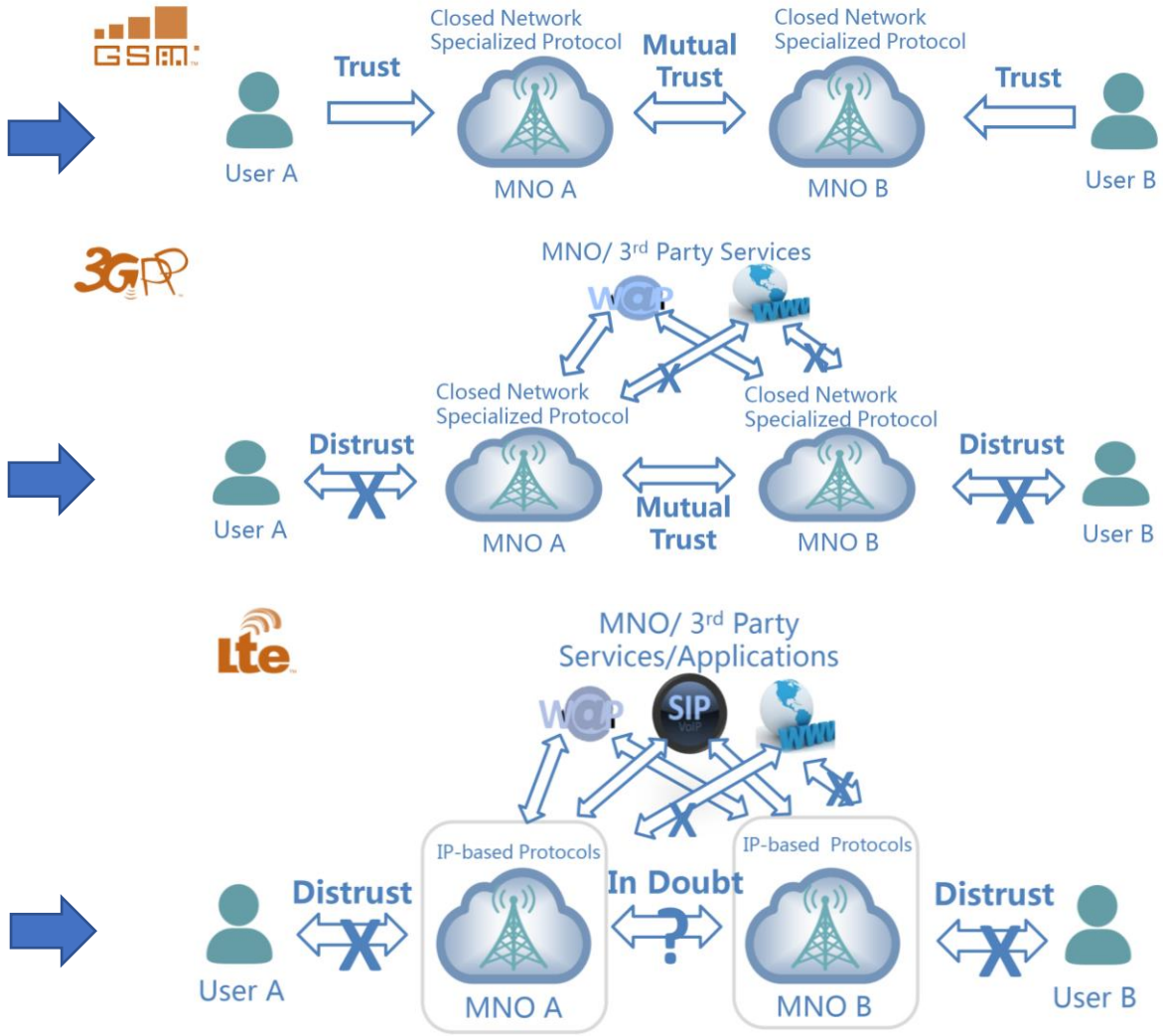
- **Nell'ambito della trasmissione ''elettronica'' della informazione**
- **Sicurezza significa:** prevenire l'accesso non autorizzato a messaggi a risorse e infrastrutture di comunicazioni consentendo allo stesso tempo la fruizione del servizio di comunicazioni tra le parti autorizzate (intended parties)
- **Privacy:** significa proteggere l'identità, la posizione e i dati personali dell'utente
- Una **minaccia (threat)** è un ''metodo'' (una qualunque strategia) finalizzata a compromettere:
  - security e/o privacy
  - denial of service (DoS) to the user
  - theft of service by an unauthorized user
  - access/modification to information by an unauthorized user
  - control of restricted resources by an unauthorized user
  - physical damage to resources
- **Trust** definisce il livello di fiducia che si ha quando: ***interagendo con una entità si ritiene che questa si comporti esattamente come ci si aspetta (ossia secondo ad esempio una policy definita) e, soprattutto, che non sia fonte di minacce***.
- **Superficie di attacco:**
  - Una superficie di attacco consiste nella possibilità da parte di qualcuno/qualcosa di raggiungere e di sfruttare una vulnerabilità del sistema
- Esempi di superfici di attacco sono:
  - Open ports on outward facing Web and other servers, and code listening on those ports
  - Services available on the inside of a firewall
  - Code that processes incoming data, email, XML, office documents, and industry-specific custom data exchange formats
  - Interfaces, SQL, and Web forms
  - An employee with access to sensitive information vulnerable to a social engi-
    neering attack

Sicurezza nei sistemi radiomobili

- **Modelli di interazione basati sulla fiducia tra gli ‘’attori’’ (dispositivi, sottosistemi) che realizzano un sistema**
- All'inizio il modello era **fidarsi di tutti**
- Negli anni '90 il modello di comportamento è cambiato in ‘’*morbido all'interno*’’ e ‘’*duro verso l’esterno*’’ in pratica: fidandosi di dipendenti e colleghi ma non di estranei,
- Ciò ha portato allo sviluppo di politiche di accesso, firewall, ecc.
- Oggi le procedure operative standard impongono
  - Di non fidarsi di nessuno
  - Di monitorare costantemente tutte le attività
  - Cercare in modo proattivo le vulnerabilità e
  - Utilizzare più livelli di protezione (nel caso in cui uno fallisca)

Il rapporto di fiducia (trust) e sua evoluzione: dal 2G al 4G per arrivare al 5G

- In 2G la fiducia è richiesta (e ottenuta utilizzando una SIM) dell'UE da parte della/e rete/e per evitare la minaccia di **furto del servizio**
  - Tuttavia, si presume che l'UE si fidi della rete e la minaccia di intercettazioni sull'interfaccia radio rimanga valida, ma si presume che la crittografia sia sufficiente per gestire questo problema. In pratica si assume che la fiducia sia
  - 1. all'interno di qualsiasi rete mobile
  - 2. tra la rete di servizio e la rete domestica (o qualsiasi altra rete mobile)
- Nel 3G non si presume più che l'UE possa fidarsi della rete (*a causa della possibilità di **false stazioni base***) e la crittografia sulla interfaccia radio viene rafforzata (ma è ancora ''pasticciata'')
- Nel 4G ci sono più attori che interagiscono (aumentano quindi le superfici di attacco): UE, rete di servizio, rete domestica, reti di trasporto altre reti (3GPP e non 3GPP). Le ipotesi sono:
  - UE e reti hanno una reciproca mancanza di fiducia,
  - la privacy degli utenti deve essere rispettata e occorre impedire non solo le intercettazioni ma anche il tracciamento
  - tra le reti potrebbe esserci fiducia (almeno in una certa misura) ma le diverse reti mobili devono comunque autenticarsi a vicenda
  - l'interfaccia radio deve usare algoritmi efficaci di crittografia

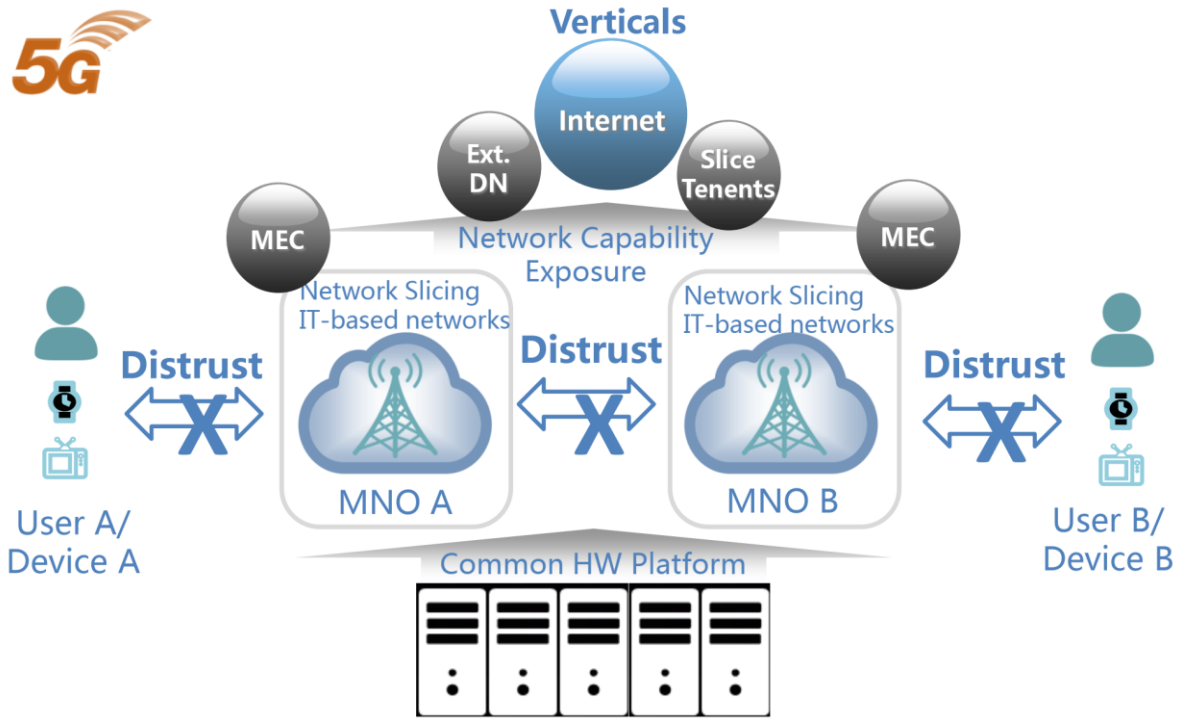


La fiducia nel 5G e il principio zero-trust

- Since 5G is designed to enable critical applications, such as
  - critical infrastructure (electric, water, transportation, traffic control)
  - emergency response
  - smart cities
  - autonomous cars

the threats can be much more significant than theft of service and eavesdropping

- **Furthermore the trust model involves many (new) entities**
  - UE
  - new host types (laptops, IoT, vehicles)
  - home network
  - serving network
  - new transport mechanisms
  - cloud service providers
  - third-party application function providers
  - private network operators
  - direct peer-to-peer connections (e.g., for V2V)
- **Il principio zero-trust** sembra essere il più adeguato per trattare con una **moltitudine** di attori **sparsi** ed **eterogenei** che devono interagire

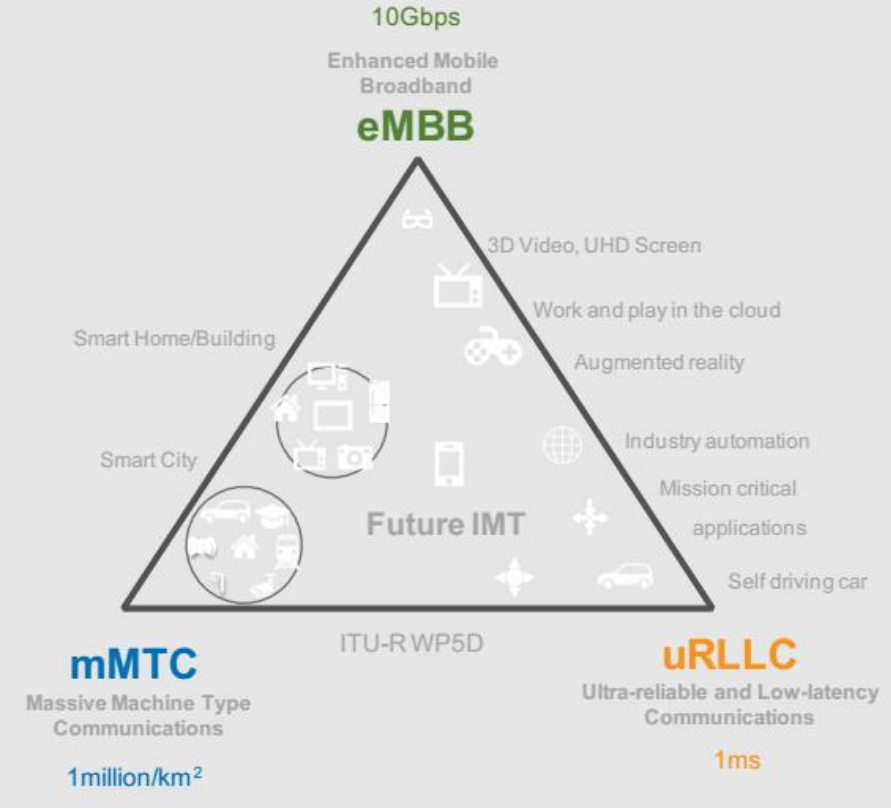


Zero Trust principle: is a network security strategy based on the philosophy that **no person or device inside or outside of an organization's network should be granted access to connect to IT systems or workloads unless it is explicitly deemed necessary.** The Zero Trust model relies on strong authentication and authorization for every device and person before any access or data transfer takes place on a private network, no matter if they are inside or outside that network perimeter. Furthermore:

- Access is granted only to resources that should be used; other resources are hidden to authorized users.
- Continuous monitoring of users/systems activities are an important component in Zero-Trust paradigm implementation.

Perchè garantire la sicurezza nel 5G è sfidante ?

Quali servizi offre il 5G e a chi/cosa !!! **Il 5G è stato concepito per essere l'"unica tecnologia" per abilitare la comunicazione tra diverse tipologie di utenti che necessitano di servizi di connettività con requisiti molto differenti**



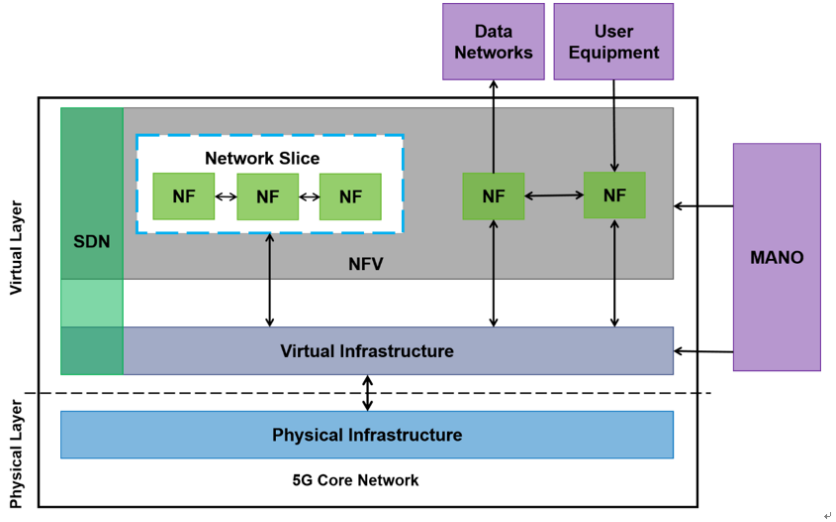
Inoltre il 5G lo si vuole usare per monitorare le infrastrutture critiche

Identificare le vulnerabilità è il primo obiettivo ai fini della sicurezza del sistema 5G

https://www.3gpp.org/news-events/3gpp-news/5g-wiseharbour

Perchè garantire la sicurezza nel 5G è sfidante ? (cont.)

- **Nel 5G si assiste alla convergenza tra IT e la infrastruttura che supporta la telecomunicazione (ICT)**
  - Il nucleo di rete del 5G (detto 5GS) si basa su **una infrastruttura fisica della rete di telecomunicazione** (ICT) che consente di implementare le funzioni di rete (NFs) mediante **tecniche di virtualizzazione** (Nota: in passato le NFs erano implementate attraverso dispositivi fisici dedicati). **Network functions are pushed to the cloud of connected servers throughout the network**.
  - **SDN, NFV, and cloud computing are the key enablers of the 5G network towards a programmable, scalable, all IP infrastructure for voice and broadband**
  - **Obviously,** due to a flat IP-based network architecture, cyberattacks such as IP spoofing and port scanning can harm the 5G network if not appropriately secured from the very beginning. Moreover, in cloud-native computing architecture, user information is stored, processed, and shared by many co-located services following techniques such as replication, distributed file synchronization, and controlled data flow, to name a few.
- **Billions of Hackable IoT Devices**
  - New vulnerabilities are contributed significantly by billions of insecure smart devices, which are tiny computers equipped with high-end sensors. These devices give rise to the massive 5G IoT. Small devices are often hackable by side-channel attacks, exploiting software security weaknesses, and doing reverse engineering. Once an attacker manages to get access to the device, **he can virtually do many malicious activities to capture or modify sensitive user data** stealthily and can even install unwanted software for continuous unsolicited user activity monitoring. Thus, IoTs accessing 5G networks open up more point of entries to hack into subscribers' privacy domain.
- **La rete 5G utilizza tecniche di intelligenza artificiale ai fini del management/controllo della rete**
  - The 5GS adopts a massive number of third-party services, network management and orchestration system, and intrusion detection systems that unleash the power of machine learning, **which itself is not secure.**
  - **In ambito** 5G, AI and its subfields such as machine learning and deep learning have been adopted to accomplish a variety of tasks, including resource management, carrier sensing, cross-channel learning, user requirement profiling, and from the security point of view, even anomalous traffic detection for cyber defense.
  - It is well known that machine learning techniques are increasingly getting popular also among hackers to initiate smarter and faster yet low-cost attacks.
- **Quindi come si deve organizzare il processo che si occupa della sicurezza del sistema 5G ?**
  - Securing the 5G network requires intrinsic security features to be developed as an **integral part of the 5GS development process -> SECURITY BY DESIGN**.
  - Every module del 5GS should have secure communication protocols and interfaces over which they transfer user and control data.

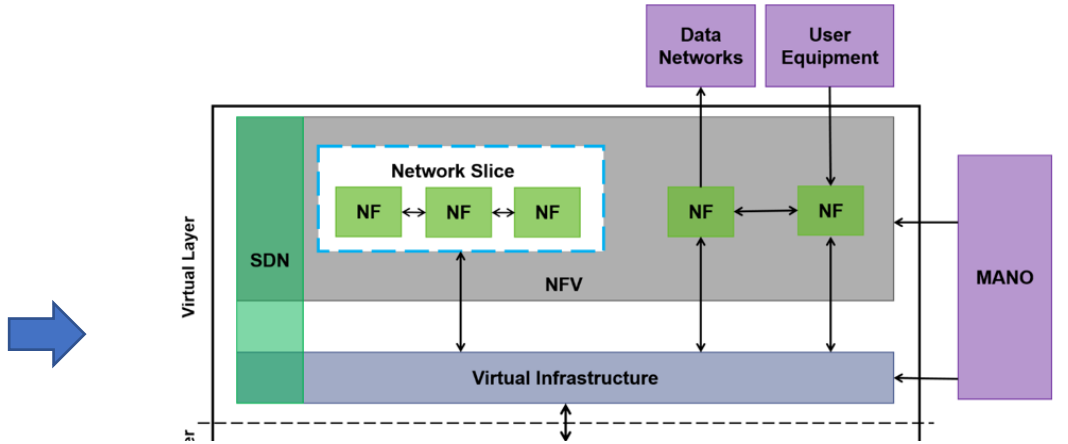


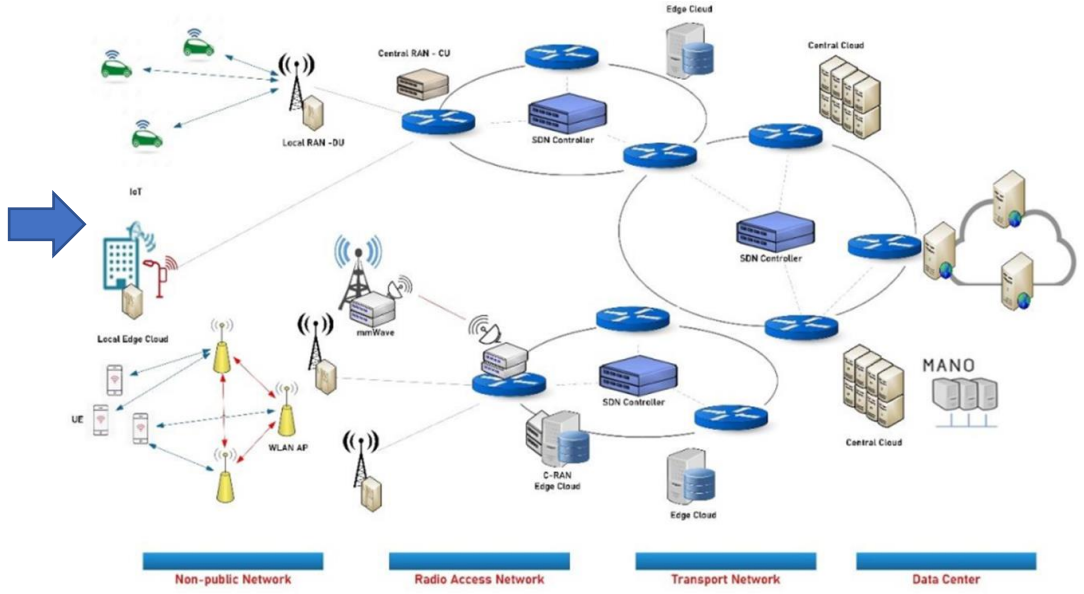
In practice, we cannot envisage 5G security as a separate layer of shield that can save the whole 5G system after its deployment.

Perimetro di sicurezza del 5G

- Due aspetti di sicurezza da considerare nell'identificare il perimetro del 5G e quindi le superfici di attacco:
  - **Sicurezza della infrastruttura software di rete (evidenti problemi di cybersecurity)**
    - One of the most relevant aspects in the transition from previous generations of mobile telecommunications into 5G is the fact that part of the network functions, previously **performed by physical appliances, are now executed by software** that virtualizes the functionality of physical components.
    - Additionally, some of these physical components were mostly proprietary and incompatible with other solutions but with 5G, the network software can run in any commercial-of-the-shelf (COTS) hardware, allowing the operators to have more independence from manufacturers and share physical infrastructures among various tenants and applications
  - **Sicurezza (si parla anche di safety) della infrastruttura fisica della rete 5G**
    - Nonetheless, the physical 5G architecture is going to remain exposed to more generic threats that are pertinent to physical components, such as *damage/theft, sabotage, natural disasters, outages, failures and malfunctions, just to name the most important ones*.
    - **NOTA:** While in previous mobile networks such failures had a more "restricted" influence in service provisioning, with the 5G virtualization failures of physical components may have an amplified impact, typical to shared resources.

- **Studio delle vulnerabilità nel 5G:** approccio classico allo studio della sicurezza di un sistema -> occorre identificare
  - Chi sono coloro che hanno interesse nel 5G (gli stakeholders) e sono a vario titolo coinvolti nel processo di rendere sicuro il sistema 5G
  - Obiettivi dell'attacco
  - Chi sono i responsabili degli attacchi
  - Identificare i componenti della rete oggetto di minacce
    - Identificare le vulnerabilità **evidenti** nelle componenti della rete e delle tecnologie utilizzate





Infrastruttura fisica del 5G

NOTA: ad oggi siccome le implementazioni del 5G sono ancora **parziali**, le potenziali minacce per il 5G sono state identificate soltanto ''sulla carta'' a partire dalle specifiche del sistema e prescindendo per ora dai risultati basati su possibili implementazioni reali della rete 5G.

Stakeholders coinvolti nella realizzazione del sistema 5G e sicurezza

- Stakeholders will play different roles in the 5G ecosystem. Among other things, these entities will be responsible for **assuring the security of the network** at different levels and in separate layers.
- The list of stakeholder roles in the 5G ecosystem is the following:
  - *Service customers (SC)*;
  - *Service providers (SP)*;
  - *Mobile Network Operators (MNO) also known as Network Operators (NOP)*;
  - *Virtualisation Infrastructure Service Providers (VISP)* and
  - *Data Centre Providers (DCSP)*.
- e vista l'importanza delle applicazioni del sistema 5G (es. monitoraggio sistemi critici) si aggiungono i:
  - *Network infrastructure providers*;
  - *National Regulators (NRAs)*;
  - *Information sharing and analysis centres (ISACs)*;
  - *National cybersecurity coordinators/agencies/centres (NCSCs)*;
  - *National 5G Test Centres (NTCs)*;
  - *National Certification Authorities (NCAs)* and
  - *Competent EU institutions, European Commission Services, Agencies, Bodies,*
  - *Committees and Groups (including NIS-CG, ECCG, ECSO, ENISA and BEREC)*

Obiettivi delle minacce alla rete 5G

- Overall, threats considered most relevant are the main traditional categories of threats: this concerns threats related to the compromise of **confidentiality, availability and integrity**
- More specifically, a number of threat scenarios targeting 5G networks were found to be particularly concerning:
  - Local or global 5G network disruption (Availability);
  - Spying of traffic/data in the 5G network infrastructure (Confidentiality);
  - Modification or re-routing of the traffic/data in the 5G network infrastructure (Integrity and/or Confidentiality);
  - Destruction or alteration of other digital infrastructures or information systems through the 5G networks (Integrity and/or Availability)
- The **severity of specific threat scenarios** to 5G networks may thus vary according to a number of factors, in particular:
  - the number and type of users impacted;
  - the time duration of the event before detection or remediation;
  - the type of services impacted (public security, emergency services, health, governmental activities, electricity, water, etc.) and the
  - extent of damage and/or related economic losses;
  - the type of information breached (sensitive or not).
- Infine, l'**autenticazione** (a diversi livelli e su attori/sottosistemi di rete diversi) è un altro dei problemi importanti da considerare nel sistema 5G.
  - Prevenire l'uso non autorizzato (che magari non danneggia la rete in termini di confidenzialità, dispnibvilità, integrità etc.) della infrastruttura di comunicazione è uno dei problemi più rilevanti per gli operatori

Responsabili degli attacchi

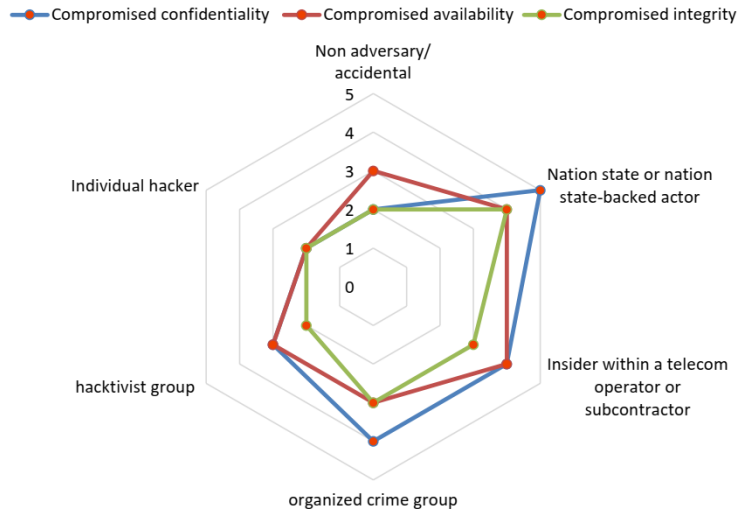
- The relevance of the threat actors in the 5G context has been assessed by combining two parameters:
  - the estimation of their capabilities (resources) and
  - their intention to perform or attempt attacks against 5G network infrastructures (motivation).

- Threats posed by **States or State-backed actors**, are perceived to be of highest relevance. They represent indeed the most serious as well as the most likely threat actors, as they can have the motivation, intent and **most important the capability to conduct persistent and sophisticated attacks on the security of 5G networks**.

- Further categories of actors could also be considered to have an important motivation to target 5G networks in order to serve their interest, i.e. organized crime groups, corporate entities seeking to gain competitive advantage in the technological field through Intellectual Property (IP) theft or cyber terrorists.

TITLE	DESCRIPTION
Non-Adversary/ Accidental	Non-adverserial/accidental threats manifest themselves as events that result from human error, natural phenomena, and systems failures.
Individual hacker	Individual hackers represent amateur criminal or hobbyist hackers driven by financial motivation or a desire for notoriety.
Hacktivist group	This threat actor has a political agenda. Their goal is to either create public attacks that help them distribute propaganda, or to cause damage to organizations they are opposed to. The ultimate goal is to find a way to benefit their cause or gain awareness for their issue.
Organised crime group	Organised crime groups are motivated by financial gain.
Insider	In the context of the security of 5G networks an insider threat refers to an insider working within a mobile network operator, or a mobile network's supplier. An insider may work for an organised crime group, a hacktivist group or a State actor, but individual motivations are not excluded.
State actor or state-backed actor	The motivations of this category of attacker are primarily political.
Other possible actors: Cyber-terrorists and corporate entities	Cyber terrorists are motivated by political aims and are likely to have very similar capabilities as an organised crime group. Corporate entities may seek to gain competitive advantage in the technological area through Intellectual Property (IP) theft, theft of sensitive commercial data or by causing reputational or operational damage to their global competitors through cyberattacks.

NIS



Componenti della rete 5G oggetto di minacce

- The following table presents the main categories of elements and functions and their overall level of sensitivity

- **Core network** functions of the 5G network are generally considered as ***critical***. Indeed, affecting the core network may potentially compromise the confidentiality, availability and integrity of the entire network services

- **Access network** functions were also rated with relatively ***high sensitivity***. However, the assessment of the degree of sensitivity of specific elements within the access functions varies according to a number of factors.

CATEGORIES OF ELEMENTS AND FUNCTIONS		EXAMPLES OF KEY ELEMENTS
Core network functions	**CRITICAL**	User Equipment Authentication, roaming and Session Management Functions
		User Equipment data transport functions
		Access policy management
		Registration and authorization of network services
		Storage of end-user and network data
		Link with third-party mobile networks
		Exposure of core network functions to external applications
		Attribution of end-user devices to network slices
NFV management and network orchestration (MANO)	**CRITICAL**	
Management systems and supporting services (other than MANO)	**MODERATE/HIGH**	Security management systems
		Billing and other support systems such as network performance
Radio Access network	**HIGH**	Base stations
Transport and transmission functions	**MODERATE/HIGH**	Low-level network equipment (routers, switches, etc)
		Filtering equipment (firewalls, IPS...)
Internetwork exchanges	**MODERATE/HIGH**	IP networks external to MNO premises Network services provided by third parties

NIS

Alcune vulnerabilità già identificate per il 5G (1/2)

- **Typical vulnerabilities related to hardware, software, processes and policies**
  - 5G networks **will be largely based on software**, major security flaws, such as those deriving from poor software development processes within equipment suppliers, could make it easier for actors to maliciously insert intentional backdoors into products and make them also harder to detect. This may increase the possibility of their exploitation leading to a particularly severe and widespread negative impact.
  - Moreover, new types of technical vulnerabilities related to specific 5G technologies are likely to appear, affecting for example the technology used in SDN and NFV, including Reviews of the practices of one of the major network equipment suppliers as regards 4G equipment and services have been for instance carried out by the UK Huawei Cybersecurity Evaluation Centre (HSCEC).
  - Cloud systems, and their configuration. (**more cloud systems in 5G deployment -> Edge DC, Metro DC, Core DC etc**.)
  - Lawful interception functions enabling authorized public authorities to gain access to networks will also become software based. Such processes, if not properly managed, could be misused for malicious actions.
  - Another type of vulnerability in the context of massive **5G use by verticals** may relate to data leakages between multiple virtual environments or slices (e.g. to spy on offers/data of a competitor). Slice isolation is a key problem identified by the industry and subject of intensive work today.
  - **Nota sulla vulnerabilità legate alla implementazione OPEN SOURCE:** On the other hand, the National Vulnerability Database (National Vulnerability Database 2019) publicly lists recent exploits, which could be potential targets by the attackers. Another risk of using open-source software modules at enterprise scale is sluggish development practices (such as copying code from unreliable sources) and **slow process of security patching**. Hence, it is indeed a challenge to secure 5GS, which mainly adopts several open-source software.
- **Per tutti gli stakeholders**
  - Lack of specialised and trained personnel to secure, monitor and maintain 5G networks
  - Lack of adequate internal security controls, monitoring practices, security management systems and insufficiencies in risk management practices
  - Lack or inadequate security or operational maintenance procedures, such as software update/patch management
  - Lack of compliance with 3GPP standards or incorrect implementation of standards

.

Alcune vulnerabilità già identificate per il 5G (2/2)

- **Per gli operatori radiomobili**
  - **Poor network design and architecture** (including lack of effective emergency and continuity mechanisms, inappropriate or misconfiguration for instance in virtualization or of administration or access rights, etc.): this may significantly increase the exposure to negative consequences (e.g. lack of isolation of low trust systems, potentially larger scope of security breaches).
  - **Poor physical security for network and IT infrastructure**: deficiencies in physical security can lead to inadequate protection of personnel, hardware, software, networks and data from any malicious actions and events.
  - **Poor policies for local and remote access to network components**: 5G networks will be composed of a large amount of virtual devices, which can be remotely accessed throughout the network. This vulnerability becomes significantly more acute in cases where the maintenance of networks will be performed by third-party suppliers.
  - **Lack of or insufficient security requirements in the procurement process:** this vulnerability can take the form of inadequate strategies for the selection of suppliers or a lack of prioritisation of security over other aspects in the procurement process.
  - **Poor change management process:** this vulnerability could limit the possibility to prevent human errors and unauthorised configuration changes
- **Per i supplier**
  - The increased role of software and services provided by third party suppliers in 5G networks leads to a greater exposure to a number of vulnerabilities that may derive from the risk profile of individual suppliers.
  - The risk profiles of individual suppliers can be assessed on the basis of several factors, notably:
  - The likelihood of the supplier being subject to interference from a non-EU country. This is one of the key aspects in the assessment of non-technical vulnerabilities related to 5G networks14. Such interference may be facilitated by, but not limited to, the presence of the following factors:
    - a strong link between the supplier and a government of a given third country;
    - the third country's legislation, especially where there are no legislative or democratic checks and balances in place, or in the absence of security or data protection agreements between the EU and the given third country;
  - The characteristics of the supplier's corporate ownership;
    - the ability for the third country to exercise any form of pressure, including in relation to the place of manufacturing of the equipment.

Vulnerabilità: Network slicing e MEC

- **Network slicing**

Slices provide inherent security through segmentation, slices can also be used to provide additional security protection and security services specific to the use case and customer requirements.

- **End-to-end security**
- In fact, **Network slices are end-to-end logical networks**, so it is natural to aim for end-to-end security. The concept of end-to end security is closely connected to the concepts of isolation and orchestration. Moreover, it is dependent on the business model and on the associated trust model.
- **Resource isolation**
- **Each slice may be perceived as isolated set of resources configured through the network environment and providing defined set of functions.** Level and strength of isolation may vary depending on requirements and usage scenarios for slicing.
- The **isolation** of the slices can be considered in at least four areas:
  - **Isolation of traffic**: the network slices should ensure that data flow of one slice does not move to another.
  - **Isolation of bandwidth**: slices should not utilize any bandwidth assigned to other slices.
  - **Isolation of processing**: while all virtual slices use the same physical resources, independent processing of packets is required.
  - **Isolation of storage**: data related to a slice should be stored separately from data used by another slice

IMPORTANTE: le NF che realizzano la core-network o uno slice girano su piattaforme software in generale diverse che sono all'interno dei vari DCs e tali piattaforme possono essere gestite in vario modo dall'operatore ma anche da terze parti che contribuiscono alla operatività dei DCs stessi

- **MEC**

Security aspects

- In principle the MEC provides inherent security protection due to the isolation and containerization.
- However, the MEC architecture is exposed to a number of threats:
  - The use of open source code, more interfaces, and new APIs introduce new threats.
  - Shared hardware resources can result in cross-contamination.
  - Vulnerabilities in the shared host platform, Container-as-a-Service (CaaS) and Platform-asa-Service (PaaS) can impact the container security.
  - Containers requiring elevated privileges can cause security risk to both host as well as other tenant containers.
  - Dependency upon central orchestration introduces a new threat vector.
  - High data volume and sessions increase risk from an attack.
  - Applications running in a micro-service architecture are as vulnerable to the same attacks as traditional applications
- **Physical security of MEC**
- Improper physical and environmental security of edge computing facilities can lead to destruction of edge computing facilities, un-authorised access at system level as an entry point to all hosted resources, theft of data on local storage.

Standardizzazione e soluzioni per la sicurezza nel 5G

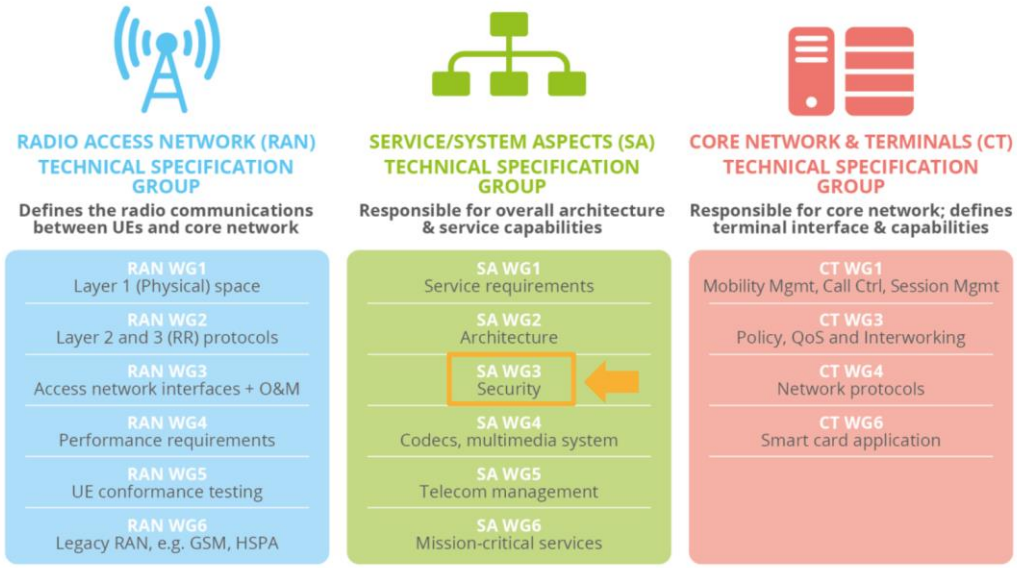
Standardizzazione della sicurezza per il 5G

- Differentemente dai sistemi 4G, il 5G raccoglie ai fini della sicurezza contributi da diversi stakeholders e questo è anche legato all'apertura dell'architettura di rete verso il mondo IETF (es. uso del REST).
- Ci sono quindi molti enti di standardizzazione e gruppi di lavoro che si occupano delle specifiche di sicurezza nel 5G.
- Gli attori principali sono:
  - 3GPP: 3rd Generation Partnership Project
  - ETSI: European Telecommunication Standards Institute
  - ITU: international telecommunication union
  - IETF: Internet Engineering Task Force

  I loro risultati possono contribuire direttamente alla specifica TS 33.501
- Attori secondari (ma non per questo meno importanti)
  - GSMA
  - IEEE

Attività del 3GGP

- The 3rd Generation Partnership Project, or 3GPP, is the main body developing technical specifications for 5G networks, including security specifications.
- **These specifications (Rel. 16 and newer) bring a number of security enhancements in comparison to previous generations of mobile networks.**
- At the same time, however, some of these security controls are defined as optional or there is a degree of flexibility left to suppliers on how to implement and for operators on how to interpret and utilise the controls.
- Having a good understanding of these security controls is important for vendors, system integrators and operators in order to build, deploy and manage resilient 5G networks, but it is equally important for cybersecurity and national regulatory authorities in charge of cybersecurity policy development and implementation.
- In addition to 3GPP, other standardization bodies and industry groups have been working on developing related technical specifications and standards. Some of these standards, such as those related to authentication and encryption, form the basic building blocks of the mechanisms incorporated in 3GPP security specifications.
- Others have been developing specifications in specialized domains and for specific technologies that 5G will heavily rely upon, such as virtualization.



Attività del 3GPP

Attività del 3GPP per la sicurezza del 5G

- L'architettura di sicurezza e le relative procedure per il 5G sono definite all'interno del documento di specifica rilasciato dal 3GPP: **TS 33.501**

SECURITY ARCHITECTURE AND PROCEDURES

- ✓ Security architecture and procedures for 5G system (TS 33.501)

SECURITY ASSURANCE (Vedi presentazione successiva del Prof. Bianchi)

- ✓ Catalogue of general security assurance requirements (TS 33.117)
- ✓ SCAS for the next generation Node B (gNodeB) network product class (TS 33.511)
- ✓ 5G SCAS; Access and Mobility management Function (AMF) (TS 33.512)
- ✓ 5G SCAS; User Plane Function (UPF) (TS 33.513)
- ✓ 5G SCAS for the Unified Data Management (UDM) network product class (TS 33.514)
- ✓ 5G SCAS for the Session Management Function (SMF) network product class (TS 33.515)
- ✓ 5G SCAS for the Authentication Server Function (AUSF) network product class (TS 33.516)
- ✓ 5G SCAS for the Security Edge Protection Proxy (SEPP) network product class (TS 33.517)
- ✓ 5G SCAS for the Network Repository Function (NRF) network product class (TS 33.518)
- ✓ 5G SCAS for the Network Exposure Function (NEF) network product class (TS 33.519)
- ✓ 5G SCAS; Non-3GPP InterWorking Function (N3IWF) (TS 33.520)
- ✓ 5G SCAS; Network Data Analytics Function (NWDAF) (TS 33.521)
- ✓ 5G SCAS; Service Communication Proxy (SECOP) (TS 33.522)

OTHER SECURITY SPECIFICATIONS, STUDIES AND REPORT

- ✓ Study on Lawful Interception (LI) service in 5G (TR 33.842)
- ✓ Lawful Interception requirements (TS 33.126)
- ✓ Lawful Interception (LI) architecture and functions (TS 33.127)
- ✓ Security; Protocol and procedures for Lawful Interception (LI); Stage 3 (TS 33.128)
- ✓ Study on security aspects of 5G network slicing management (TR 33.811)
- ✓ Study on security aspects of enhancement of support for edge computing in 5GC (TR 33.839)
- ✓ Study on security enhancements of 5G System (5GS) for vertical and LAN services (TR 33.819)
- ✓ Study on 5G security enhancements against False Base Stations (FBS) (TR 33.809)
- ✓ Key issues and potential solutions for integrity protection of the User Plane (UP) (TR 33.853)
- ✓ Study on authentication enhancements in the 5G System (5GS) (TR 33.846)
- ✓ SECAM and SCAS for 3GPP virtualized network products (TS 33.818)

REQUIREMENTS FOR USE-CASES

- ✓ Security aspects of MTC and other mobile data applications communications enhancements (TS 33.187)
- ✓ Proximity-based Services (ProSe); Security aspects (TS 33.303)
- ✓ Security aspects of 3GPP support for advanced V2X services (TS 33.536)

OTHERS

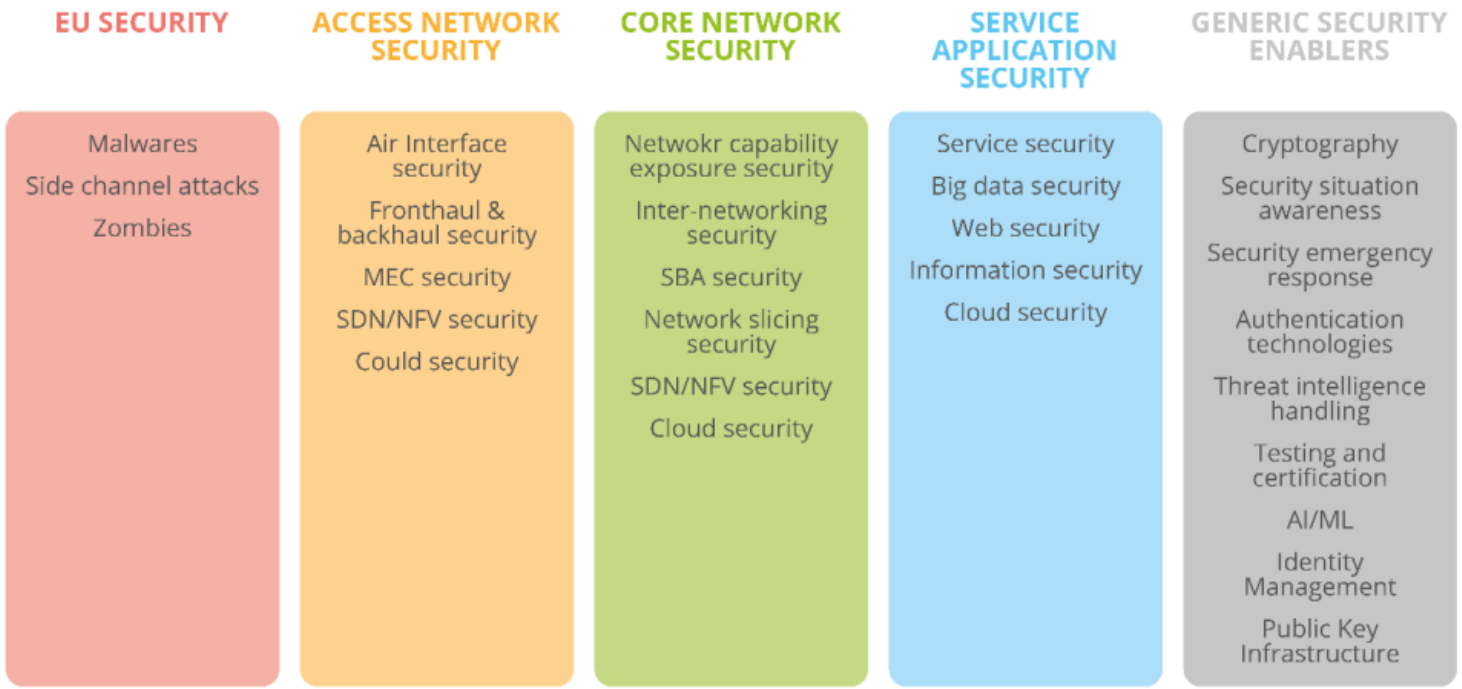
- ✓ Authentication and Key Management for Applications (AKMA) based on 3GPP credentials in 5GS (TS 33.535)
- ✓ Security aspects of Common API Framework (CAPIF) for 3GPP northbound APIs (TS 33.122)

Attività del ETSI

- Anche l'ETSI ha numerosi sottogruppi che si occupano della sicurezza del sistema 5G
- Network Function Virtualisation Security (NFV SEC) working group
- Technical Committee for Cybersecurity (TC CYBER)
  - addressing the security of infrastructures, devices, services and protocols. Their recent work has been related to 'cybersecurity for consumer Internet of Things', 'global cybersecurity ecosystem' and 'techniques for assurance of digital material used in legal proceedings'
- Technical Committee for Lawful Interception (TC LI)
- Technical Committee for Intelligent Transport Systems (TC ITS)
- Industry Specification Group on Securing Artificial Intelligence (ISG SAI)
- Security Algorithms Group of Experts (SAGE)

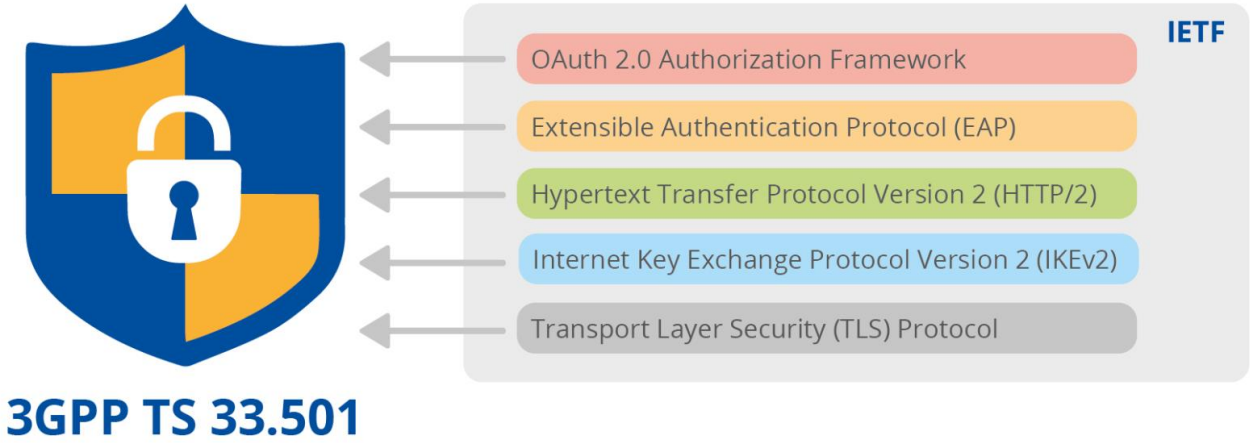
Attività del ITU

- Sono stati istituiti diversi gruppi di studio (SG) che si occupano degli aspetti di sicurezza riportati di seguito.



Attività del IETF

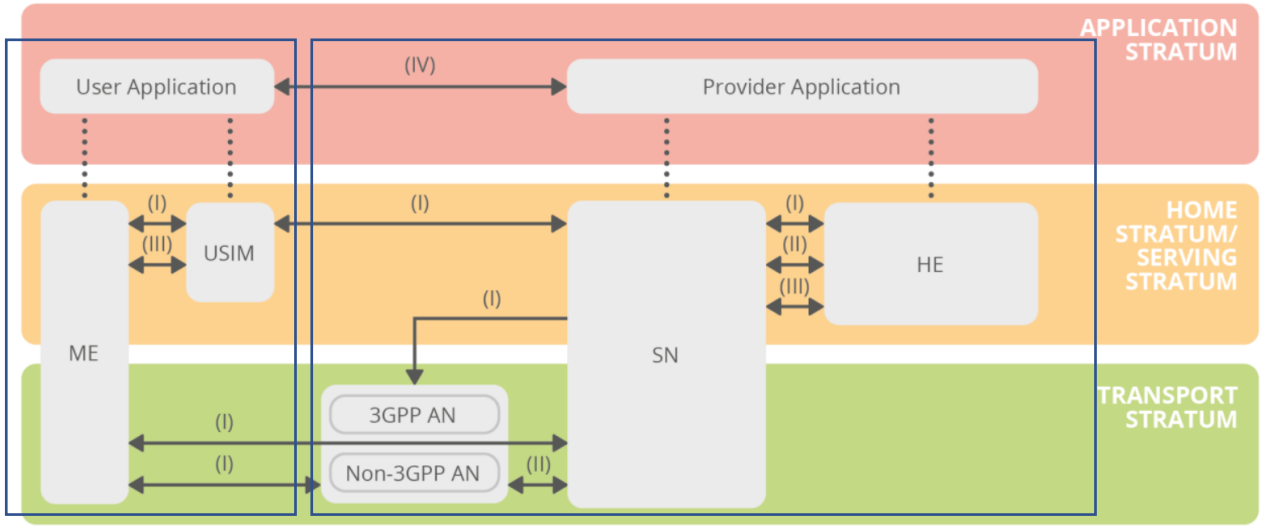
- Attività principali:
- Standardizzazione e aggiornamento del protocollo TLS (v 1.3)
- OAuth 2.0 is the industry-standard protocol for authorization.
  - OAuth 2.0 focuses on client developer simplicity while providing specific authorization flows for web applications, desktop applications, mobile phones, and living room devices. This specification and its extensions are being developed within the IETF OAuth Working Group.



La specifica 3GPP TS 33.501

- **Security architecture**
  - The general UMTS architecture is modelled, at a high level, from both physical and functional viewpoints. The physical aspects are modelled using the **domain concept** and the functional aspects are modelled using the **strata concept**.
  - **Domain:** contiene le entità deputate a svolgere alcune funzionalità specifiche di un segmento della rete (es. Dominio che identifica la sezione di accesso)
- Some clarifications on the infrastructure domain
  - **Serving Network Domain:** The serving network domain is the part of the core network domain to which the access network domain that provides the user's access is connected**. It represents the core network functions that are local to the user's access point and thus their location changes when the user moves.** The serving network domain is responsible for routing calls and transport user data/information from source to destination.
  - **The home network environment** domain represents the core network functions that are conducted at a **permanent location regardless of the location of the user's access point**. The USIM is related by subscription to the home network domain. The home network domain therefore contains at least permanently user specific data and is responsible for management of subscription information. It may also handle home specific services, potentially not offered by the serving network domain.
- I **domini** e gli strati in figura comunicano tra di loro come indicato dalle frecce usando le specifiche funzionalità che garantiscono la sicurezza nella interazione tra le diverse entità del Sistema 5G.
- Gli strati **contengono le entità** alcune elencate di seguito che appartengono **ai diversi domini** (ME, USIM, SN, HE etc.)

Legenda: ME: mobile equipment, SN: service network, HE: home environment



Transport stratum:
- includes: PHY of air interface, transport network in RAN, UPF of core
  - low security sensitivity (enables non-trusted vendors to provide RAN)
  - only utilizes temporary identifiers and keys

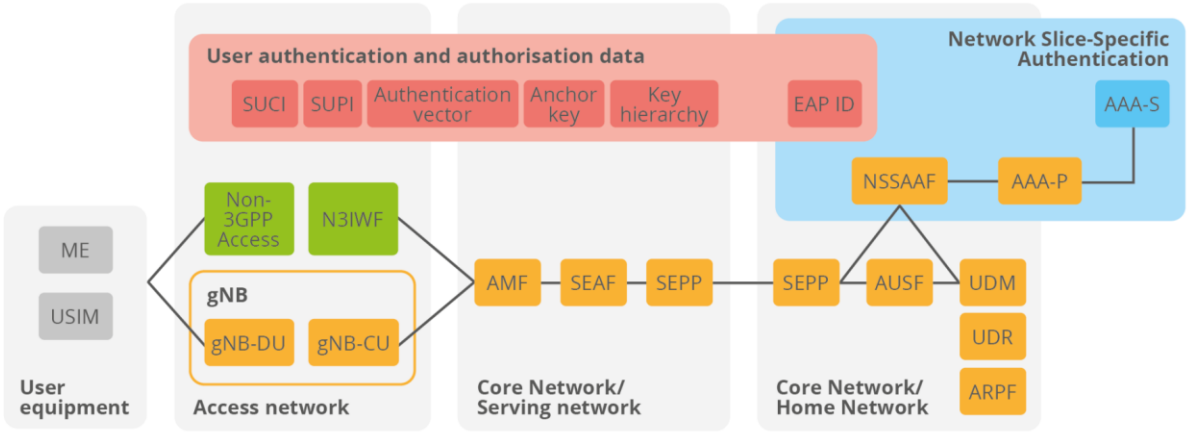
Network stratum - *Serving* Network: contiene
- includes: AMF, NRF, NEF, SEPP, SMF
  - relatively high security sensitivity
  - utilizes mid-level derived keys (such as AMF keys)

Network stratum - *Home* Environment
- includes: UE's SIM, home network's AUSF and UDM
  - high security sensitivity
  - utilizes SUPIs, user root keys, and high-level keys

Application stratum
- includes: MEC, AF, 3d party functionalities, mobile payment
  - responsibility of application service providers
  - separated from mobile networks
  - utilizes end-to-end security

Funzionalità di sicurezza per l'interconnessione delle entità (NFs) nei diversi domini

- **Network access security (I)**
  - enables UE to authenticate and securely access services – mutual authentication, integrity protection, encryption
  - protects against attacks on the air interface and from RAN to serving core
- **Network domain security (II)**
  - protects RAN to core (IPsec) and serving-core to home-core (TLS, PRINS)
  - protects control and user planes
- **User domain security (III)**
  - secures end-user access to UE (passwords, PIN codes, etc)
  - SIM access
- **Application domain security (IV)**
  - enable user applications to exchange messages with provider applications
  - mechanisms provided by application providers and transparent to mobile
- **SBA domain security (V)**
  - enable NFs in the service based architecture (SBA) to securely communicate (TLS)
  - features include NF registration, discovery, and authorization (OAuth)



- Le funzioni per la visibility and configurability of security is not shown in the figure.

Cosa si può fare per combattere le minacce ?

- Strategie: alcune di queste già adottate nei sistemi precedenti ma sensibilmente migliorate nel 5G
  - Physical security – preventing access to communications devices and links
  - Emission security – preventing interception and jamming
  - Privacy enforcement – protecting user's identity and blocking impersonation
  - Authorization – preventing unauthorized access to resources
  - Source authentication – confirming the source of a message
  - Integrity – preventing tampering with messages
  - Confidentiality – preventing eavesdropping
  - DoS blocking – preventing Denial of Service
  - Topology hiding – thwarting traffic analysis
  - Anti-hacking – preventing injection of computer malware

Novità introdotte dalla TS 33.501: riassunto

- Il 5G include numerosi miglioramenti tecnici rispetto alle generazioni precedenti (4G).
- Alcuni di essi saranno illustrati in maggior dettaglio dal Prof. Bianchi nella **successiva** presentazione

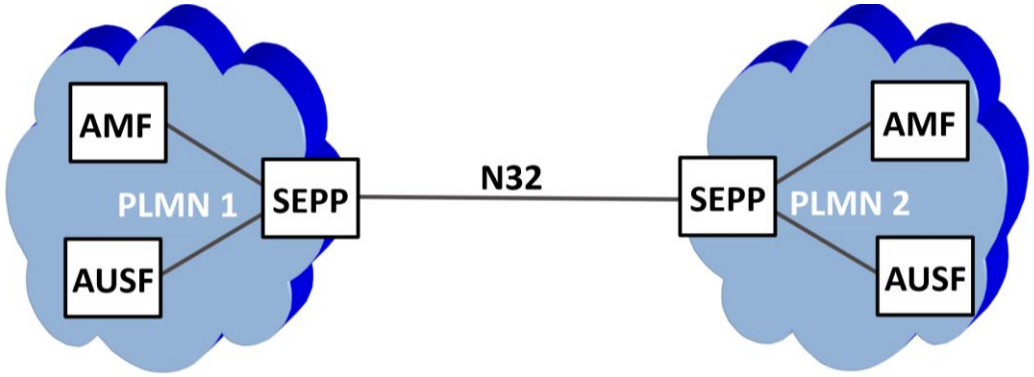
https://www.gsma.com/security/securing-the-5g-era/

Function	LTE	5G
Privacy and Integrity Cipher	•Encryption on radio path between mobile station and eNodeB (LTE base station) •Control plane ciphering and integrity between UE and Mobility Management Entity (MME) •128-bit algorithms supported	In addition to LTE: •Current support of 256-bit algorithms proposed for future release •Integrity implemented preventing unauthorised change of user data.
Authentication Key Agreement (AKA)	•Shared key provisioned in the UICC and the AUSF (Authentication Server Function) in the network. •This provides mutual authentication between the UE and the network.	In addition to LTE: •Access-agnostic authentication (EAP). 5G-AKA and EAP-AKA' supported for both 3GPP and non-3GPP access technologies. •Protects the confidentiality of the initial non-access stratum (NAS) messages between the device and the network.
Security Anchor Function (SEAF) or anchor key	None	Allows re-authentication of the UE when it moves between different access networks or even serving networks without having to run the full authentication.
Subscriber Permanent Identifier (SUPI)	Identifier sent in plaintext prior to network authentication	The Subscription Concealed Identifier (SUCI) provides a mechanism to use the home network public key to encrypt the MSIN part of the subscriber identifier (IMSI). Protecting the confidentiality of the initial non-access stratum (NAS) messages between the device and the network.
Home Control	None	HPMN can verify that the UE is present and requesting service from the VPMN – useful in roaming scenarios and fraud prevention.
Network Exposure Function (NEF)	None	•Network Functions securely expose capabilities and events to 3rd party Application Functions (AF) via NEF. •Enables secure provision of information in the 3GPP network by authenticated and authorized Application Functions. •Certificate based mutual authentication may be used. •After the authentication, NEF determines whether the Application Function is authorized to send requests for the 3GPP Network Entity.
Security Edge Proxy Protection	None	Protects the home network edge, acting as the security gateway on interconnections between the home network and visited networks.

Un esempio a livello di cybersecurity: Network protection

- 5G introduces a new network architecture element: the Security Edge Protection Proxy (SEPP).
- Problem: security issues arose in previous generations when communications bridged several mobile networks (e.g., when *roaming*)
- To solve such problems 5G introduced a perimeter security function called **S**ecurity **E**dge **P**rotection **P**roxy and a new N32 interface
- The SEPP sits at the perimeter of the 5GC and protects all outgoing messages before sending to a 2nd PLMN over N32

- **SEPP receives and verifies all incoming messages on N32 interface before forwarding to the appropriate NF**



The SEPP provides end-to-end protection for application layer control plane messages between NFs belonging to different core networks from being exposed or manipulated by other parties

Un ‘’suggerimento’’ da tenere a mente

- Security technical specifications and standards define controls that make a foundation for development and implementation of secure networks and for development of related security assurance and certification schemes.
- However, many experts agree that “***security posture of a deployed network cannot be realized through standardization alone***”. Based on standards and specifications, suppliers develop network equipment and operators design the overall network, procure, configure and deploy network equipment and manage and operate the network.

We **must** consider **security responsibilities for both suppliers and operators**, it is worth looking at their respective security lifecycle processes, related to product development and network design, deployment and operation.
Example: for suppliers **it could be of interest to define Security Testing and Assurance procedures**. In particular appropriate tests should be defined to ensure that security controls have been correctly implemented. To this purpose, a basic set of predefined test-cases is identified and explained in a series of 3GPP documents that form the SCAS (Security Assurance Specifications) scheme.

La Physical Layer Security (PLS) nel 5G

Non solo cybersecurity !!!

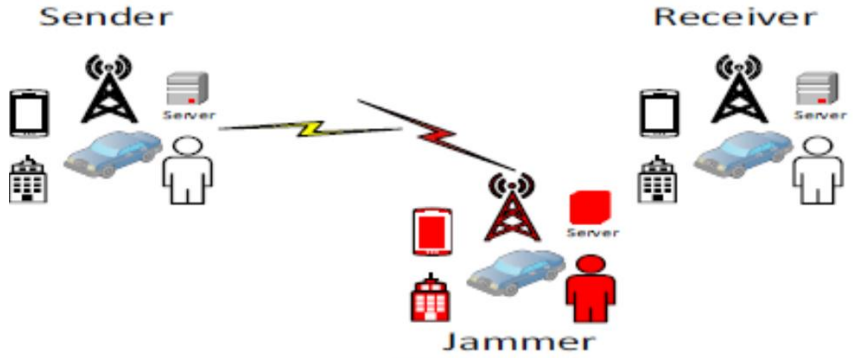
- **Problemi di sicurezza sulla interfaccia radio**
- Sono ben note le numerose minacce che riguardano la rice-trasmissione dei segnali radio
  - (problemi di TRANSEC in gergo militare)
- Alcune di queste sono:
  - Eavesdropping (intercettazioni),
  - Jamming (‘’*marmellamento*’’ 😂 o meglio ‘’**inceppamento**’’)
  - Man in the Middle
  - Distributed DoS
- Tecniche di sicurezza a livello di strato fisico sono utili contro questo tipo di minacce e non solo !!

La Physical Layer Security (PLS)

Minacce tipiche sulla interfaccia radio

Eavesdropping

DDoS



Jamming

MITM

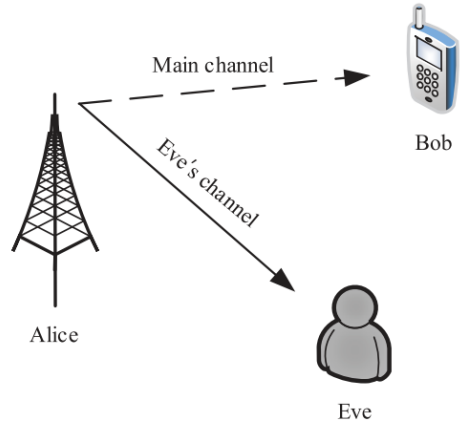
Motivazioni che portano alle tecniche di PLS

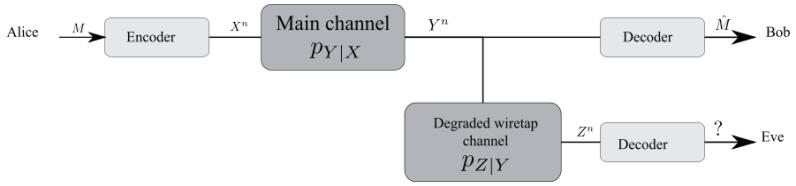
- Alongside the opportunities 5G bring due to such heterogeneous applications, major challenges regarding information security emerge raising more concern about **privacy** than ever before.
- In many use cases, **5G connects critical infrastructure** with highly sensitive and confidential information being transmitted, posing a threat not only for the information conveyed but to the industry and society.
  - In this sense, lightweight, efficient, and service-based security solutions to attend the diverse restrictions of 5G-and-beyond applications are required.
- Traditionally, **network security is provided by bit-level cryptography-based techniques**, carried out at upper layers. However, those methods are limited to satisfy **ALL** the requirements of 5G-and-beyond applications due to the following reasons:
  1. cryptographic methods based on public keys are extremely challenging in large-scale and decentralized networks;
  2. secure links required for the exchange of private keys cannot be guaranteed in some scenarios;
  3. so far, public-key encryption has been unbreakable by using very long key pairs; however, the advance on computational capabilities, such as **advanced quantum computers (vedi Presentazione del Prof. Baldi)**, could crack key pairs in just few hours; thus, **eavesdropping and active attacks** are a high risk in future networks; and
  4. demand for extra delay and complexity to provide strong security are undesirable for some 5G applications, especially those related to URLLC services.
- A new paradigm for providing enhanced security in wireless networks is referred to as **physical-layer security (PLS)**, which can potentially offer secure transmissions by efficiently exploiting the properties of wireless medium and high

Una idea alla base per alcune tecniche di PLS

- **Against eavesdropping:**
- The basic idea behind PLS techniques is **to degrade the channel for eavesdroppers, thus preventing them from gaining information about the confidential messages** from the received signal.
- In this way, PLS techniques can offer an additional level of security, which, integrated with traditional cryptography techniques, can safeguard the highly sensitive data expected to be transmitted over future networks.

- Come fare -> esempio: **generare rumore artificiale !!! (vedi dopo)**



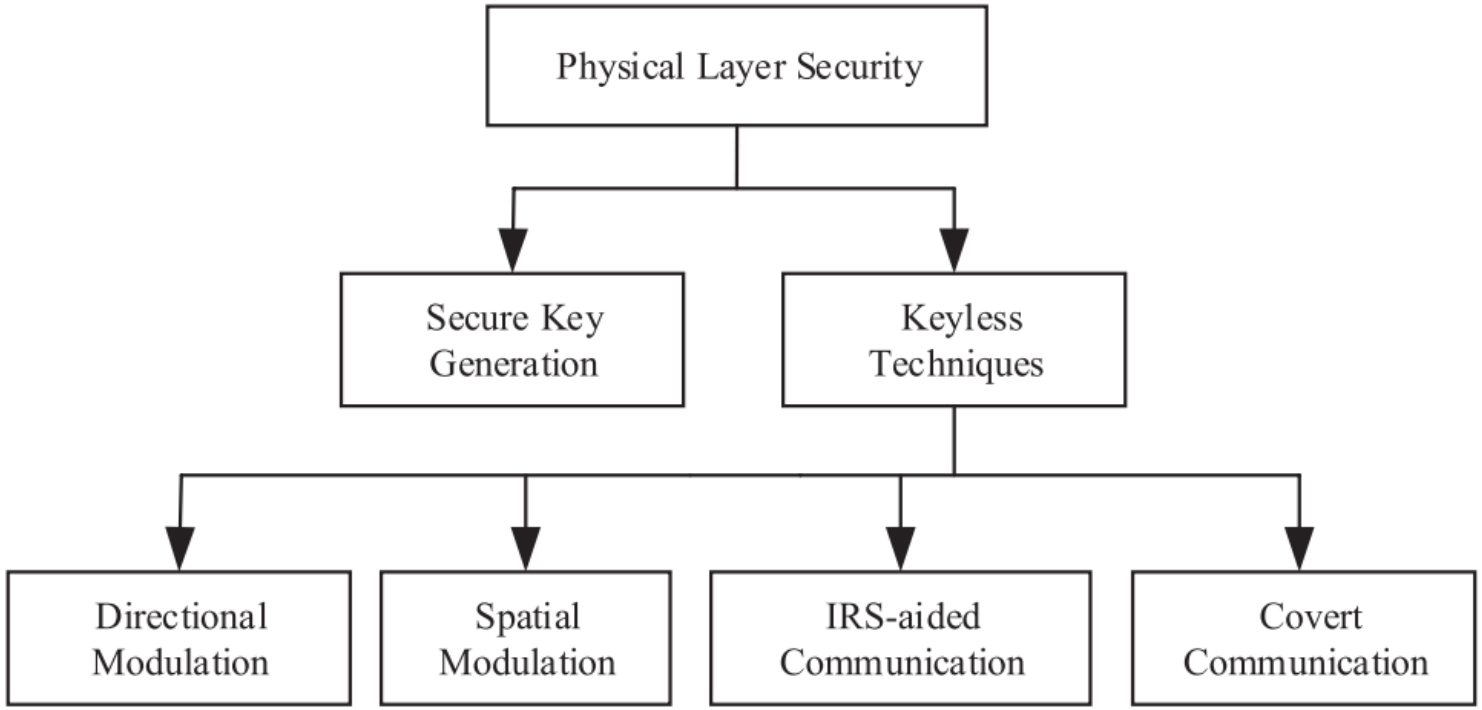


To illustrate how secrecy could be possible over a noisy channel without any encryption mechanism, a degraded additive white Gaussian noise (AWGN) wiretap channel is considered, as shown in Figure. The degraded wiretap channel **[Alice-Eve]** has lower signal-to-noise ratio (SNR) than the main channel **[Alice-Bob]**.

Consequently, for a given binary constellation employed by Alice and Bob, the bit error rate (BER) for the main channel is lower than the BER for the wiretap channel.

Consider that the difference is large enough so that after decoding of the repeated symbols sent by Alice, Bob is able to identify a unique symbol, while Eve can only see a cloud of points all over the constellation, which would make her unable to decode the sent symbol.

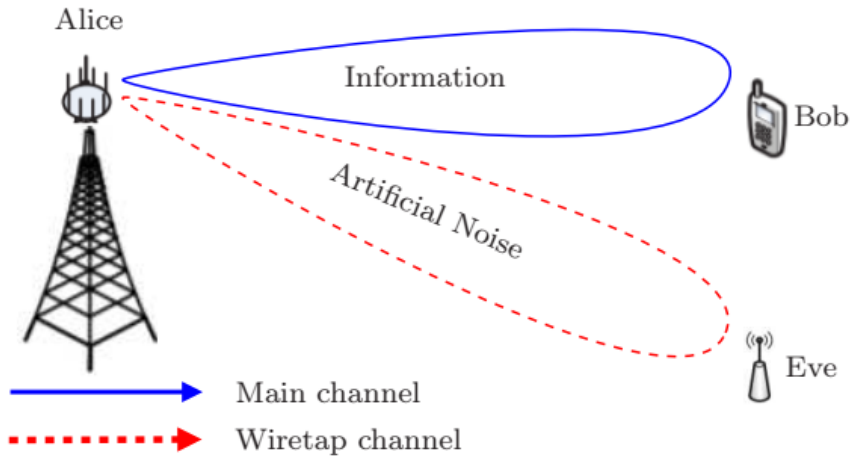
Una classificazione delle tecniche di PLS



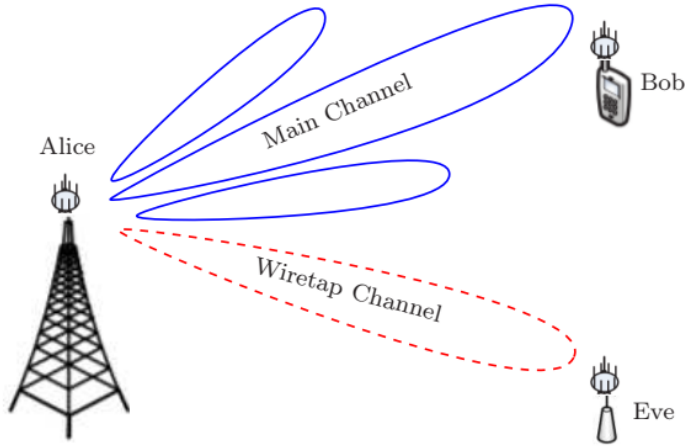
An illustration of PHY security

Caso multi-antenna: MIMO approach

- For this purpose, a trustworthy node, which can be Alice, Bob, or a third one, is in charge of sending an interfering signal (jamming) to intentionally degrade the wire-tap channel and thus hampering Eve's chances on gaining any information from the secret message, while the legitimate channel remains unaffected.Thus, by selectively degrading the eavesdropper's channel, secret c



Rumore artificiale e multi-antenna

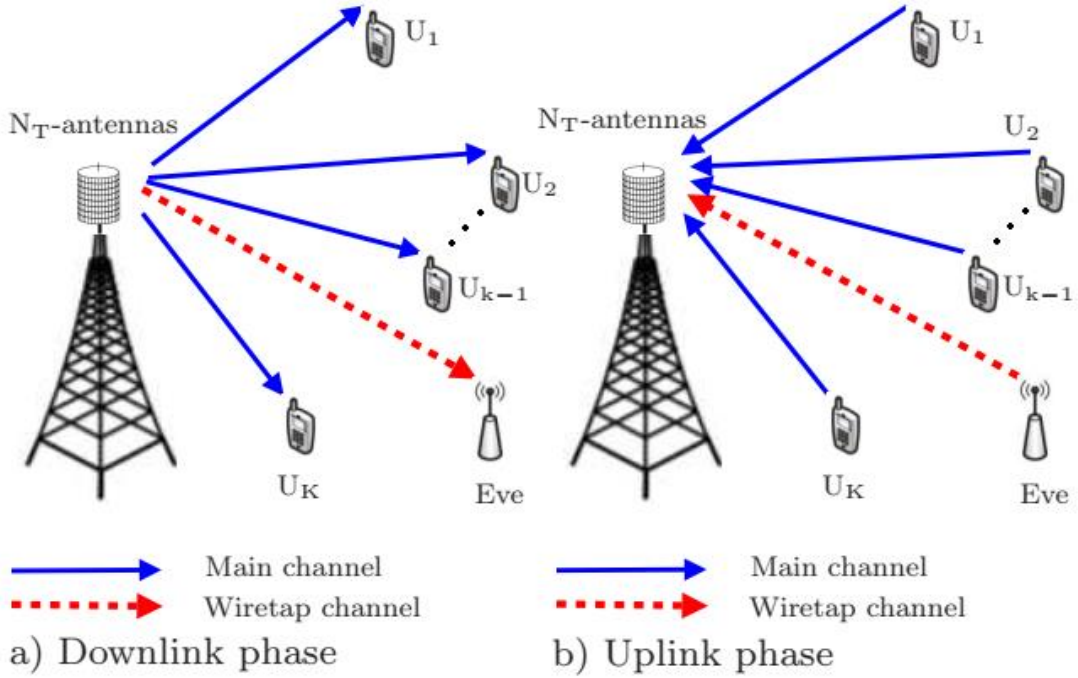


Multi-antenna diversity: oriento il beam verso Eve in modo da creare un canale degradato (es. lobo secondario o metto un nullo)

Ipotesi: posso sapere dove è posizionato l'eavesdropper

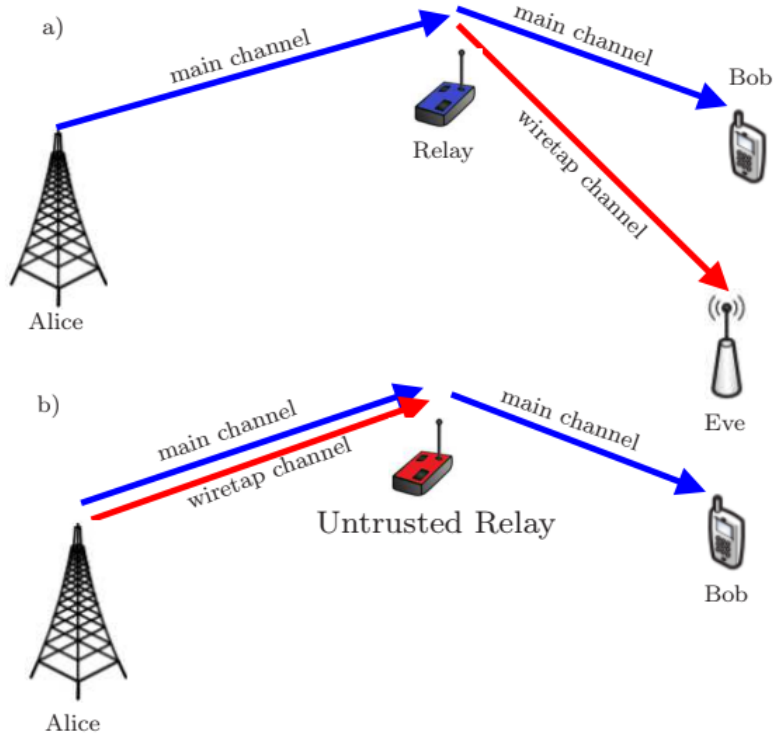
Massive MIMO and security

- For security purposes, massive MIMO gives a very oriented beam guides to the location of the legitimate user. So, the information leakage is reduced to undesired locations (i.e., Eve) significantly
- **This can be applied for both DL and UL**



Caso di cooperative diversity

- Uso di un relay cooperativo
- Cooperative communications:
- Relaying techniques allow the transmitter sends its information to the destination through a relay located between the two nodes.
- The most famous re-transmission protocols are:
  - amplify and forward (AF) (trasparente), and
  - decode and forward (DF) (immagazzinamento e rilancio).
- Relays can be configured in different ways to counteract eavesdropping.
- Specifically, they can behave like a **conventional relay** to attend the legitimate communication (see Fig. (a)), and/or they can also act as jammers by sending AN to degrade Eve's channel.
- **Ma attenzione:** the relay can take the role of potential eavesdroppers when they are untrusted !!!! (Fig.b)
- **Interessante è il caso in cui il relay è un drone.**



PLS per generazione di chiavi per migliorare l'autenticazione

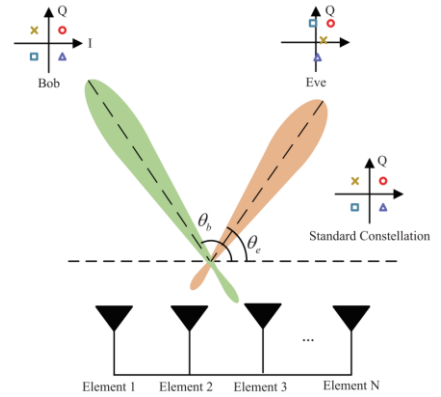
- Authentication methods target to verify the identity of the legitimate parts, thus preventing two types of spoofing attacks: **impersonation and substitution**.
  - In the former, the attacker sends messages to a legitimate receiver in order to be confused with other legitimate users,
  - In the latter, the attacker intercepts legitimate messages, modifies them, and then retransmits the altered messages to legitimate users.
- Moreover, because digital keys are generally used to identify and provide rights to users, attackers using unauthorized security keys cannot be efficiently detected in those scenarios, when physical-layer properties are overlooked.
- Therefore, physical-layer attributes of devices and environments, i.e. *the so-called physical-layer device fingerprints*, can be used to perform authentication with low computational power, energy, and overhead requirements, while being robust as those attributes are hard to be mimicked or predicted. This technique is referred to as **physical-layer authentication (PLA)**
  - Fingerprints can be of two types, channel-based fingerprints or analog front-end (AFE) imperfection-based fingerprints.
  - Channel-based PLA exploits wireless channel parameters such as CSI, received signal strength (RSS), channel frequency response (CFR), and channel impulse response (CIR), in order to design the authentication of devices.
  - As a downside, this approach requires significant channel monitoring, which is subject to imperfect estimates, thus being critical in highly dynamic environments as those of V2X communications.

Problemi: stima accurata del canale; inoltre il canale cambia nel tempo -> aggiornamento dinamico delle chiavi (tracking)

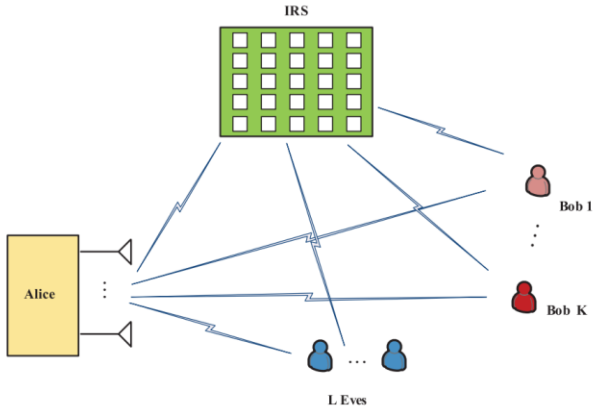
Altre tecniche per la PLS nel 5G

- **Directional modulation (DM):** The DM technique using phased arrays sends information along the direction of the desired receiver, making the constellation diagram of the received signal in the desired receiver direction the same as that of the baseband modulated signal, while the constellation diagram of the received signal in the undesired direction will be distorted, thus ensuring the safe transmission of information.
- **Covert communication:** In covert communication, when the transmitter transmits a message to the receiver, **it is guaranteed that the probability that the illegal watcher can detect the transmission is small enough**. Covert transmission technique, as an important secure transmission technique, **aims to hide the transmission behavior of the transmitter.** Compared to PHY security techniques that aim to prevent the transmitted content from being overheard by Eves, covert communication techniques can achieve a higher level of communication security.
- **Intelligent reflecting surface (IRS)-aided communication:** An IRS is an artificial surface made of electromagnetic material and composed of a large number of passive reflective units. **By configuring these reflective units to act on the phase shift and amplitude of the incident signal, fine-grained three-dimensional beamforming can be achieved, which can be used to improve channel quality, enhance received power, and extend the communication distance.** IRS transforms the traditional uncontrollable and random wireless communication environment into a programmable and relatively deterministic transmission space, and plays an active role in the signal transmission process.
- By introducing IRS into the security system, the security of the system can be further enhanced.

PHY security with IRS is entirely dependent on the ability of the IRS system to precisely direct the signal beam to the expected path **and eliminate** it when directed to Eve(s).



Directional Modulation (DM)



Conclusioni

- The purpose of 5G is to open the network up to a wider set of services and allow the mobile operators to underpin these services.
- It is an opportunity to protect services and consumers from many of today's threats. 5G comes with many built-in security controls by design, developed to enhance the protection of both individual consumers and mobile networks; this is more efficient that post-deployment add-on or extras.
- Advancement of technology and use of new architectures and features such as network slicing, virtualisation and cloud will introduce new threats that require new types of controls to be implemented.
- Come evidenziato in sede normativa Europea è fondamentale garantire la sicurezza del 5G focalizzando l'attenzione anche sui vendor degli apparati 5G
- La superficie di attacco del 5G è molto estesa
  - Attacco a livello di infrastruttura fisica –> rete di accesso –> tecniche PLS possono essere di interesse
  - Attacco a livello dei servizi e delle funzionalità di rete –> cybersecurity
  - Le soluzioni di sicurezza basate sul paradigma Zero-Trust sono di estremo interesse per il 5G.
    - **L'approccio zero trust alla sicurezza merita un seminario a parte.**
- Ricapitolando:
  - Sono stati discussi gli aspetti principali della sicurezza nel 5G
  - Sono stati elencati i principali enti coinvolti nella sicurezza per il 5G e le loro attività
  - Sono stati accennati alcuni problemi legati alla sicurezza a livello di interfaccia radio: problema del eavesdropper e soluzioni basate sulle tecniche di PLS.

Riferimenti essenziali

[1] ETSI TS 123.101 -Universal Mobile Telecommunications System (UMTS); General UMTS Architecture (2000-01)

[2] 3GPP TS 33.501 - 5G; Security architecture and procedures for 5G System (3GPP TS 33.501 version 16.3.0 Release 16) 2020-08

[3] ENISA THREAT LANDSCAPE FOR 5G NETWORKS Updated threat assessment for the fifth generation of mobile telecommunications networks (5G) (updated 2020)

[4] ENISA SECURITY IN 5G SPECIFICATIONS Controls in 3GPP Security Specifications (5G SA) (February 2021)

[5] NIS cooperation Group, EU coordinated risk assessment of the cybersecurity of 5G networks, Report 9 October 2019

[6] The Wiley 5G REF: Security, Editors-in-Chief Rahim Tafazolli, Wiley 2021

[7] Weiping Shi, Xinyi Jiang , Physical layer security techniques for data transmission for future wireless networks, Information Network, et al. 2022

Backup

Esempio: subscriber and device protection

- **5G improves confidentiality and integrity of user and device data.**
- Unlike previous generations of mobile systems 5G:
  - Protects the confidentiality of the initial non-access stratum (NAS) messages between the device and the network. As a result, it is no longer possible to trace user equipment (UE) using current attack methodologies over the radio interface; protecting against man in the middle (MITM) and fake base station (Stingray/IMSI catcher) attacks.
  - Introduces a protection mechanism called **home control**. Meaning the final device authentication to a visited network is completed after the home network has checked the authentication status of the device in the visited network. This enhancement will prevent various roaming fraud types that have hampered operators historically, and support the operator's requirement to correctly authenticate devices to the services.
  - Supports unified authentication across other access network types e.g. WLAN, allowing 5G networks to manage previously unmanaged and unsecured connections. This includes the possibility of performing a re-authentication of the UE when it moves between different access or serving networks.
  - Introduces user plane integrity checking, ensuring the user traffic is not modified during transit.
  - Enhances privacy protection with the use of public / private key pairs (anchor keys) to conceal the subscriber identity, and derive keys used throughout the service architecture (vedi prima: SUCI, SUPI)

EU 5G security toolbox

- The EU member states have agreed on a toolbox of mitigating measures to address security risks related to 5G rollout :
  - Strengthening the role of national authorities
  - To restrict supply, deployment and operation of 5G network equipment
  - Performing audits on operators
  - Assessing the risk profile of suppliers to identify **H**igh **R**isk **V**endors
- including vendors with a strong link to the government of a 3rd country
  - Controlling the use of Managed Service Providers (MSPs)
  - Ensuring the diversity of suppliers
- to avoid major dependency on a single supplier
  - Strengthening resilience at the national level
  - Identifying key assets and fostering diverse/sustainable 5G ecosystem
  - Maintaining diversity and EU capacities in future network technologies

Cosa fanno le istituzioni a livello Europeo per l'uso del 5G per i sistemi critici ?

- At EU level, security requirements relevant to the 5G networks ecosystem and related critical systems are set out notably in EU telecoms legislation and in the NIS Directive.
  - Given the foreseen interdependencies between 5G networks and many other systems in critical areas (e.g. health, autonomous vehicles, power, gas and water supply, defence), degradation or failure of 5G services may lead to significant disruptions of these systems.
  - Conversely, other critical infrastructures upon which 5G networks are dependent, such as power grids and ICS systems, have known vulnerabilities that can be the targets of cyber-attacks.
- Under the EU telecommunications framework, obligations can be imposed on telecommunication operators by the relevant Member State(s) in which it is providing service. The NIS Directive requires operators of essential services in other fields (energy, finance, healthcare, transport, water, etc.) to take appropriate security measures and to notify serious incidents to the relevant national authority.
  - The NIS Directive also foresees coordination between Member States in case of cross-border risks and incidents.
    Other relevant frameworks at EU and national level include data protection and privacy rules (in particular the General Data Protection Regulation18and e-Privacy Directive19) as well as requirements applicable to critical infrastructures.
- At national level, Member States have adopted diverse approaches to the implementation of the aforementioned security provisions and to their enforcement. Where binding rules apply to mobile network operators, they may cover different types of technical and organisational measures.
- In addition, various security measures may already be applied by mobile network operators, for instance: technical measures (e.g. encryption, authentication, automation, anomaly detection) or process-related measures (e.g. vulnerability management, incident and response planning, user-privilege management, disaster recovery planning).
- From a standardisation perspective, 3GPP SA3 has addressed several 5G security related concerns, advocating, inter alia, end-to end encryption. However, the work carried out within these bodies does not deal with security concerns related to the deployment and configuration of the technology