TCAI
TECHNOCRAFT CENTRE FOR APPLIED ARTIFICIAL INTELLIGENCE IIT BOMBAY

International Conference on 5G Network Security

9th & 10th Aug 2023

Vulnerability in 5G core and Mitigation Approaches

Manjesh Kumar Hanawal
IIT Bombay

Team Members: Shubhda Gadgil, Anjali Sharma, Sanjay Mehta

5G has brought in a paradigm shift in telecom technologies. With uRLLC, eMBB, and mMTC as three core pillars, the 5G is revolutionizing various domains. While its modular design principles using open standards have reduced the entry barriers for innovators, they are also lucrative targets for cyber threat actors. Since 5G networks are evolving as nations' critical infrastructure, their security is paramount.

Prof. Manjesh Hanawal, IIT Bombay

Vulnerability in 5G core

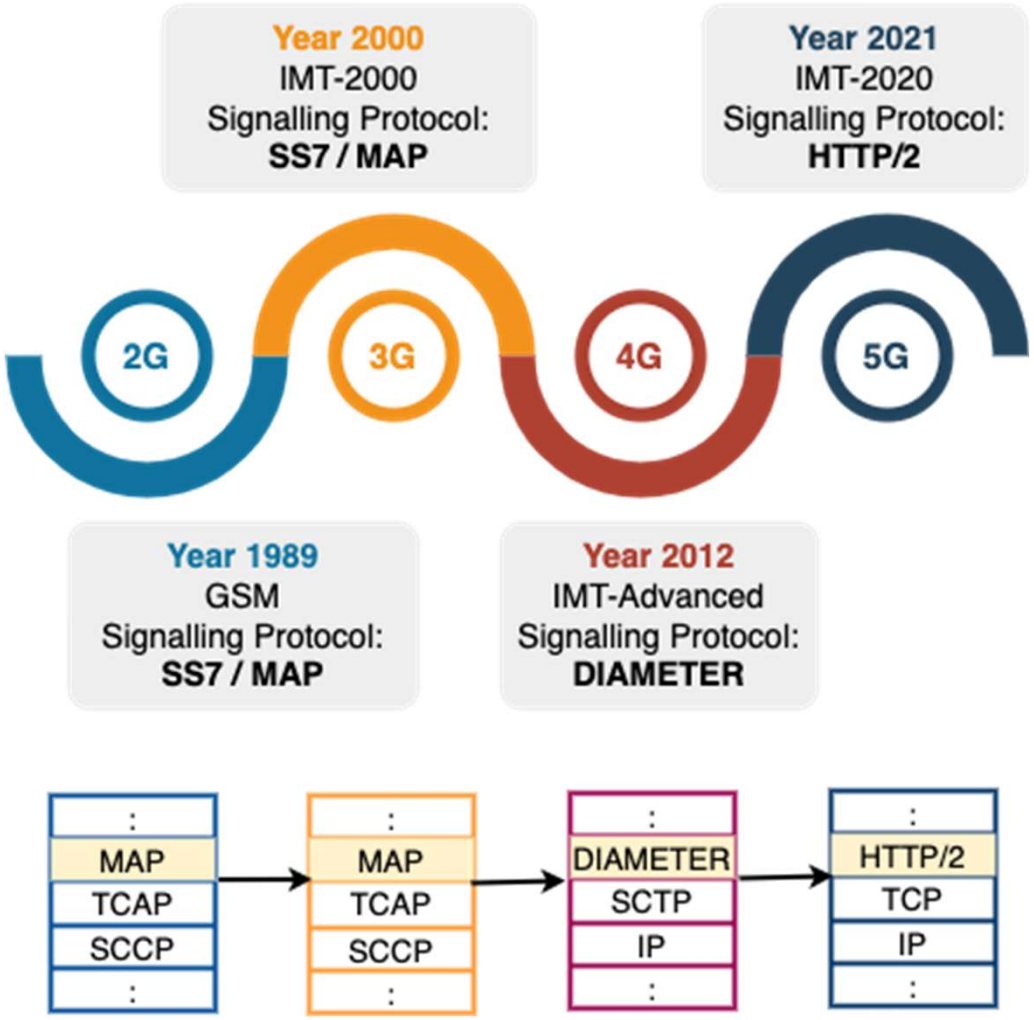
Evolution of Protocol Stack

Mobile network core signaling protocols evolved from **niche telecom-specific closed protocols to well known web-based protocols.**

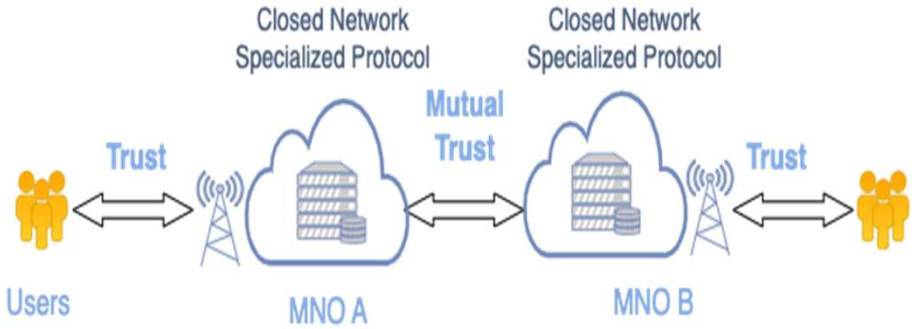
- HTTP/2 and JSON as application layer and serialization protocols, replacing Diameter.
- TCP with TLS providing encrypted communication between NFs and public land mobile network
- RESTful framework with OpenAPI as the Interface Definition Language (IDL).

As these protocols are used in the wider IT industry it will likely lead to

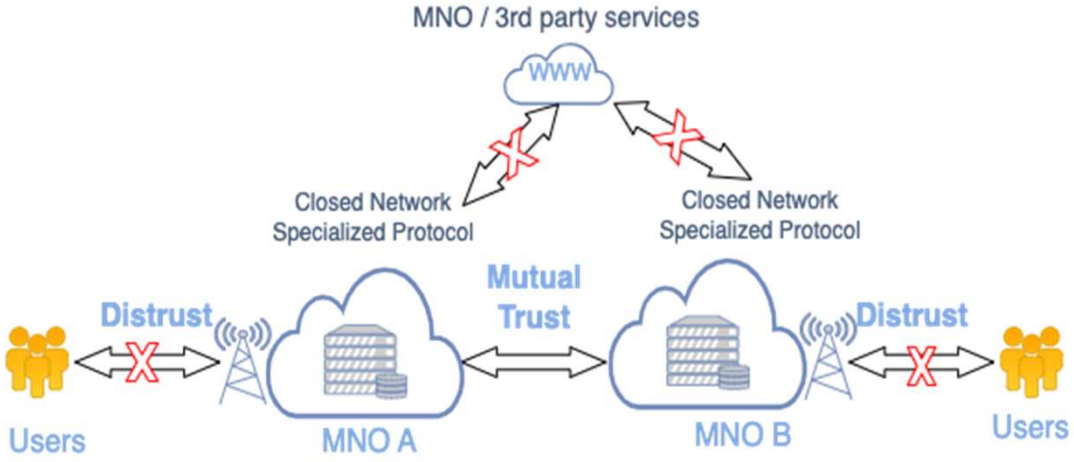
- **A shorter vulnerability to exploitation timeline**
- **Higher impact of vulnerabilities**



Evolution Of Trust Models



2G Trust Model

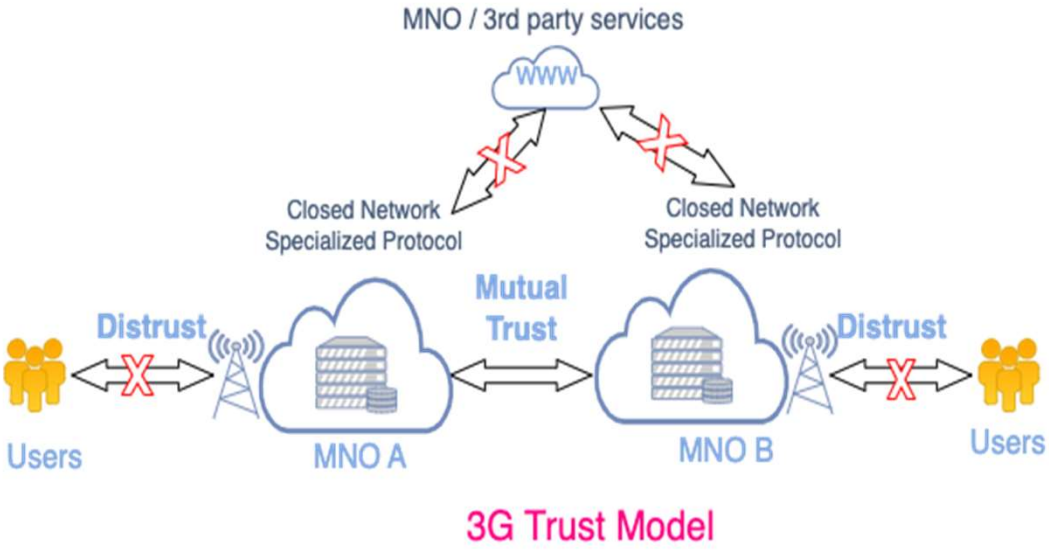


3G Trust Model

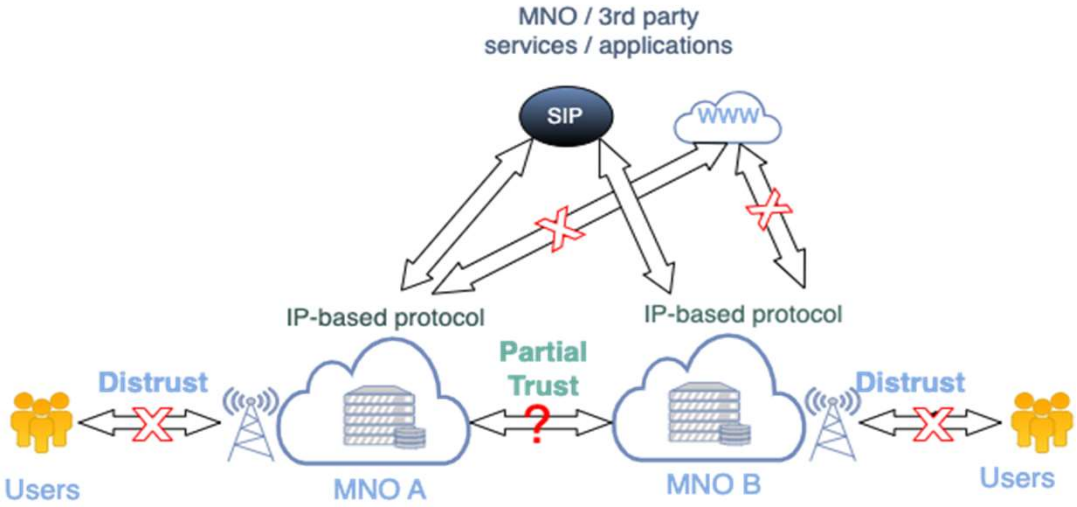
Full trust to trust only at the core

MNO: Mobile Network Operator

Evolution Of Trust Models



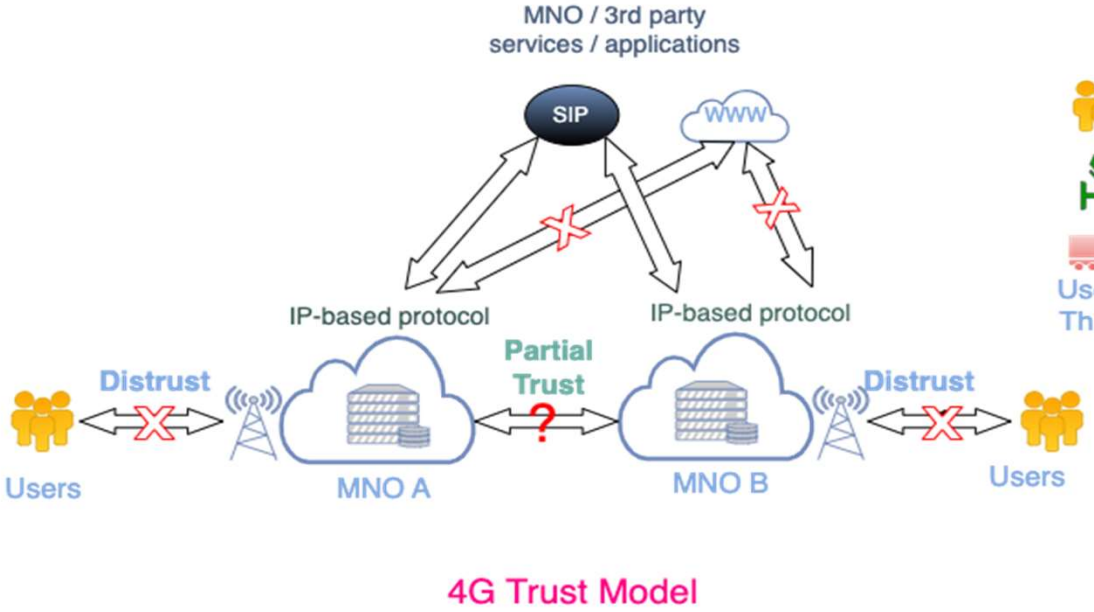
3G Trust Model



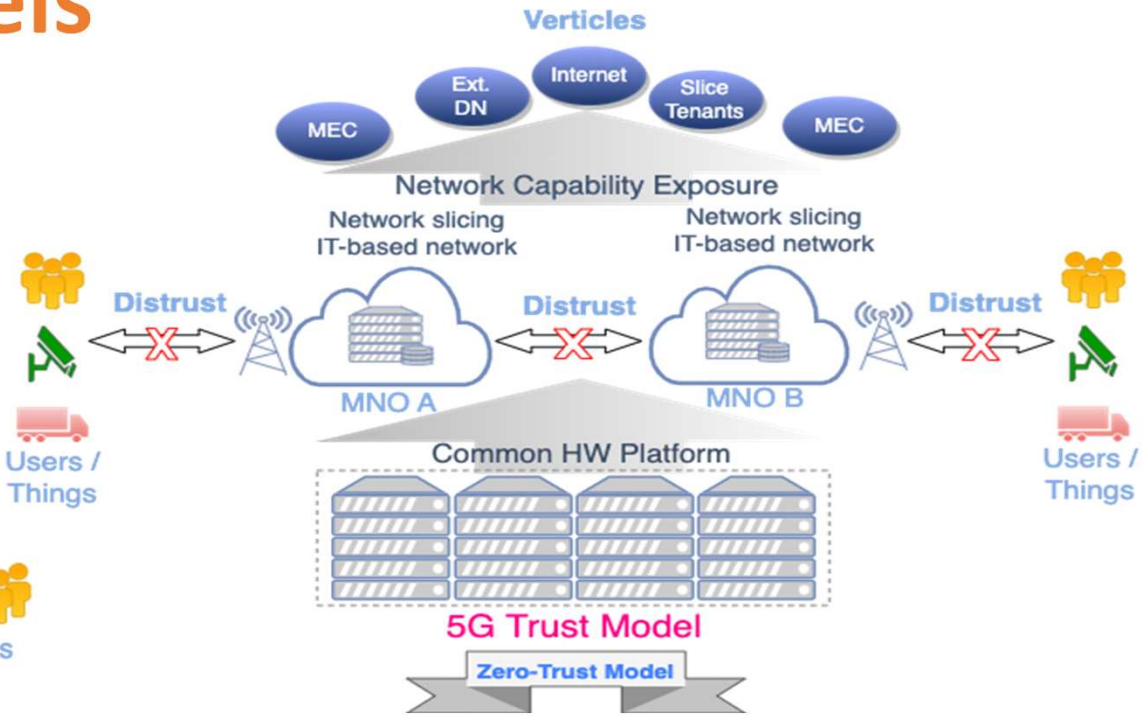
4G Trust Model

Trust at the core to partial trust at the core

Evolution Of Trust Models

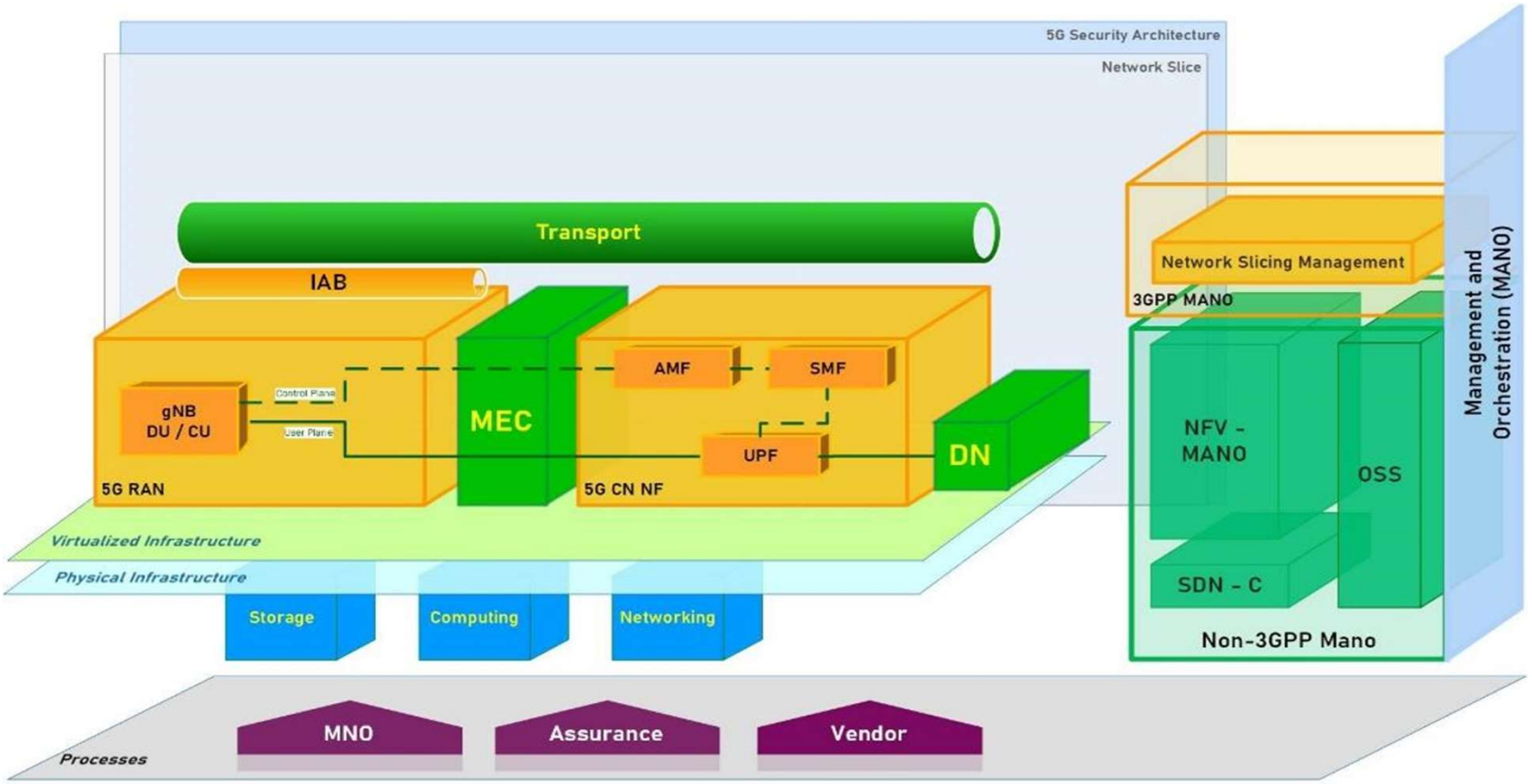


4G Trust Model

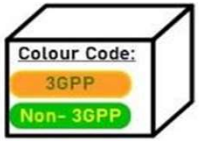


Partial trust to zero trust

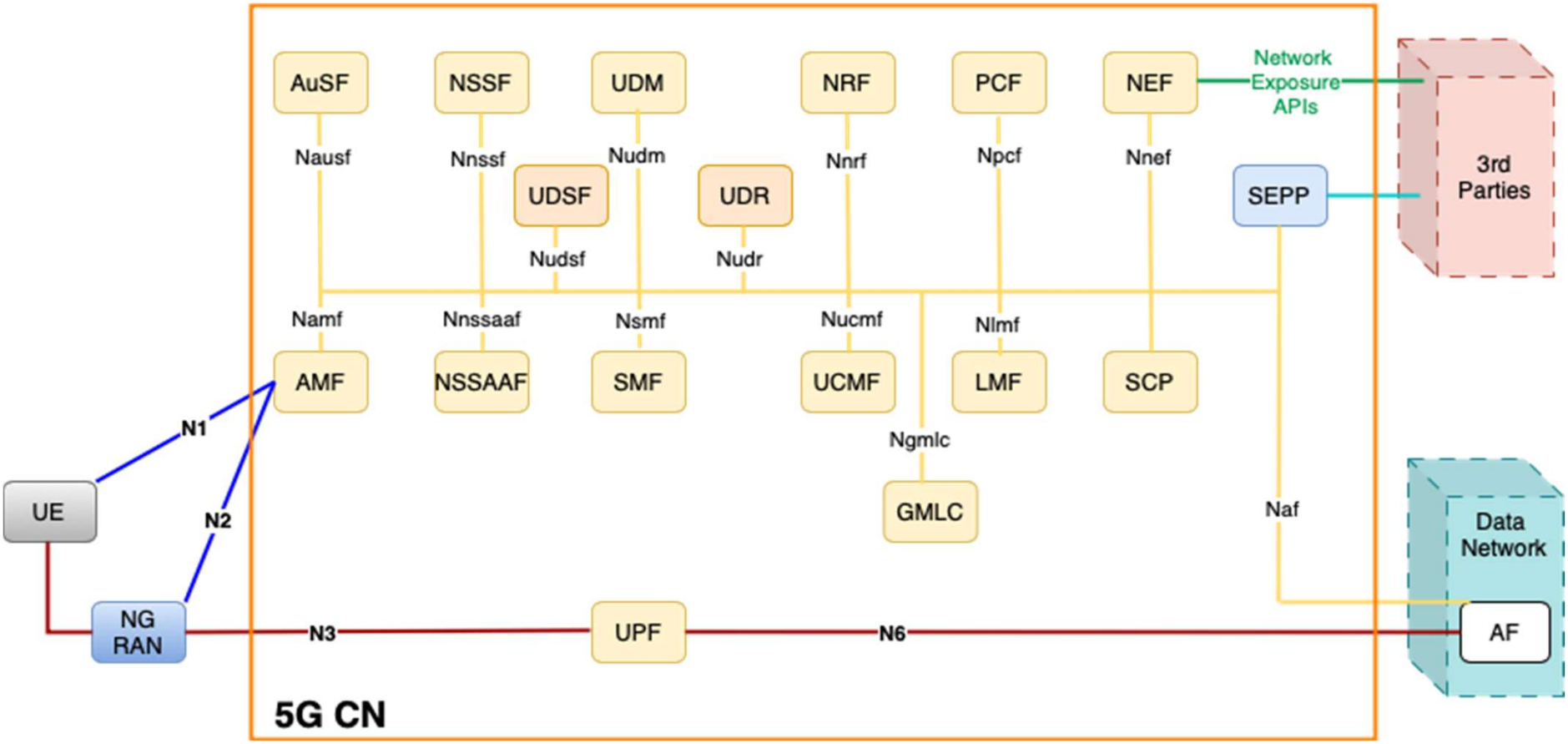
5G Generic Architecture



MNO: Mobile Network Operator
IAB: Integrated Access and Backhaul
DN: Data Network
MEC: Multi-Access Edge Cloud

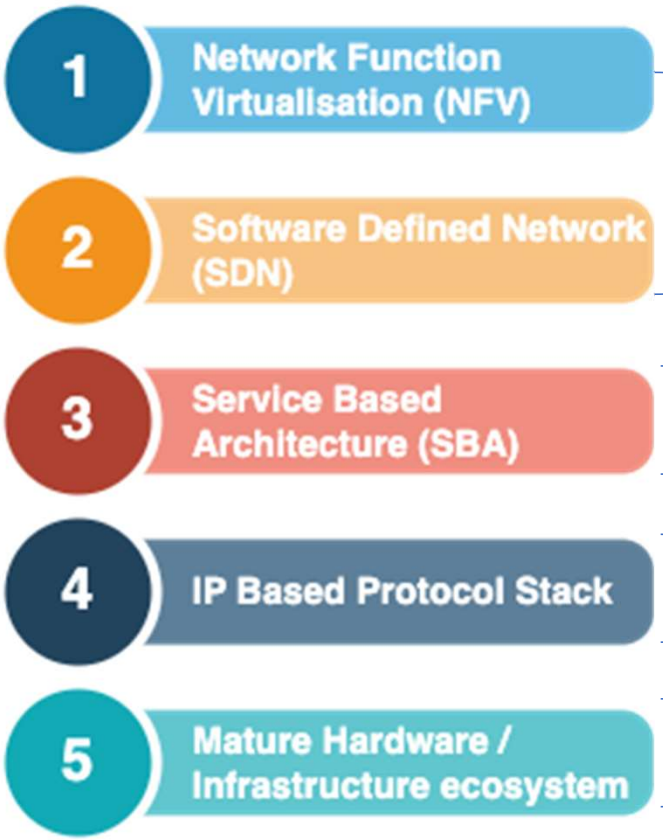


5G Core Network architecture



5G Core network structure as defined by 3GPP
(Service Based Architecture)

Key Components/Technologies enabling 5G Core



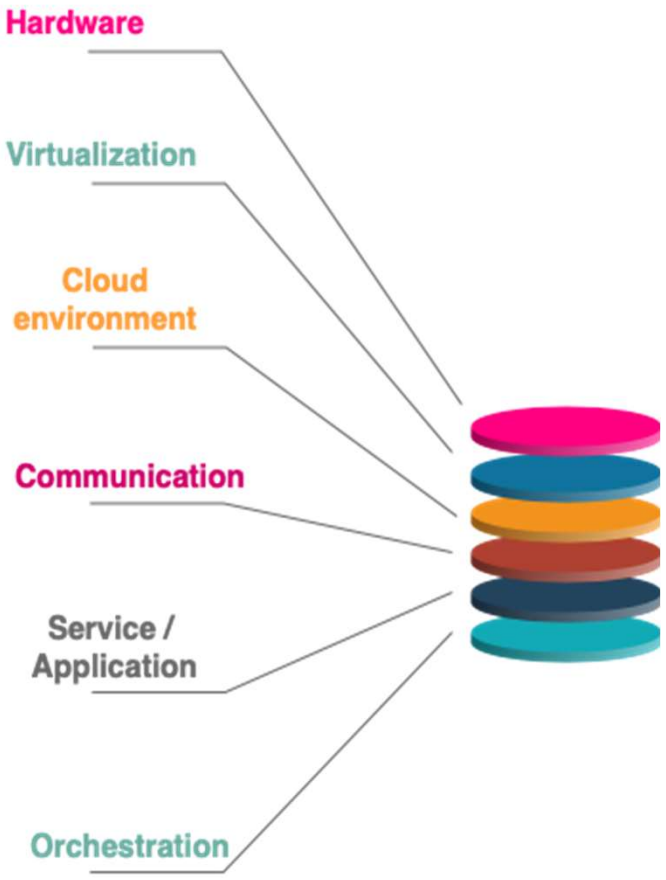
- Improve the network elasticity.
- Break the barrier of vendor-specific or proprietary solutions.
- Enable **softwarisation** of 5G core network functions (NFs) / microservices.
- Easier portability and higher flexibility.
- introduce new and complex threats.

- Enable microservice architecture.
- Flexibility of developing new services and easy integration without introducing new interfaces.
- APIs based interaction among NFs with web protocols

- Built on well-known **Internet protocols** such as HTTP and TLS
- Internet technologies are open and well known to attackers
- Less complex than niche telecom specific protocols like SS7, DIAMETER
- Lowering of entry barrier creates more permissive conditions for attacks

- Cloud based deployment
- introduce new and complex threats.

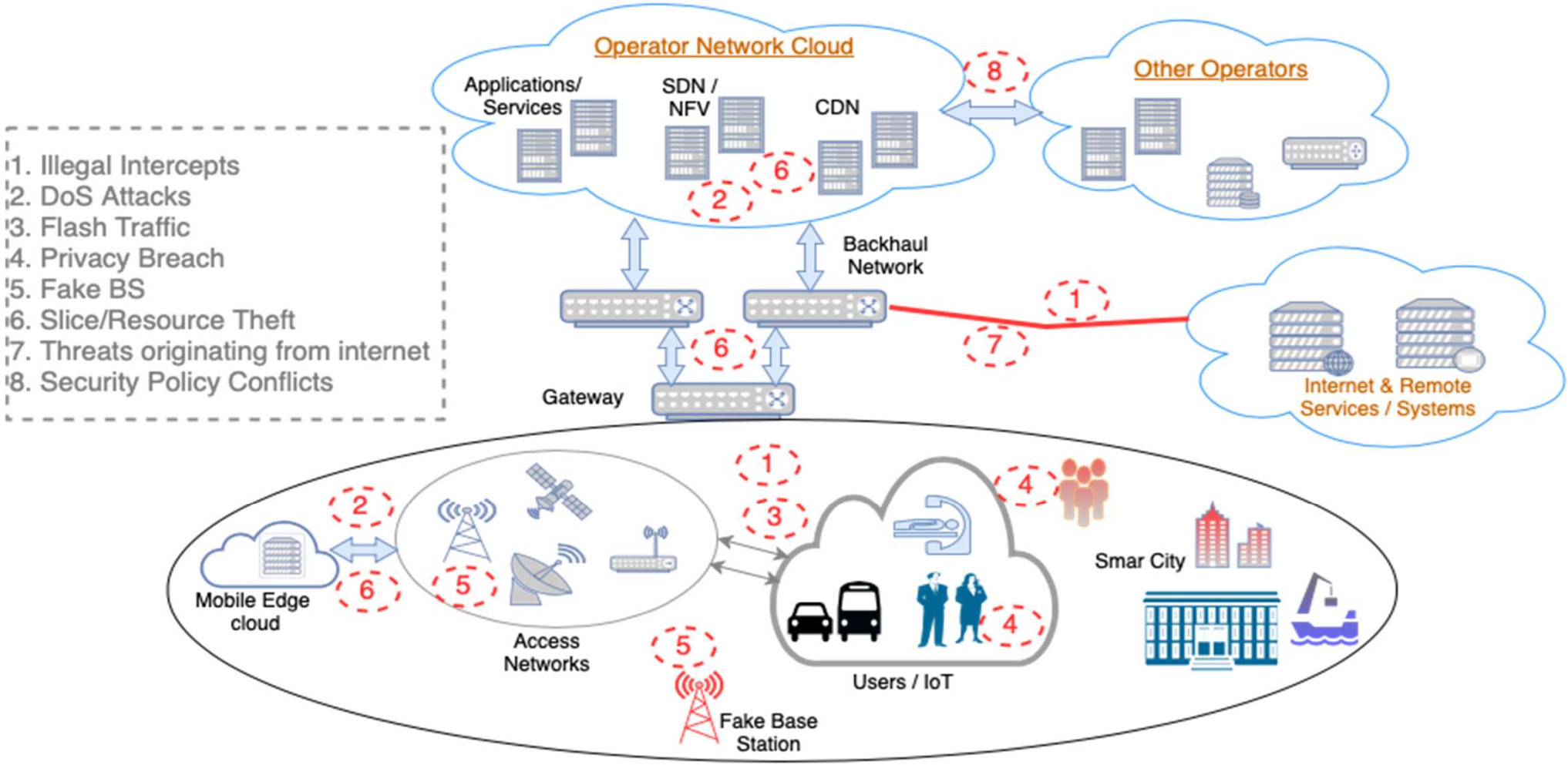
Threat Sources Landscape



Layers	Threat examples
hardware	Hardware backdoors, hardware bugs
Virtualizations	Sandbox escape, hypervisor compromise, shared memory attacks
Cloud	Unlimited control cloud providers over everything it runs
Communications	Classical attacks on the network stack, DDoS, MITM, Sniffing, Spoofing
Service/Application	Sql injection, broken authentication and access control
Orchestration	Registering malicious node and redirecting communication to them

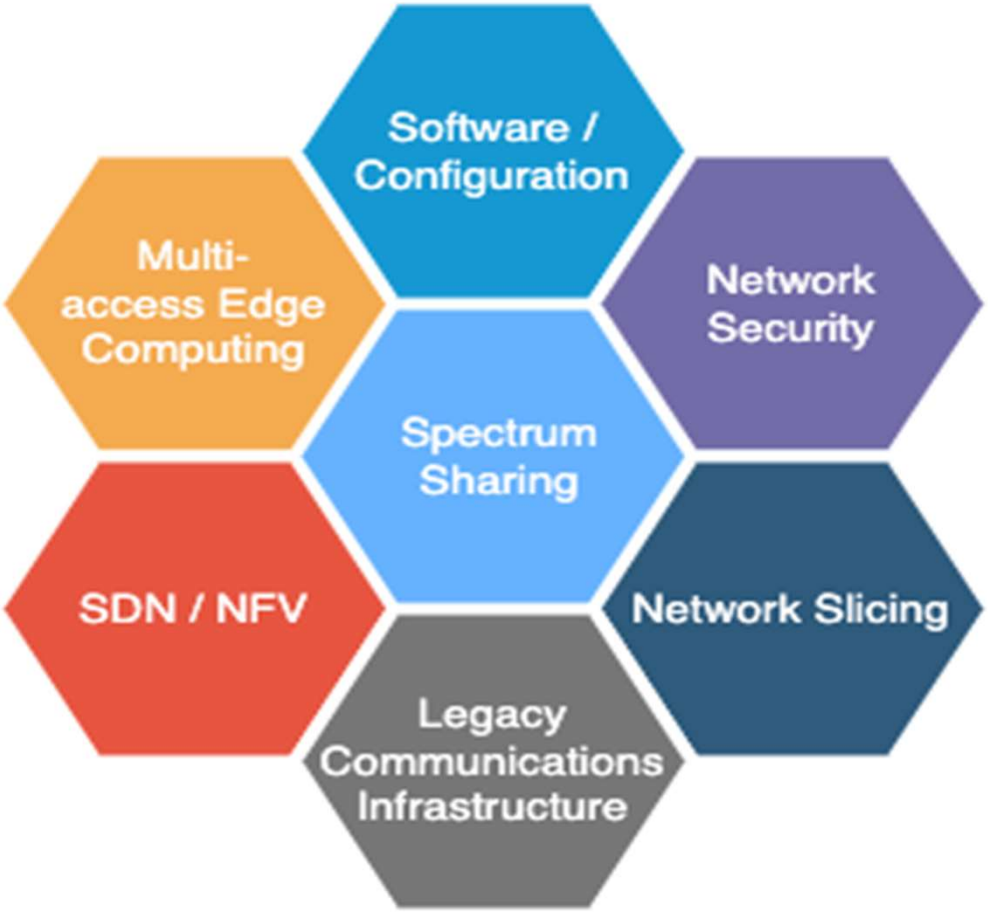
* This layered categorization is not claimed as complete, but it gives a good overview of threat sources

Security Threat Landscape



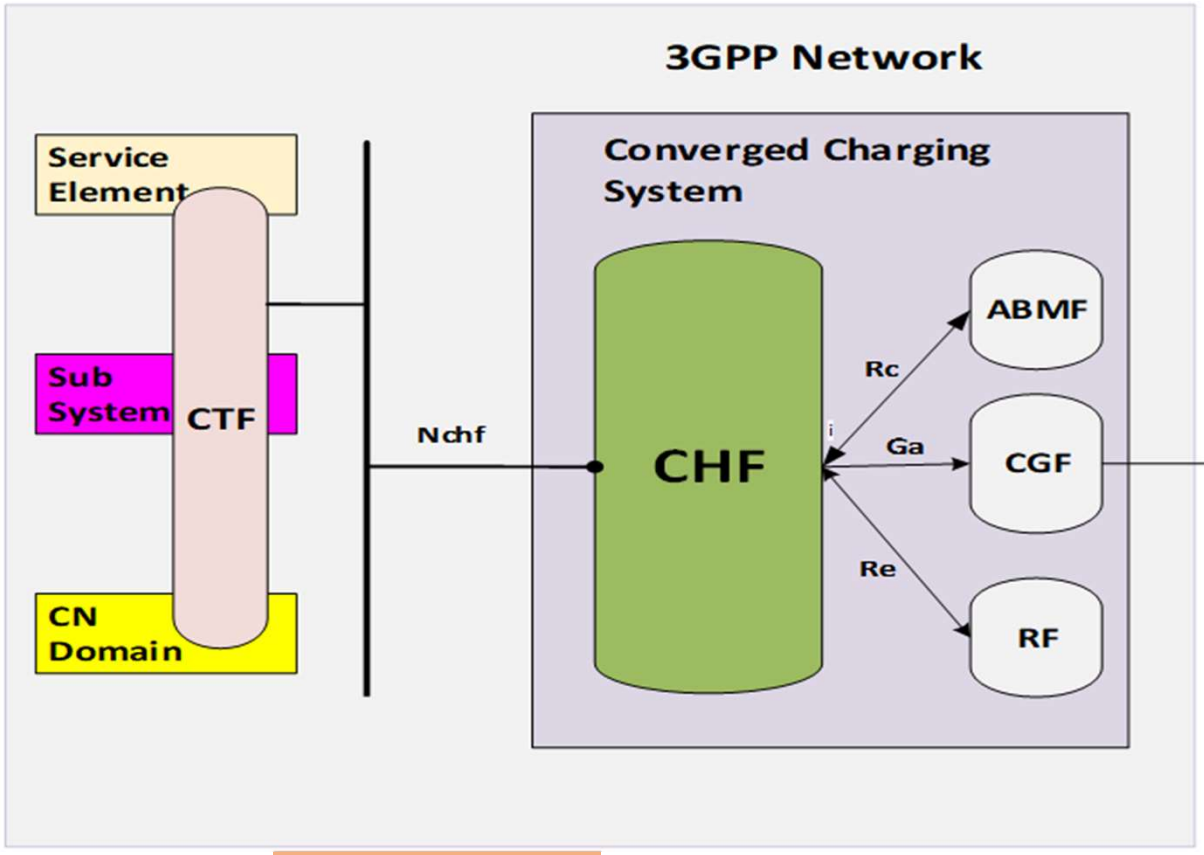
ITU: Security threat landscape in 5G networks

5G Systems Architecture Sub-Threat Vectors



ESF *Potential Threat Vectors to 5G Infrastructure* white paper, released in May 2021,

Legacy Communication Infrastructure Example



Rc - Diameter Based Interface

Ga - GTP Prime Based Interface

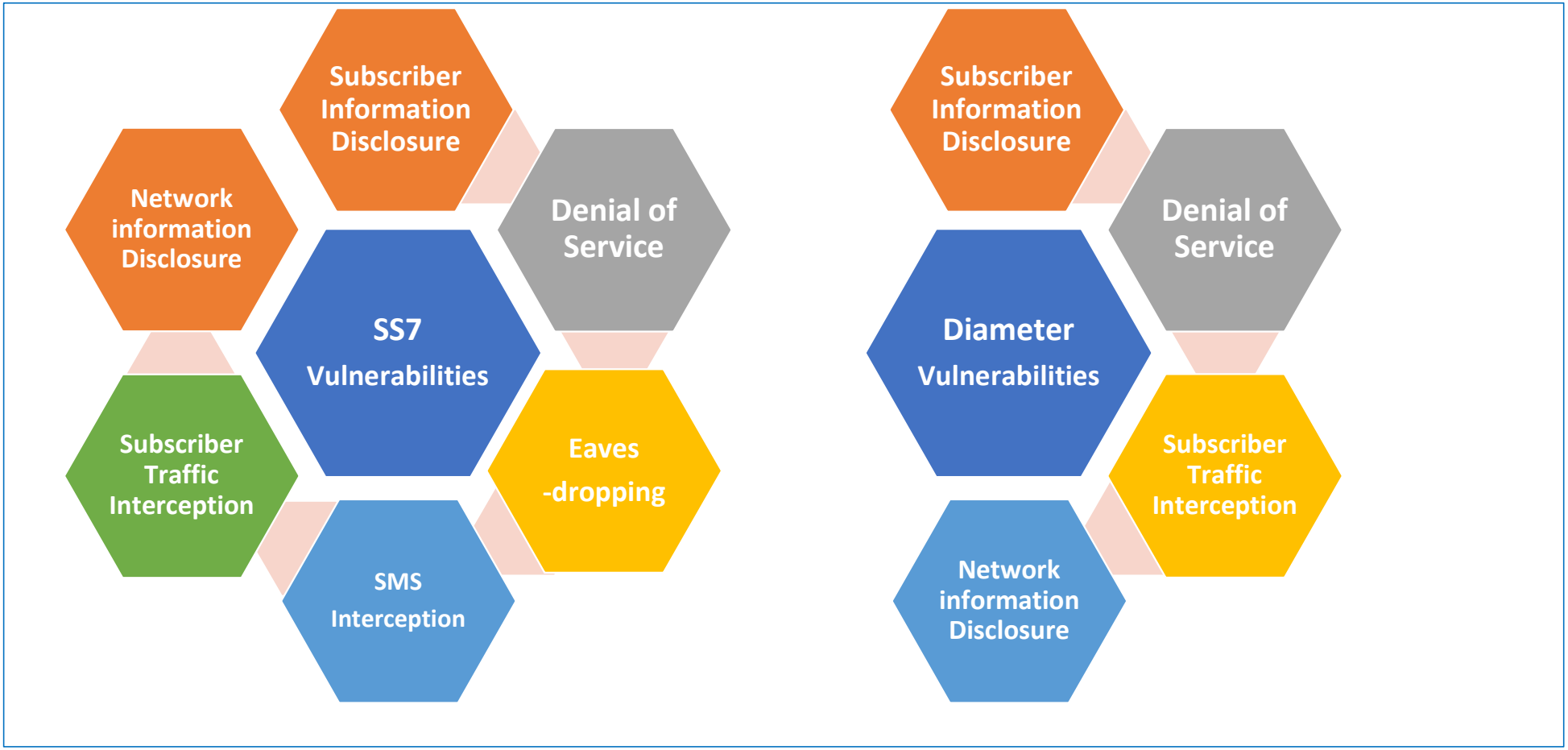
-

Re - Diameter Based Interface

Nchf Service Based Interface

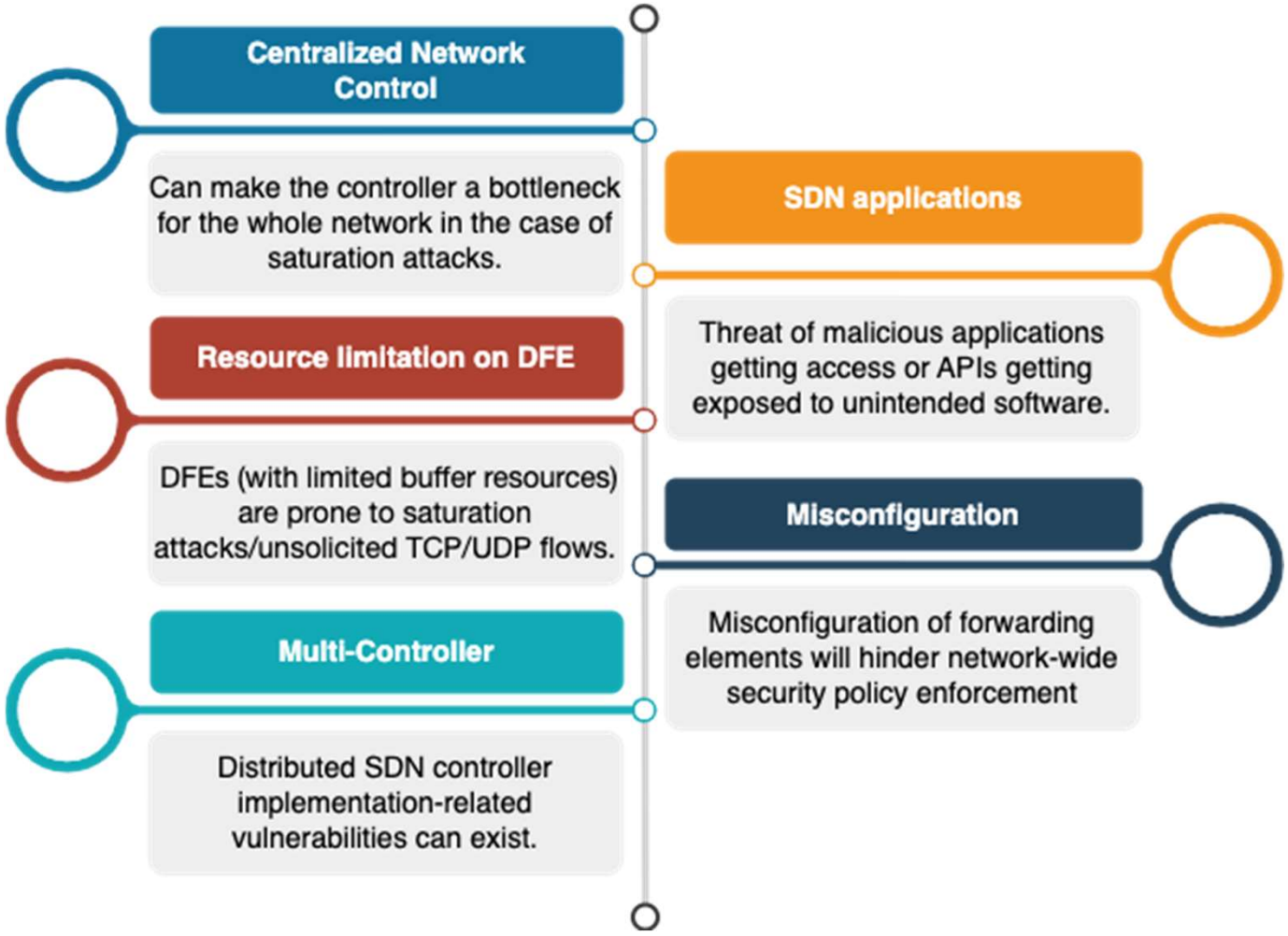
ABMF: Account Balance Management Function
CGF: Charging Gateway Functions
RF: Rating Function
CTF: Charging Trigger Functions

Threats from Legacy Protocols



Security Challenges in SDN

SDN simplifies network management with ‘softwarisation’ by enabling **programmability** and **centralized network control**.

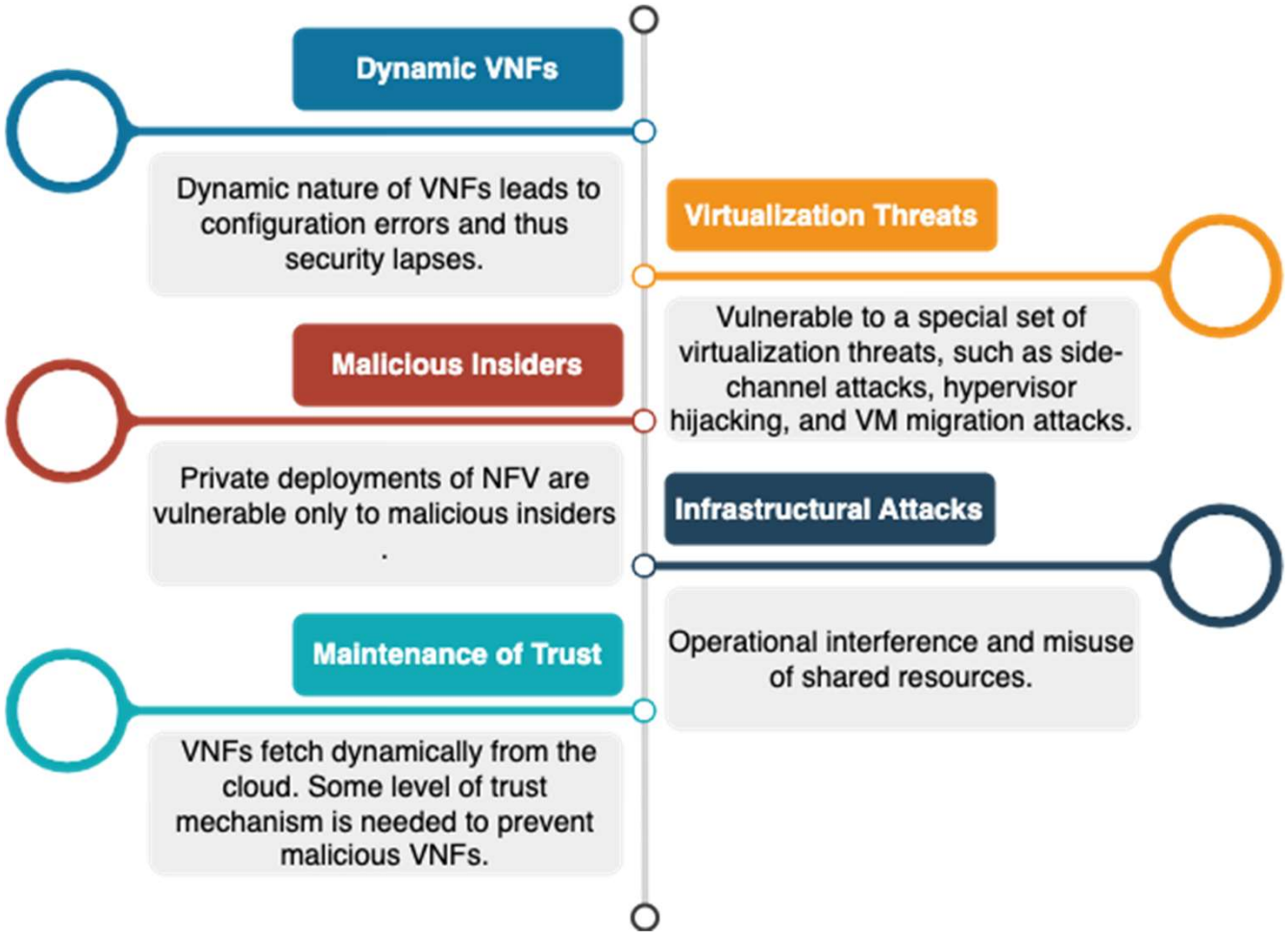


* DFE – Data Forwarding Element

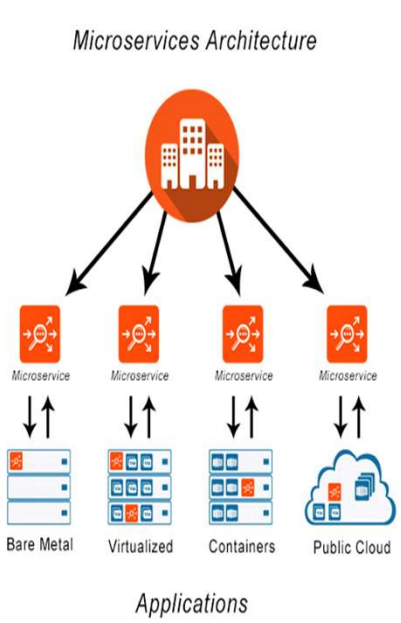
Security Challenges in NFV

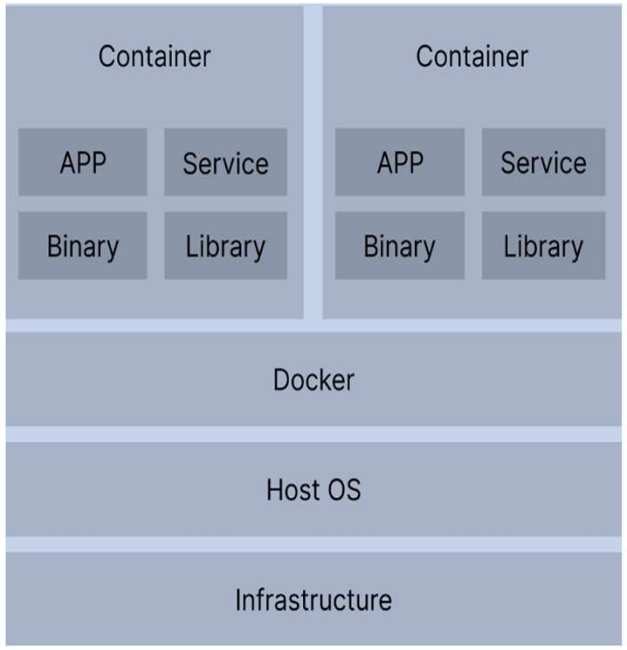
ETSI Network Functions Virtualisation (NFV) Is a technology innovation to support cloud, software and virtualization techniques.

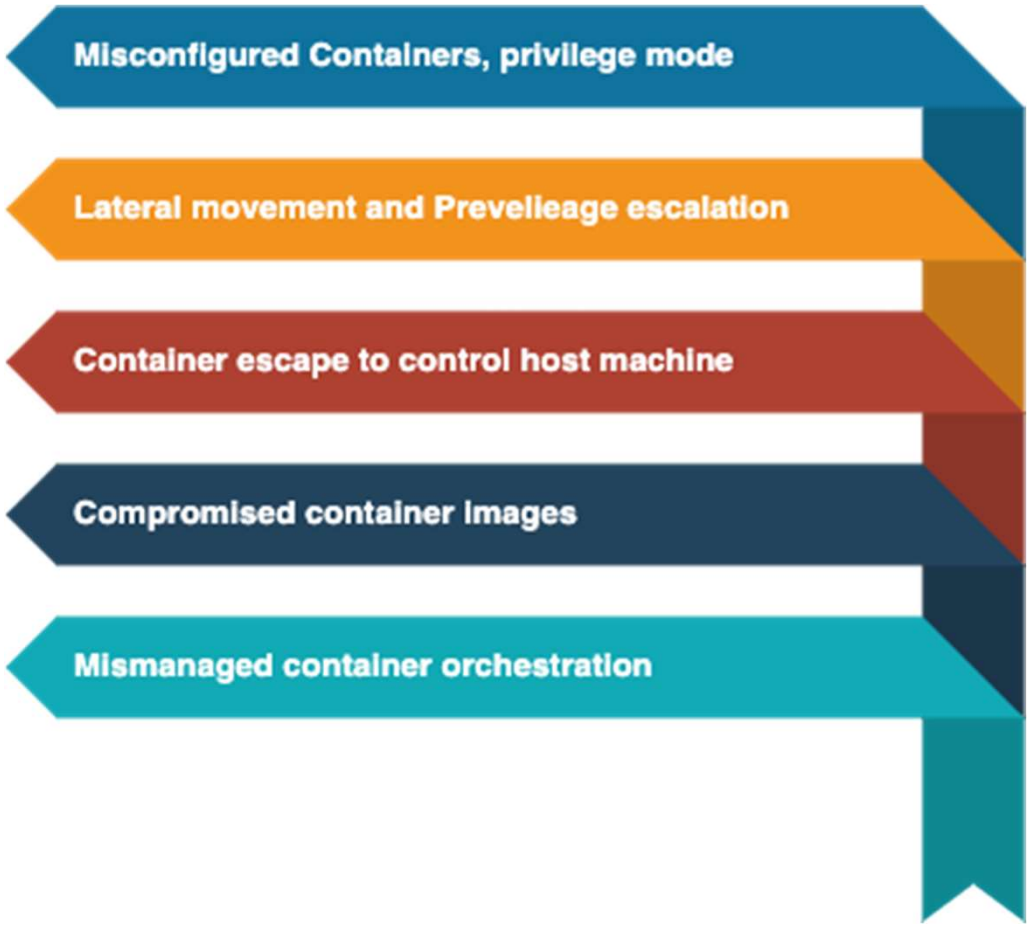
It leverages virtualization characteristics to simplify deployments with increased support for automation.



Container Vulnerabilities and Attacks

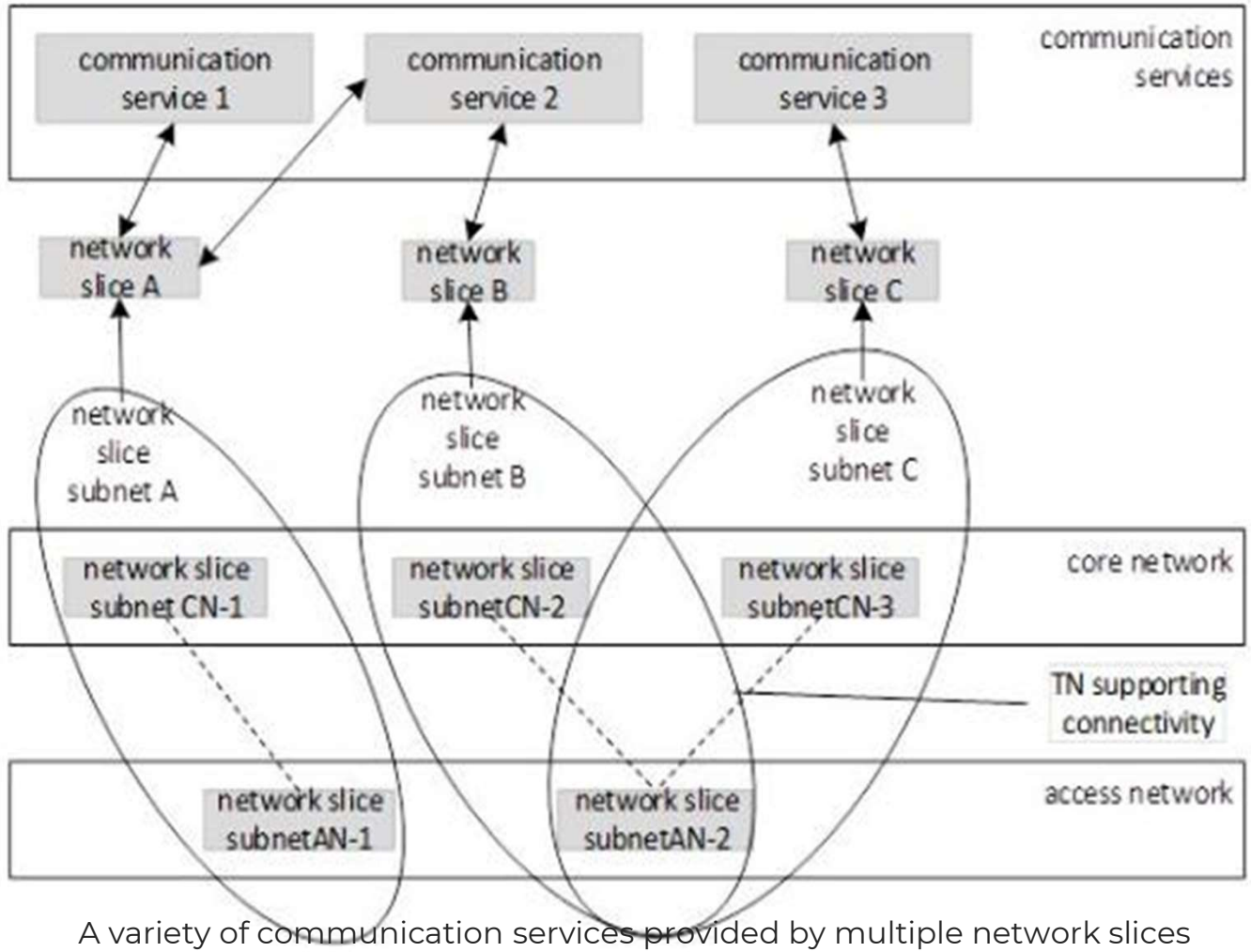






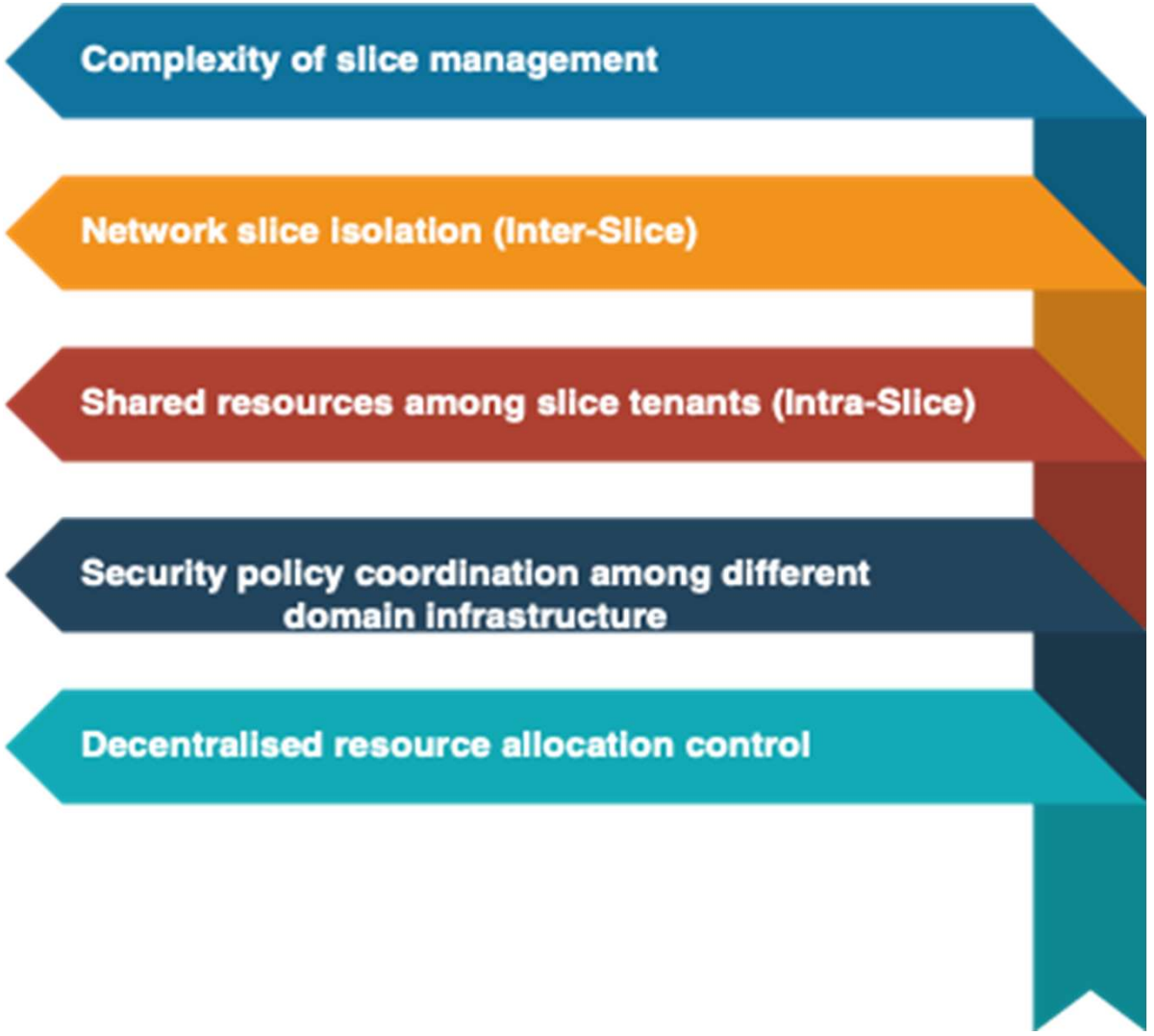
Network Slicing

- Network slicing refers to partitioning of one physical network into multiple virtual networks, each architected and optimized for a specific application/service.
- Slices are logically isolated, but resources can be shared among them.

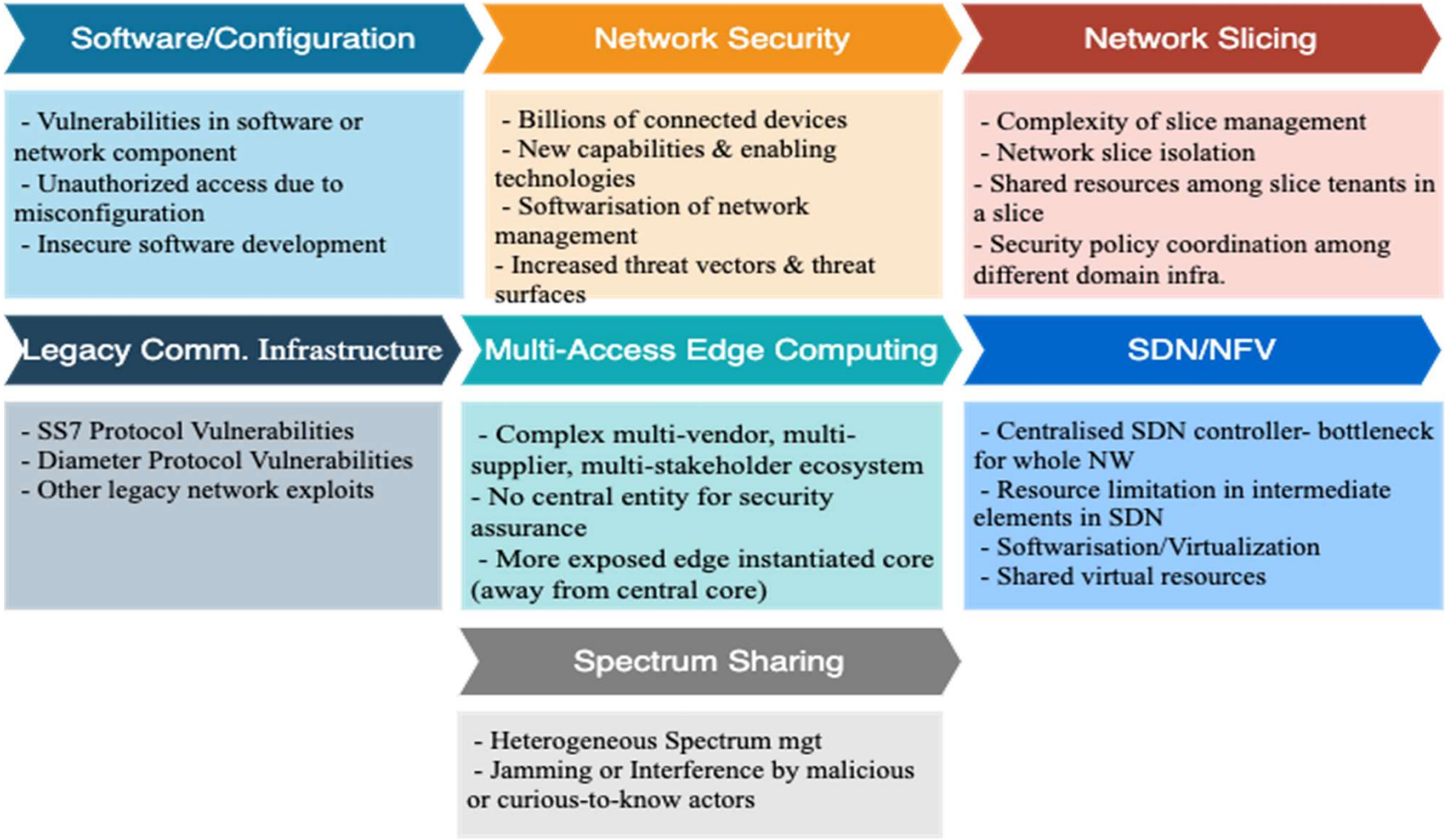


A variety of communication services provided by multiple network slices

Security Challenges in Network Slicing



5G Systems Sub-Threat Vectors-Continued



Mitigation Techniques

CIA Framework

CIA triad

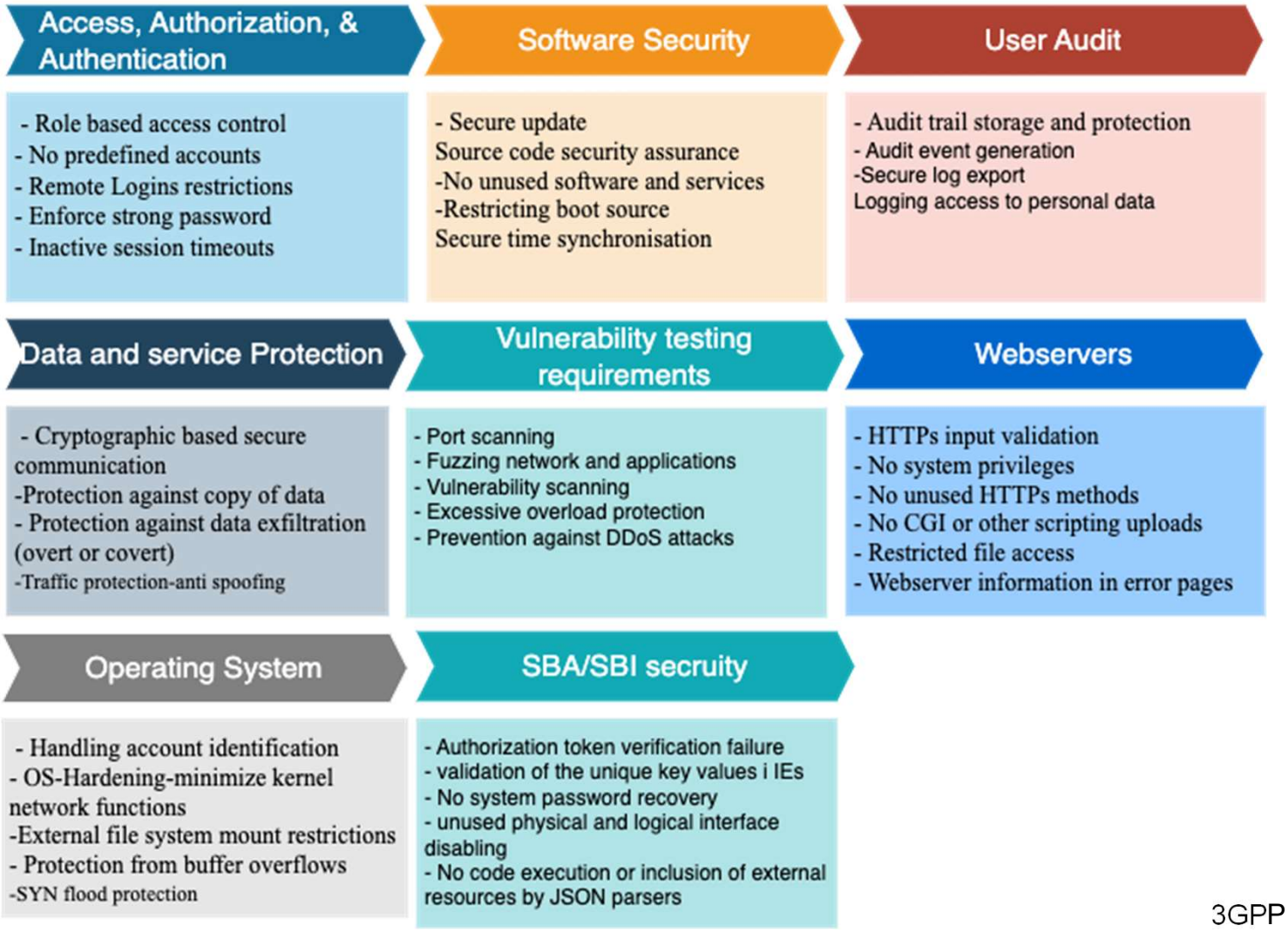
Extended CIA

Common Security Requirement of Network Core

Applies to all network functions of 5GC

3GPP SCAS, ITSAR documents

Common Security Requirement of Network Core



3GPP SCAS, ITSAR documents

Cloud security requirements

- Detect malicious cyber actor activity in 5G clouds and prevent actors from leveraging the compromise of a single cloud resource to compromise the network.

- A TEE is an area in memory protected by the processor in a computing device.

- Ensure that network and customer data is secured during all phases of the data lifecycle (at-rest, in transit, while being processed).

- Ensure that 5G cloud resources (e.g., container images, templates, configuration) are not modified without authorization.

Cybersecurity: Attack Life Cycle

1. Advanced Persistent Threat group (low-and-slow)
2. Ransomware attacks (smash and grab)

The attackers users certain Tactics, Techniques and Procedures (TTP) are launch attacks

MITRE ATT&CK framework

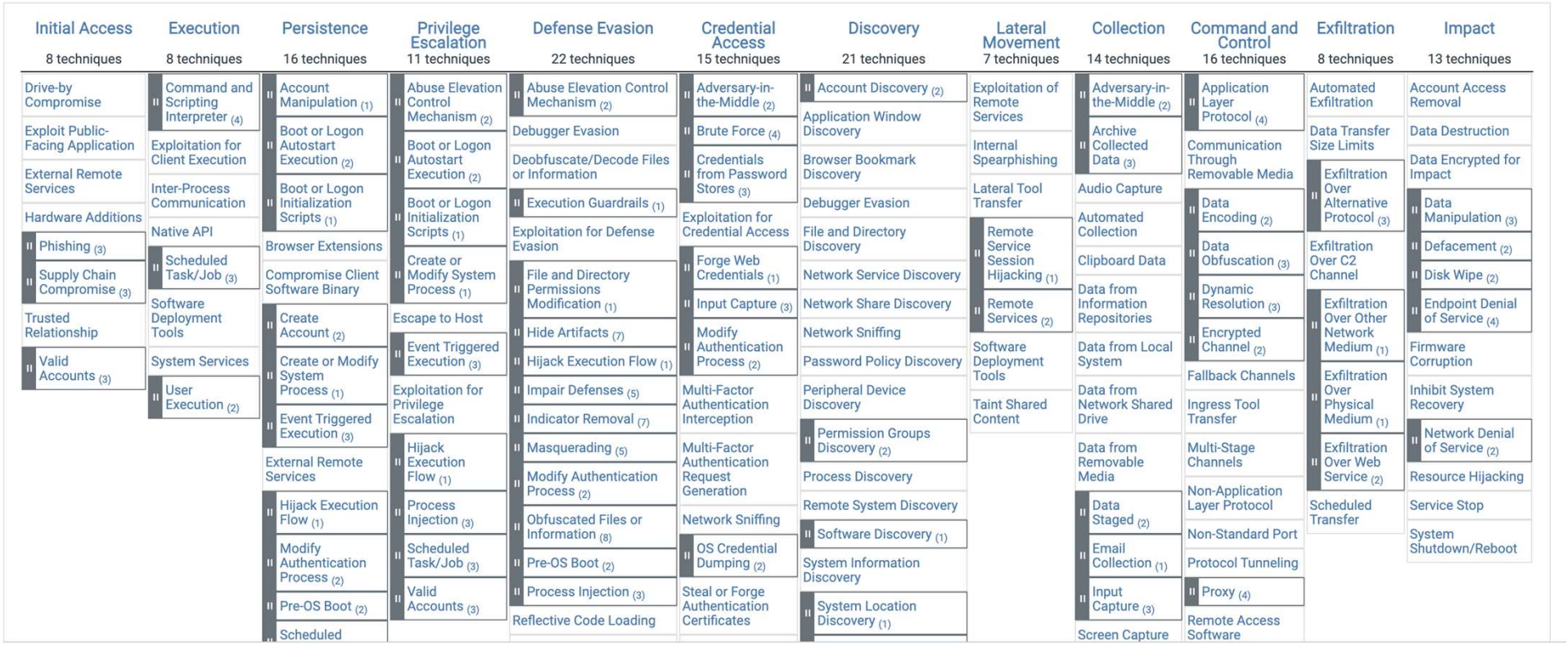
Linux Matrix

Below are the tactics and techniques representing the MITRE ATT&CK® Matrix for Enterprise. The Matrix contains information for the Linux platform.

View on the ATT&CK® Navigator

Version Permalink

layout: flat | show sub-techniques | hide sub-techniques | help



Mitigation Process

- Identity and Access Management
- Endpoint monitoring
  - Log collection and storing
  - Continuous log monitoring
  - Threat hunting
- Manage and respond
- Vulnerability Assessment
- Up to date knowledge of vulnerabilities
- Use of open source intelligence
- Incidence response
- Audit and compliance
- Enforce security best-practices
- Behavioral analytics (AI/ML techniques)

Invite all to visit our booth: Vajra

Thank you!