RECOMMENDATIONS TO MITIGATE PRIVATE 5G INFRASTRUCTURE SECURITY THREATS

By CSA SINGAPORE Cyber Security Agency of Singapore, in consultation with GSMA Singtel

December 2025

Contents

NOTICE

The purpose of this document is to suggest best practices and measures to help enterprises intending to deploy private 5G networks to mitigate cybersecurity risks to these networks. The contents herein are non-binding and meant to be informative in nature and are not intended to exhaustively identify potential 5G threats nor exhaustively specify processes or systems that enterprises should put in place to address or prevent such threats. Enterprises are encouraged to consider how the recommendations may be applied to their specific circumstances and to seek professional advice where required. Enterprises should exercise professional judgement when implementing the recommendations and should also consider if additional measures are necessary to ensure cybersecurity for their systems.

This document does not replace or supersede any applicable legal, regulatory, or operational obligations governing private 5G networks in any jurisdictions. The use of this document and implementation of the recommendations herein does not exempt or automatically discharge the operators from any such obligations or duties. The contents of this document are not intended to be an authoritative statement of the law or a substitute for legal or other professional advice.

This document should not be regarded as suggesting any plan in relation to the issuance of new licences for radio spectrum for private 5G networks in Singapore. For avoidance of doubt, compliance with the recommendations in this document does not constitute an entitlement to operate private 5G networks in Singapore.

The Cyber Security Agency of Singapore (CSA) shall not be responsible for any inaccuracies, errors and/or omissions contained herein, nor for any damage or loss of any kind (including any loss of profits, business, goodwill, or reputation, and/or any special, incidental, or consequential damages) in connection with any use or reliance on this document.

Foreword I

Since the introduction of 5G mobile services about four years ago, it has empowered enterprises and consumers with high-speed and ultra-low latency connectivity. Private 5G networks are increasingly being adopted globally, enabling customised services built on top of their 5G service, such as routing to resources hosted on the cloud and dedicated radio resources to ensure service performance. While offering superior performance, reliability, and control, private 5G networks also introduce a new dimension of cybersecurity risks – driven by architectural complexity and multi-vendor integration.

This document is a step towards building up the understanding of such risks and how to mitigate them. Using a threat-centric approach, it offers pragmatic and actionable cybersecurity recommendations for organisations deploying private 5G networks. The guidance herein is informed by real-world observations, industry collaboration, and alignment with global best practices.

As 5G technology matures, so must our cybersecurity practices. CSA encourages mobile network operators, critical information infrastructure owners, solution providers, and enterprises that plan to use private 5G to adopt the principles laid out in this document. By embedding security into the foundation of digital systems, we can harness the full potential of 5G while safeguarding our systems and data.

Mr. Chua Kuan Seah
Deputy Commissioner of Cybersecurity and
Deputy Chief Executive (Development)
Cyber Security Agency of Singapore

Foreword II

The deployment of 5G networks presents a pivotal opportunity for innovation, economic growth, and improved societal outcomes. At the same time, it demands greater vigilance and a collaborative approach to cybersecurity. As trusted mobile connectivity becomes integral to smart cities, healthcare, transportation, and industrial automation, robust cybersecurity must be treated as a strategic imperative.

The GSMA welcomes this publication as a timely and helpful reference that contributes to the global effort of ensuring secure and resilient private 5G systems. We commend Cyber Security Agency of Singapore for its efforts in developing this guide, which aligns with best practices in the industry and promotes a shared understanding of evolving cyber risks for telecommunication systems.

We hope this document will serve as a valuable resource for both national and international stakeholders, to build a secure digital ecosystem where innovation can thrive without compromise.

David Turkington

Mr. David Turkington
Head of Technology, Asia Pacific
GSMA

1. Introduction

1.1 Background

Private 5G networks provide organisations dedicated wireless connectivity for localised and high-performance operations. They offer reliable, low-latency communication for industries that require tailored quality services. Private 5G offers higher throughput, lower latency, and tighter control over traditional Wireless Fidelity (Wi-Fi) or Long-Term Evolution (LTE). These capabilities facilitate applications like automated manufacturing, real-time video analytics, and mission-critical IoT deployments. For example, in smart manufacturing, private 5G provides uninterrupted high-speed connectivity to enhance high-precision quality control in manufacturing operations; in healthcare, indoor private enterprise 5G supports the use of mixed reality technology to enhance and augment healthcare delivery.

Private 5G expands the cybersecurity threat surface because the customisation options often involve integrating diverse devices and technologies. The increased reliance on edge computing and the integration of third-party applications further introduces potential vulnerabilities. Private 5G networks are attractive targets for data theft and sabotage when they process sensitive information such as sensitive operational data or critical infrastructure details. The convergence of telecommunications and information technology (IT) in private 5G networks also necessitates a holistic security approach that addresses the combined challenges across both domains.

1.2 Purpose

Recommendations to Mitigate Private 5G Infrastructure Security Threats provides guidance to mitigate cybersecurity threats in private 5G deployments and support secure, reliable network operations. It highlights key threats to 5G deployments and outlines corresponding measures that organisations can implement. Aimed at an international audience and developed in consultation with GSMA and Singtel, the recommendations extend beyond Singapore's specific 5G deployments and use cases. The document complements *the Guidelines for CII Owners to Enhance Cyber Security for 5G Use Cases*[1]*,* published by CSA in 2022 for users of 5G services, including CIIOs. Together, these two publications seek to address a wider range of 5G use cases across different industries.

1.3 Scope

This document provides cybersecurity recommendations for private 5G deployments. It focuses on the Radio Access Network (RAN), Multi-access Edge Computing (MEC), the transport network and

[1] CSA, Guidelines for CII Owners to Enhance Cyber Security for 5G Use Cases, Apr 2022

the 5G Core. These components may be owned or operated by Mobile Network Operators (MNOs) or enterprises, depending on the deployment model. The scope does not provide risk assessments for 5G implementations, network functions or applications. It also does not cover threats or recommendations for end users of 5G services.

1.4 Intended Audience

The intended audience of this document includes, but is not limited to, global enterprises' management and network teams who intend to deploy and operate private 5G networks, their cybersecurity teams and solution providers.

2. 5G Architecture

The 5G infrastructure and architecture mark a transformative shift from earlier mobile network paradigms, driven by virtualisation and a Service-Based Architecture (SBA). Virtualisation allows core components like the Access and Mobility Management Function (AMF), Session Management Function (SMF), and User Plane Function (UPF) to be deployed as software on flexible platforms, enhancing scalability and agility (See Figure 1). This approach enables dynamic resource allocation and rapid service deployment, crucial for private 5G networks requiring tailored solutions. Furthermore, the virtualisation of the Radio Access Network (RAN) and Multi-access Edge Computing (MEC) facilitates network slicing, allowing for customised network instances to meet specific application demands.

Central to 5G's architecture is the SBA, which utilises standardised APIs for communication between core network functions. The SBA decouples network functions into modular services, enabling network functions to interact seamlessly, allowing for scalability, flexibility, and efficient service delivery. This architecture empowers private 5G operators to finely control network resources and service delivery, optimising performance and security for diverse applications within deployments.

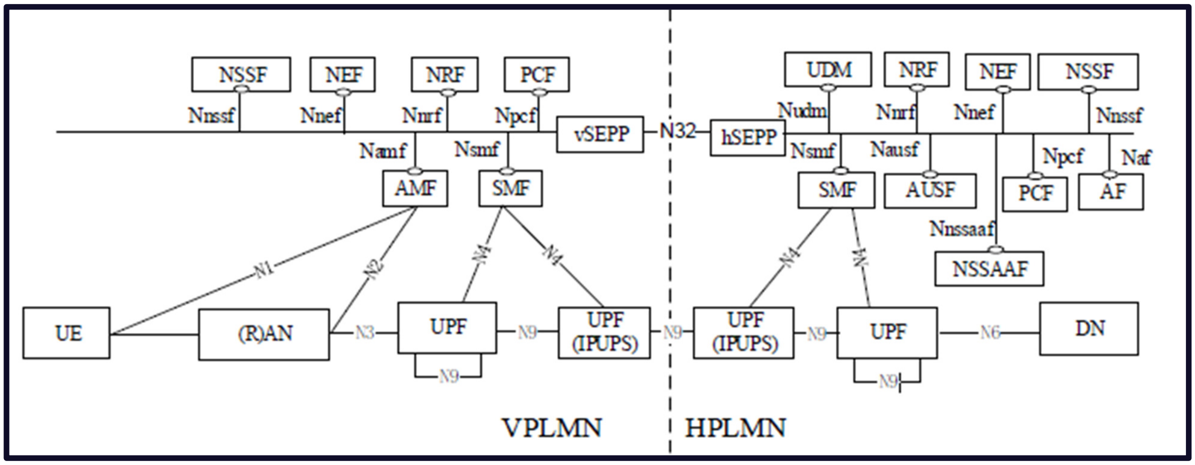


Figure 1: Roaming 5G System Architecture. Source: GSMA FS.40 – 5G Security Guide

The 5G architecture, as defined by the Third Generation Partnership Project's (3GPP) standards and depicted in GSMA *FS.40 – 5G Security Guide document*, incorporates significant security enhancements compared to previous mobile network generations. The SBA allows for finer-grained security policies and the isolation of critical network functions. Furthermore, encryption of both control plane and user plane enhances confidentiality, collectively contributing to a more resilient and secure mobile network infrastructure.

3. Private 5G Deployment Types

3GPP has defined Private 5G as mobile networks which are intended for non-public use, i.e., they provide 5G connectivity to a select group of devices based on the needs of its users due to their use case, to have better control of the quality of service or how the data could flow within the network.

This concept is not new to previous generations of mobile communication technologies. However, the introduction of virtualising the systems and network components of the 5G infrastructure has widened the possible combinations of 5G solutions, and how enterprises and public mobile network operators can deploy private 5G. Enterprises can also work with external partners, in addition to public mobile network operators, to deliver the full suite of solutions required for their private mobile network service, based on the local regulations, level of control needed and costs.

In GSMA's *Exploring 5G Private Network Opportunities in Asia Pacific* document, published in February 2023, the possible private 5G network deployments are grouped into the three broad categories below. Private 5G deployments include those where an existing mobile network operator's licensed spectrum is used and are not limited to those where the radio frequency spectrum is licensed to an enterprise. Implementation of private 5G networks varies across countries due to differing regulatory frameworks. In Singapore, private 5G networks are currently deployed through hybrid model based on operator's public 5G network. The private 5G networks mentioned henceforth in this document will refer to 5G networks that fall into any of the three categories (Note that the "standalone" here does not refer to the different options of 5G architecture – 5G Standalone and 5G Non-Standalone).

Standalone enterprise-led	Standalone operator-led	Hybrid (based on operator's public 5G network)
•Can be built by enterprises or mobile operators •Uses allocated new 5G spectrum •Meets stringent reliability, security, availability and latency requirements •Costly and requires dedicated operational personnel	•Built by mobile operators on behalf of enterprises •Uses the operator's licensed 5G spectrum •Meets stringent reliability, security, availability and latency requirements •Benefits from the operator's long-standing experience in network management	•Based on a 'slice' of an operator's public network •Uses the operator's licensed spectrum •Shares use of the operator's public 5G resources (e.g., RAN, core, cloud) to varying levels •Quicker and easier to set up and manage than standalone variants

Table 1: Private 5G Network Deployment Scenarios, Source: GSMA Intelligence

4. Private 5G Infrastructure Threats and Mitigations

The Private 5G infrastructure threats presented in this document draw upon a combination of observed attacks against prior mobile network generations and adapts them to 5G systems. The document highlights threats that could introduce risks to private 5G deployments by analysing possible vulnerabilities in control plane functions, user plane data flows, edge applications. These risks are associated with industrial automation and critical infrastructure use cases from diverse cybersecurity-focused resources.

While 3GPP's specifications are designed for 5G networks to be inherently more secure than previous generations of mobile networks, not all security features are enabled by default. 5G deployment is complex hence this document aims to bring cybersecurity awareness to enterprises that wish to deploy private 5G networks.

The diagram below depicts seven threats covered in this document. Readers should acknowledge that the threats mentioned in this document are not exhaustive and should not be considered a comprehensive catalogue of attack vectors. Furthermore, the threats are not presented in any order of priority.

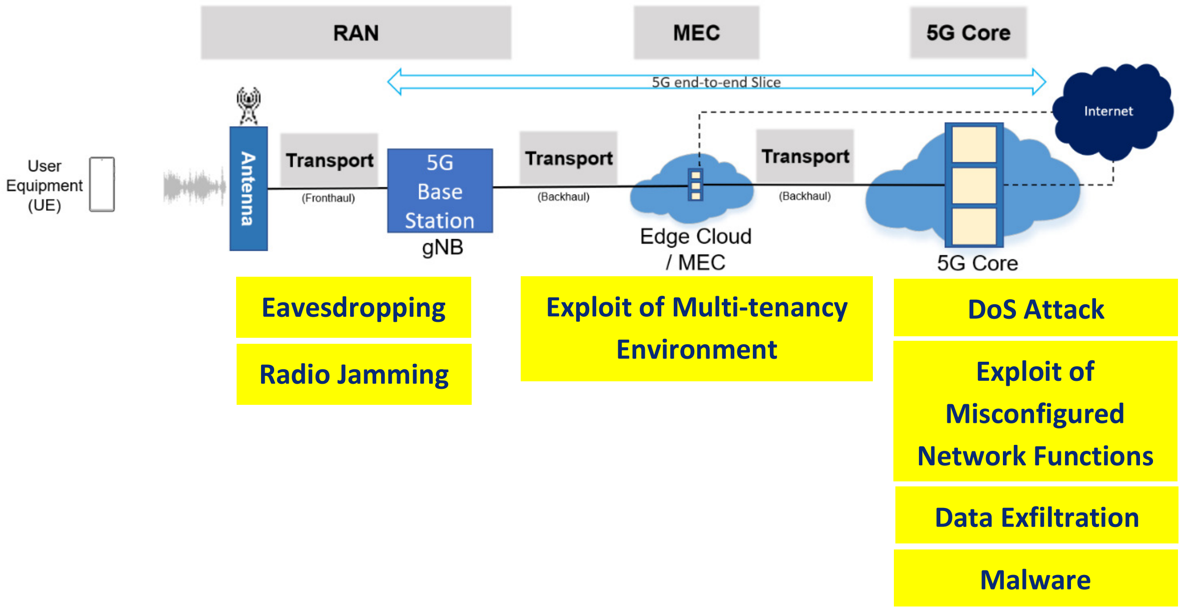


Figure 2: High Level 5G Architecture with Threats

Enterprises deploying private 5G networks must conduct their own risk assessments, considering their specific threat landscape and risk tolerance. Readers are encouraged to evaluate the mitigations covered and prioritise their implementation based on their own judgement, aligned with regulatory requirements, security requirements, and operational needs.

In addition, readers can also refer to GSMA's official document *FS.31 – Baseline Security Controls, version 5.0*, which outlines a comprehensive set of fundamental cybersecurity controls to help operators understand and develop security posture to a foundation level. These baseline controls are also applicable to private 5G networks.

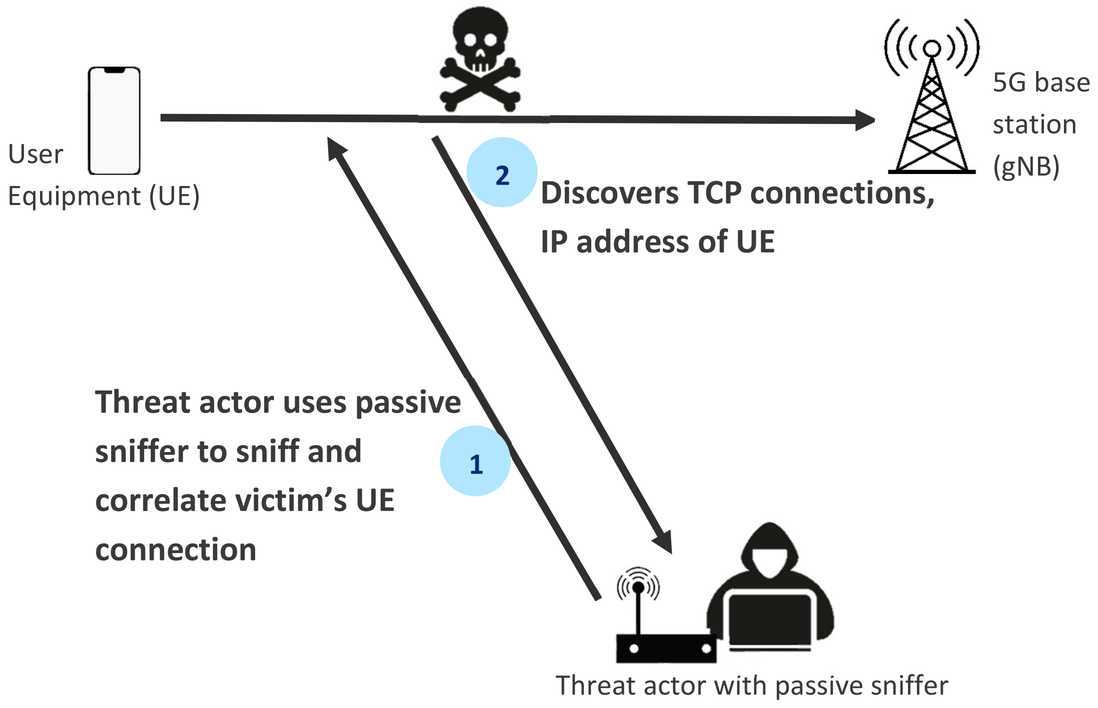
4.1 Eavesdropping

Threat Description
Eavesdropping is an attack which involves sniffing on the network traffic by various means to capture information about an environment, such as authentication materials passed over the network. In the 5G environment, a threat actor with access to an interface without encryption can monitor traffic exchanges and obtain UE information.

Impact
Confidentiality
Sensitive data, such as private messages, application data and unencrypted login credentials can be sniffed by the threat actor. This can allow the threat actor to carry out further cyber-attacks, or to cause other damages, depending on the data captured.

Possible Attack Scenario

Threat actor could passively eavesdrop network traffic between the victim's UE and gNB during periods when encryption has not yet been activated (such as the initial access and registration phase) or where radio interface has been misconfigured or compromised. The information transmitted over the air between the UE and gNB can then be decoded by the threat actor. Threat actor places a passive sniffer, comprising of software defined radios and directional antennas in the vicinity of the target's private 5G coverage and correlate the UEs' connection to identify, track and observe victim's network traffic. With the captured data over the air, the threat actor can discover the TCP connections and associated external IP address of the victim's UE, among other sensitive information.


5G base station (gNB)
User Equipment (UE)
2
Discovers TCP connections, IP address of UE
Threat actor uses passive sniffer to sniff and correlate victim's UE connection
1
Threat actor with passive sniffer

Cybersecurity Recommendations

a) **Subscriber Concealed Identifier (SUCI)**: Verify and enforce that Subscriber Concealed Identifier is used for all initial authentication, disabling any fallback mechanisms that might transmit the IMSI in plain text.

b) **Transport Layer Security (TLS) for user plane**: For user plane traffic, implement TLS between User Equipment and application servers, using strong cipher suites and robust certificate management.

c) **Packet Data Convergence Protocol with AES**: Implement Packet Data Convergence Protocol encryption using 3GPP-approved algorithm (e.g., AES-based NEA) for the control plane and user plane traffic on the radio interfaces between UE and gNB.

d) **Network Slicing**: Limits exposure by segmenting traffic for specific user groups to reduce attack surface if a breach occurs.

e) **Local Breakout of User Plane Function**: Reduce the attack surface and the risk of interception over external transport network by keeping sensitive data traffic within physical and logical boundaries.

4.2 Radio Jamming

Threat Description

Wireless communication networks which rely on the open air as the communication medium are inherently susceptible to interferences, which is one of the fundamental causes of its performance degradation. Similarly, in cellular networks like 5G, radio jamming is a specific variant of Denial of Service (DoS) against mobile networks, i.e. making radio resources unavailable by transmitting noise. While 5G has improved upon LTE’s vulnerable downlink channels such as Physical Format Indicator CHannel (PFICH), it is still vulnerable to smart jamming attacks, which target narrow control channels.

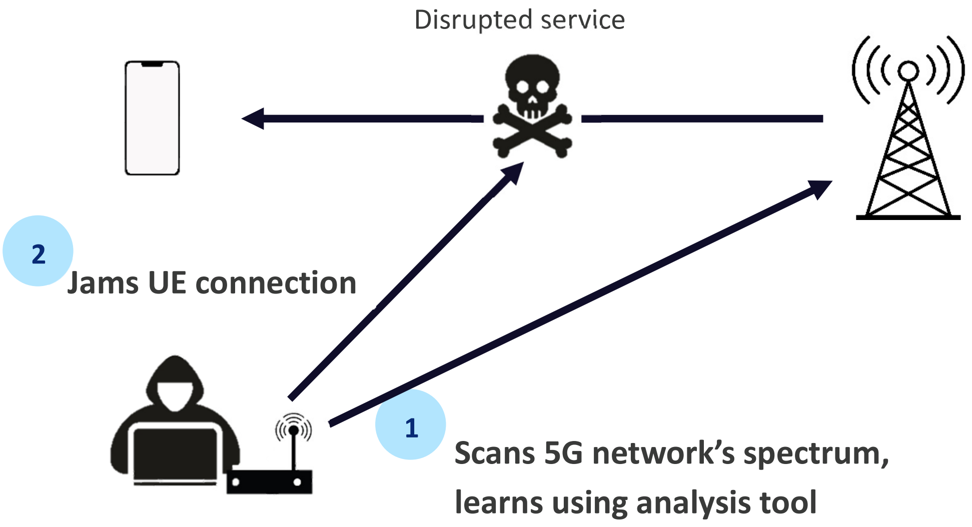
Impact

Availability

Radio jamming blocks legitimate signals, leading to inability to establish or maintain connection with devices and base station. Critical applications and devices may fail to operate with the loss in connection, leading to disruptions, such as system failure.

Possible Attack Scenario

Threat actor, using a software-defined radio (SDR) passively scans the private 5G network's spectrum, identifying specific frequencies and timing patterns of the control channels used for device registration and handover. Utilising protocol analysis tools, threat actor learns the structure of the broadcast channel messages and Radio Resource Control (RRC) signalling and programs the SDR to selectively jam these channels, targeting the synchronisation signals and initial access procedures. This will cause connection failure to the private 5G network.



Cybersecurity Recommendations

a) **Load balancing**: Design the network to balance loads across multiple channels or frequencies, making it more resilient to localised jamming in one area or channel.

b) **Monitoring and detection:** Implement monitoring and detection systems to detect abnormal interference levels, which may indicate targeted jamming of control channels.

c) **Anti-jamming techniques:** Use advanced anti-jamming techniques such as frequency hopping, spread spectrum, and beamforming to minimise the effectiveness of jamming attacks and attempts.

d) **Multiple-input and Multiple-output (MIMO) for multiple simultaneous data streams**: Implement MIMO with multiple simultaneous data streams along various paths, reducing the effect of single-path interference.

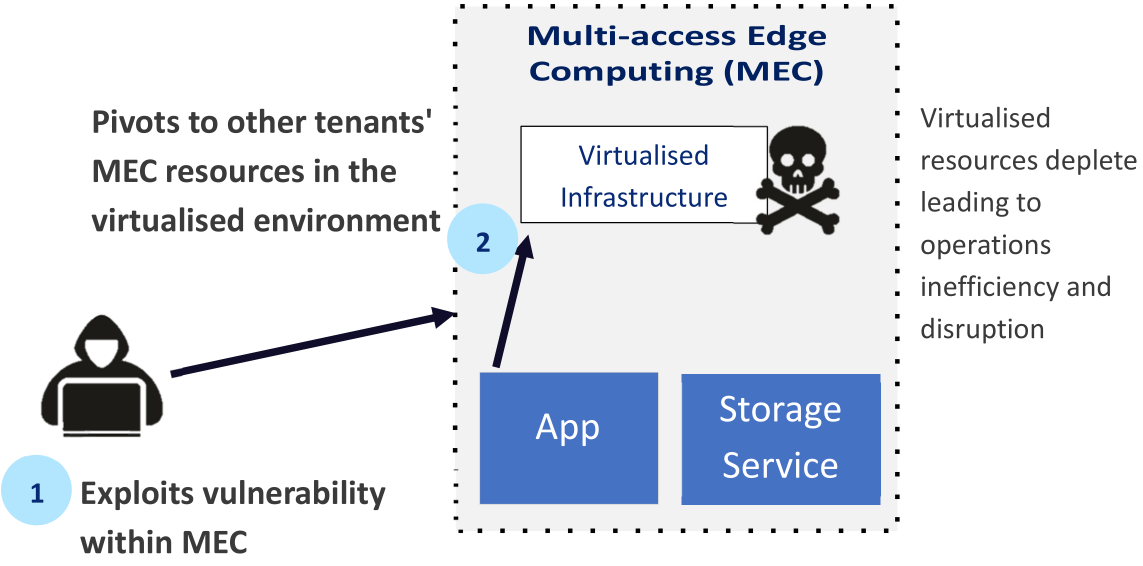
4.3 Exploit of Multi-tenancy Environment

Threat Description
In a multi-tenancy environment like the 5G MEC, multiple tenants (users or applications) would share computing resources. Proper isolation ensures that each tenant's data and resources are segregated securely. If tenant isolation is not properly implemented, one tenant might gain unauthorised access to functions or resources.

Impact
Confidentiality
Sensitive data from one tenant could be exposed to other tenants, including confidential business information, personal user data, or intellectual property.
Integrity
Malicious tenants could modify or corrupt data belonging to other tenants, leading to inaccurate information and operational errors. Tenants could manipulate applications or services belonging to other tenants, causing disruptions or unauthorised modifications. A compromised tenant could use their access to alter the configurations of shared network functions, affecting all tenants in the environment.
Availability
A malicious tenant could consume excessive resources, such as Central Processing Unit (CPU), memory, or bandwidth, leading to performance degradation or service outages for other tenants. Tenants could launch DoS attacks against other tenants or shared MEC resources, rendering them unavailable. Improper isolation can lead to unintended interactions between tenant workloads, causing service disruptions or failures.

Possible Attack Scenario

A threat actor exploits a zero-day vulnerability within the MEC platform's hypervisor solution which allows the threat actor to escape their allocated virtual environment. They pivot to gain unauthorised access to a neighbouring tenant's MEC resources. The threat actor deploys a resource-intensive payload which affected the neighbouring tenant's application running on the MEC, causing their system to operate inefficiently.


Multi-access Edge Computing (MEC)
Pivots to other tenants' MEC resources in the virtualised environment
2
Virtualised Infrastructure
Virtualised resources deplete leading to operations inefficiency and disruption
App
Storage Service
1
Exploits vulnerability within MEC

Cybersecurity Recommendation

a) **Robust hypervisor-based isolation**: Implement robust hypervisor-based isolation solutions to separate virtual machines (VMs) hosting different workloads, preventing resource contention and unauthorised access. Within VMs, use containerisation technology to further isolate individual applications, enhancing security and portability where possible.

b) **Strong authentication and authorisation**: Use strong authentication and authorisation mechanisms, including multi-factor authentication, to control administrative access to the hypervisor and virtual machines through virtual interfaces. Isolate network traffic using Virtual LANs (VLANs) and network zones to separate management, control, and data plane traffic.

c) **Strict access control policies:** Implement strict access control policies, including role-based access control (RBAC), to limit access to workloads and their resources based on the principle of least privilege.

d) **Secure inter-VM and inter-container communication**: Secure inter-VM and inter-container communication using encrypted channels and firewalls to restrict traffic flow to only authorised paths.

e) **Monitor resource usage and security events:** Monitor resource usage and security events to detect any anomalies that could indicate a potential security breach or resource contention.

f) **Secure communication channels**: Secure communication channels using TLS for management interfaces and Internet Protocol Security (IPSec) for communications within MEC.

g) **Trusted Execution Environments:** Utilise hardware-based security features where available to create isolated execution environments for workloads, protecting data from other tenants.

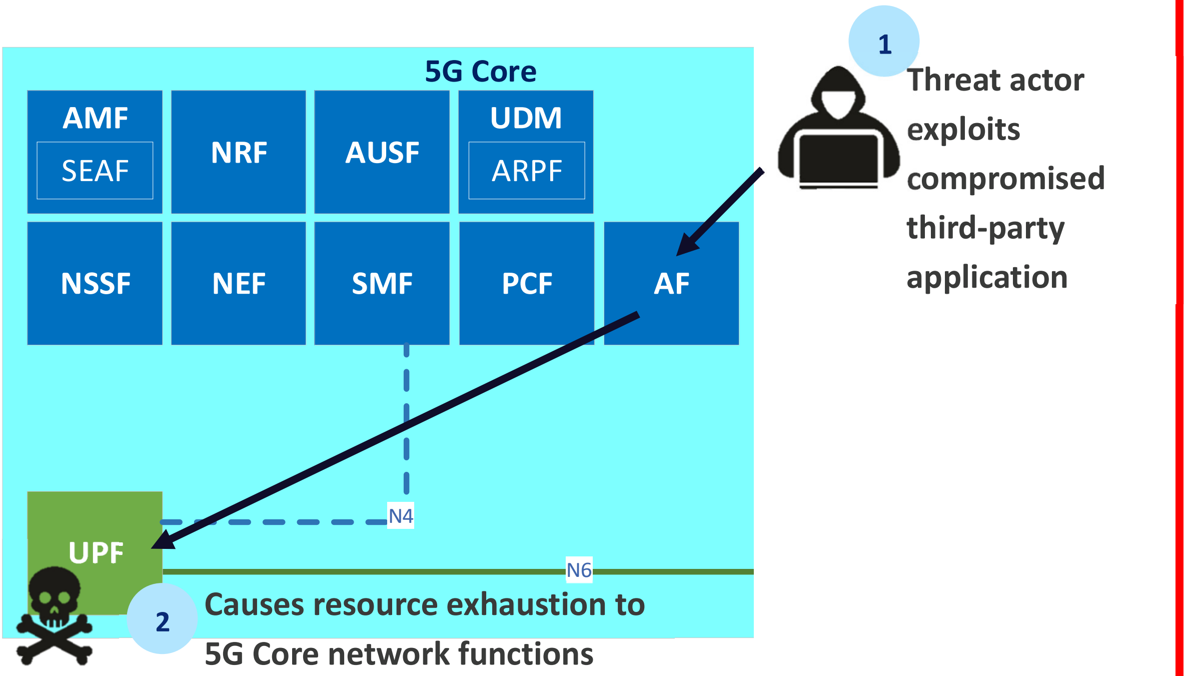
4.4 Denial of Service Attack

Threat Description
Denial of Service (DoS) attacks aim to disrupt authorised access to network resources or introduce delays to time-sensitive operations, typically by overwhelming the target systems. In 5G networks, the introduction of the Application Function (AF) enables third party applications integration, expands the threat surface and creates new potential vectors for DoS attacks.

Impact
Availability
Threat actors can flood the 5G Core with excessive requests, exhausting processing power, memory, or bandwidth, leading to service degradation or total failure. A DoS attack on MEC infrastructure can lead to localised outages, crippling low-latency applications.

Possible Attack Scenario

A threat actor exploits a known vulnerability in a third-party application integrated with a private 5G network's AF, launches a DoS attack. The attack floods the AF with a deluge of crafted requests, overwhelming its processing capacity and causing a cascading effect that disrupts critical network function. This flood of traffic then overwhelms the UPF, responsible for data forwarding, leading to significant latency and packet loss for the entire network.


5G Core
AMF
SEAF
NRF
AUSF
UDM
ARPF
NSSF
NEF
SMF
PCF
AF
N4
N6
UPF
1
Threat actor exploits compromised third-party application
2
Causes resource exhaustion to 5G Core network functions

Cybersecurity Recommendations

a) **Robust patch processes:** Verify the checksums of software to confirm the authenticity of the software and disable all unused services that might be running in the host systems, allowing only required services. Periodically check the configuration of the software is as intended. Patch the software once there are available patches from the authorized vendor to ensure software is resilient to known vulnerabilities.

b) **Rate Limiting:** Enforce reasonable rate limiting in all network elements to ensure incoming and forwarded traffic are at expected volumes. Segment network into security zones and use firewall to restrict and filter traffic between zones. Implement continuous monitoring of resources utilisation with clear thresholds and alerts for abnormal spikes.

c) **Incident response plan:** Develop an incident response plan which can include traffic diversion and failover systems, to ensure operational continuity even during an event of a DoS attack.

d) **Network Slicing**: Physical and logical isolation of high priority slices would allow different Quality of Service controls, to reduce the impact when adjacent slices are under DOS attacks.

4.5 Data Exfiltration

Threat Description

Data exfiltration attacks involve the unauthorised transfer of sensitive information from devices or systems, representing a critical security threat to both individuals and organisations. In a 5G network, this can manifest as the theft of subscriber data, proprietary business information, or other confidential content. Data exfiltration occurs after a threat actor has successfully infiltrated the targeted network, establishing a foothold to facilitate the covert transfer of stolen data.

Impact

Confidentiality

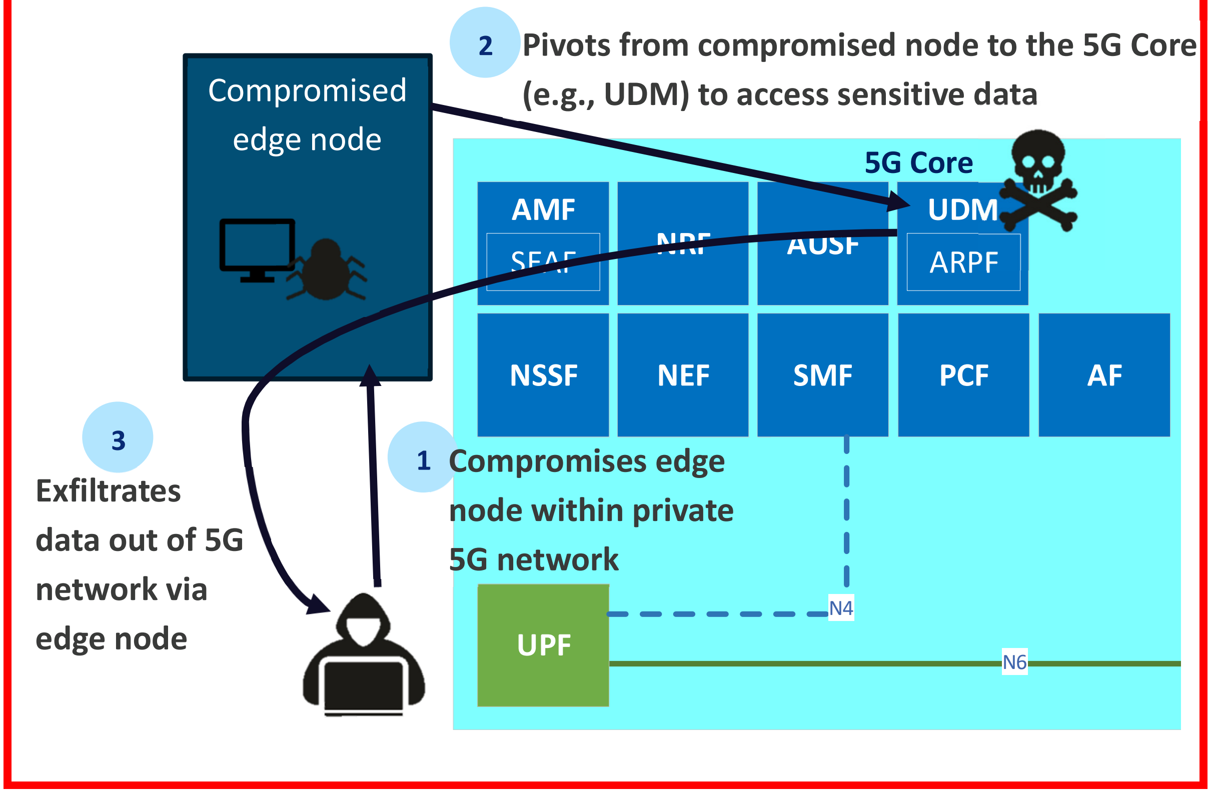
Threat actors can steal and expose sensitive subscriber data stored in private 5G networks, including user credentials, International Mobile Subscriber Identity (IMSI), location data, and call records.

Enterprises relying on private 5G (e.g., smart factories, R&D labs, healthcare institutions) store and transmit highly sensitive intellectual property (IP), including trade secrets, proprietary designs, and financial reports. Data exfiltration could result in economic espionage and loss of competitive advantage.

IoT sensors and edge devices in private 5G networks collect and transmit confidential data, such as patient records (healthcare), autonomous vehicle telemetry (automotive), and industrial process logs (manufacturing). If threat actors exfiltrate this data, it can lead to privacy violations, regulatory fines, and operational security risks. Stolen data can fuel more sophisticated cyberattacks, such as ransomware, business email compromise, and spear-phishing attacks.

Possible Attack Scenario

After establishing a persistent foothold within a private 5G network, a threat actor initiates a covert data exfiltration operation by using compromised edge nodes as staging points. Sensitive data is encrypted and compressed, disguised as routine network traffic to be gradually transferred to an external command-and-control server.


2
Pivots from compromised node to the 5G Core (e.g., UDM) to access sensitive data
Compromised edge node
5G Core
AMF
SEAF
NRF
AUSF
UDM
ARPF
NSSF
NEF
SMF
PCF
AF
1
Compromises edge node within private 5G network
3
Exfiltrates data out of 5G network via edge node
UPF
N4
N6

Cybersecurity Recommendations

a) **Role-based controls and least privilege principle:** Implement role-based controls and least privilege principle, especially for privilege accounts, to prevent unauthorised access to sensitive data. Account protection policies should include the use of multi-factor authentication (MFA) and passwords that are refreshed periodically to ensure the robustness of the access to user accounts.

b) **Strong data protection measures:** Ensure all critical data are stored in encrypted form and apply robust access control mechanism. Data encryption should also be applied for data in transit. Data masking should be used where possible to obscure sensitive information that are not necessary during transmission.

c) **Secure erasure or disposal of residual data:** Implement policies and mechanisms to erase or dispose of all residual data that are no longer required. Proper handling of decommissioned devices which may contain data should be executed and monitored by tight processes to prevent any possible data leak.

d) **Network Slicing**: Physical and logical separation of data allows different levels of security controls to be implemented, based on the sensitivity and criticality of the data.

e) **Local Breakout of User Plane Function**: Combination of physical and logical security controls would restrict attack surface and reduce exfiltration paths.

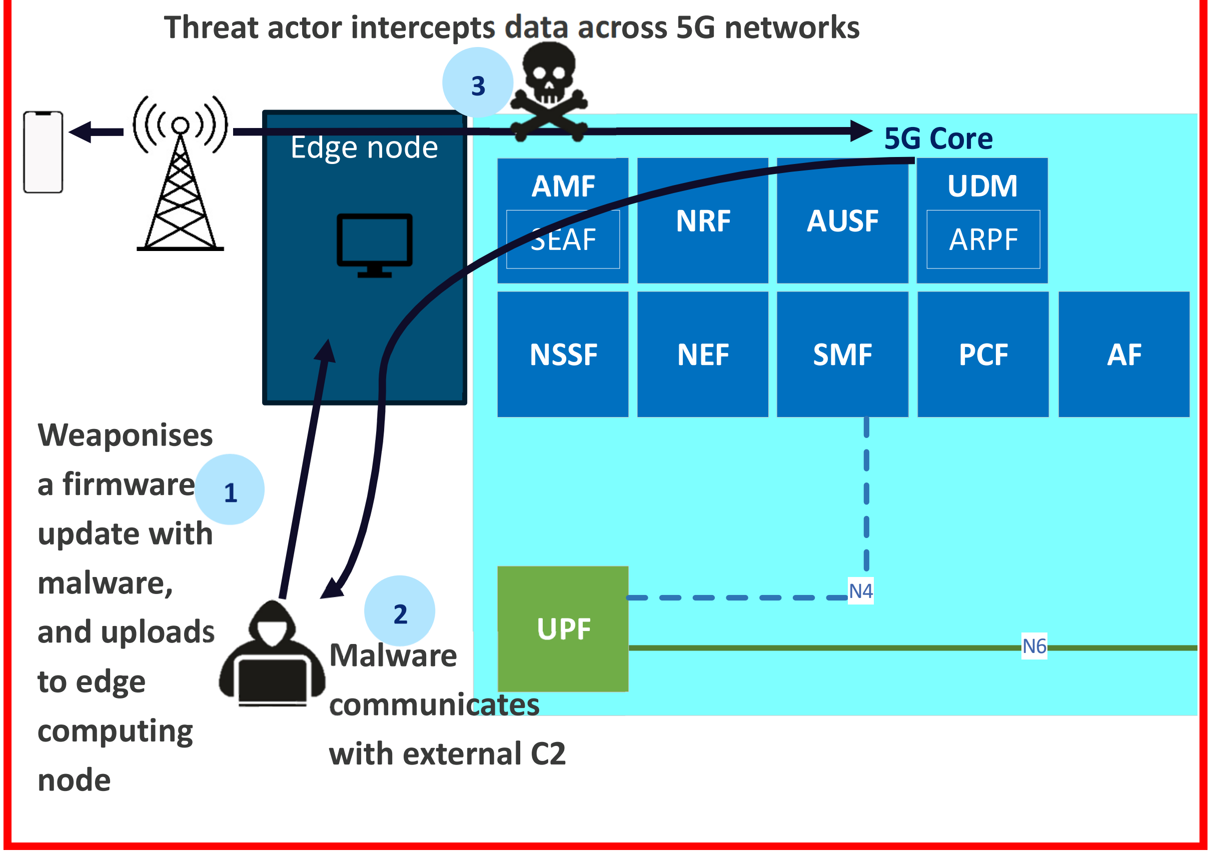
4.6 Malware

Threat Description
Malware can be a firmware or software that is intentionally included or inserted in a system for harmful purposes. Malware attacks are very broad in scope and levels of sophistication. Malware ranges from relatively simple remote access trojans (RATs) to extremely sophisticated polymorphic viruses and rootkits. In the 5G MEC, with virtualised infrastructure and third-party applications, malware can potentially compromise any layer of the software stack from the firmware to operating systems, virtualisation infrastructure, virtual machines and applications.

Impact
Confidentiality
Malware can steal sensitive data transmitted over the 5G network, including user credentials, location information, and application data.
Integrity
Malware can tamper with control plane signalling, altering network configurations and disrupting service delivery. It can modify user data transmitted over the network, leading to data corruption or manipulation. Malware can compromise network functions, allowing threat actors to inject malicious code or modify existing functions.
Availability
Malware can carry out DDoS attacks against network functions, overwhelming them with traffic and rendering them unavailable. Malware can corrupt or delete critical network configurations, leading to service outages. Malware that impacts the control plane, can stop new connections from being formed, or existing connections from being maintained.

Possible Attack Scenario

A seemingly innocuous firmware update is delivered to an edge computing node, containing a hidden malware payload. The payload exploits a zero-day vulnerability in the edge node's operating system, escalating privileges to gain root-level access and establish persistence. Once persistent foothold is achieved, the malware communicates with an external Command and Control (C2) server and can intercept data traversing across 5G network. Through the C2 server, the threat actor can read and modify the sensitive data intercepted by the malware.


Threat actor intercepts data across 5G networks
3
Edge node
5G Core
AMF
SEAF
NRF
AUSF
UDM
ARPF
NSSF
NEF
SMF
PCF
AF
N4
UPF
N6
Weaponises a firmware update with malware, and uploads to edge computing node
1
2
Malware communicates with external C2

Cybersecurity Recommendations

a) **Zoning and segmentation based on application requirements**: 5G networks should be logically zoned based on application requirements and protocols, to effectively implement a defence-in-depth strategy. Segment the network into distinct zones, such as a user access zone, an IoT zone, a critical infrastructure zone, and a management zone, each with strict access controls and firewalls to limit lateral movement. Sensitive applications and data should be designed to be within their own zone. Implement micro-segmentation within zones to further isolate individual workloads and virtual network functions, limiting the impact of any compromised component. Enforce strict traffic filtering rules between zones, allowing only necessary communication based on predefined protocols and ports. Continuously monitor traffic flow and security events within and between zones through a Security Information and Event Management (SIEM), to detect and respond to any malicious activity promptly.

b) **Robust patch management process and verification of digital signatures:** Download patches only from trusted vendor sources and verify digital signatures to ensure the patch has not been tampered with by comparing checksums provided by the vendor against the downloaded patch file. Test the patch in a non-production environment to identify any compatibility issues before rolling it out to production systems. Implement a rollback and maintain detailed records of all patches applied, including version numbers and installation dates.

c) **Protection of backup images and secure image creation**: Establish a secure image creation process, including checksum verification and digital signing of images to prevent unauthorised modifications. Store signed images in a dedicated, access-controlled repository, utilising encryption at rest and strong authentication mechanisms to restrict unauthorised access.

d) **Security Assurance:** 5G network systems and components should be tested for security assurance based on established frameworks, such as the Network Equipment Security Assurance Scheme (NESAS)**.**

4.7 Exploit of Misconfigured Network Functions

Threat Description

Misconfigurations, whether intentional or accidental, create vulnerabilities by deviating from secure system settings. In 5G networks, these weaknesses can be exploited to disrupt services, bypass security controls, redirect data, or enable fraudulent access.

Impact

Confidentiality

Improper configuration of network slicing, access control policies, or encryption settings can expose subscriber, enterprise, or IoT data. Misconfigured security policies in critical control plane protocols such as Packet Forwarding Control Protocol (PFCP) or critical core network element such as Session Management Function (SMF) can allow unauthorised rerouting of user traffic, leading to leakage of sensitive data.

Integrity

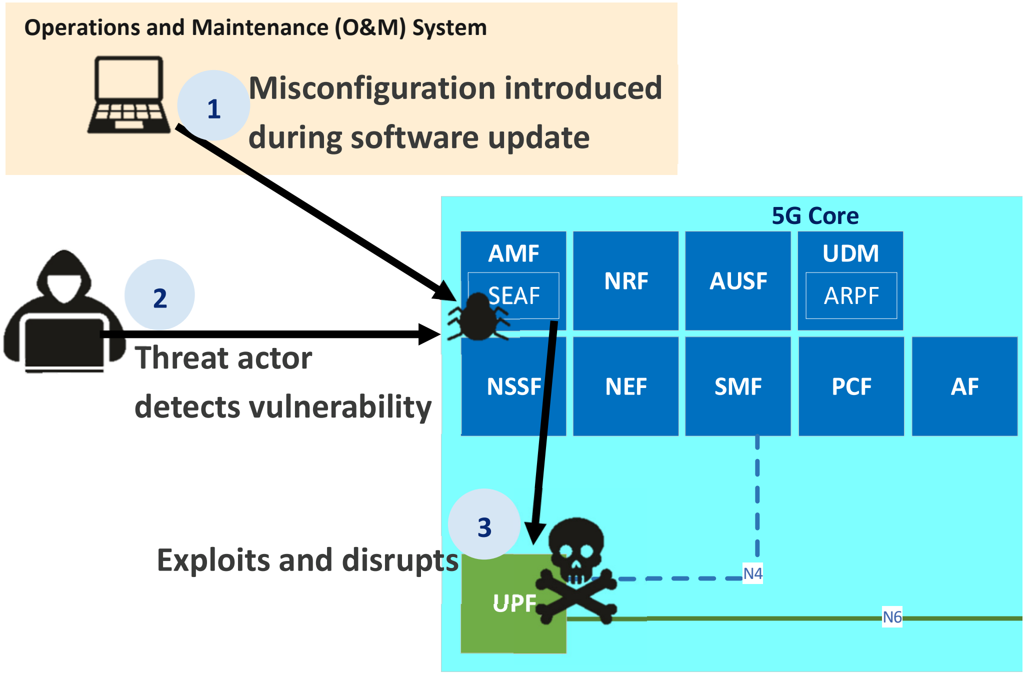
Misconfiguration of the network functions could introduce vulnerabilities that can be exploited by threat actors to carry out attacks, such as altering or injecting malicious traffic, to corrupt data or disrupt operations.

Availability

Incorrect security policies or rules may allow threat actors to flood the User Plane Function (UPF) with excessive traffic, leading to service disruptions or network crashes. Misconfigurations in firewalls, intrusion detection systems (IDS), or encryption policies can leave the private 5G network vulnerable to attacks. (e.g., disabling TLS encryption on control plane interfaces could expose the entire core network to man-in-the-middle (MITM) attacks.)

Possible Attack Scenario

A routine operational maintenance for a network function within the 5G core network inadvertently introduces a subtle misconfiguration in session establishment rules, leaving a window of vulnerability. A malicious threat actor monitoring the network, detects this anomaly and exploits the misconfiguration by crafting targeted control plane requests, overwhelming the User Plane Function (UPF) with invalid sessions, triggering disruption to service.


Operations and Maintenance (O&M) System
1
Misconfiguration introduced during software update
2
Threat actor detects vulnerability
3
Exploits and disrupts
5G Core
AMF
SEAF
NRF
AUSF
UDM
ARPF
NSSF
NEF
SMF
PCF
AF
UPF
N4
N6

Cybersecurity Recommendations

a) **System hardening:** Harden all Operations and Maintenance (O&M) systems by disabling unnecessary services and applying security patches promptly. Implement secure software development lifecycle (SSDLC) processes for any custom O&M tools. Implement version control policies for all configuration files, to allow for quick rollback to previous states in case of errors. The policies should include a rigorous testing process, including unit integration, and system testing, to validate NF configurations before deployment to production systems.

b) **Isolation of O&M networks:** Isolate the O&M network logically and physically from the user plane network, limiting connectivity and preventing lateral movement in case of a breach. Encrypt all communication within the O&M network using strong cryptographic protocols like TLS or IPsec.

c) **Change management processes:** Establish change management processes that require peer reviews and approvals for all configuration changes. Regularly audit NF configurations to identify any deviations from established baselines and enforce configuration compliance. Use RBAC to restrict configuration changes by unauthorised personnel.

d) **Secure remote access:** Remote access to private 5G systems should be authenticated by MFA, consistent with the enterprise's privilege account protection policies. Virtual Private Networks (VPNs) should be (e.g., IPsec or TLS) established with strong encryption protocols for all remote connections, protecting data in transit. Regularly audit remote access logs to detect any suspicious activity.

e) **Privileged Identity and Access Management (PIAM):** Implementing a PIAM solution can prevent misconfiguration by centralising and automating the management of privileged accounts, enforcing the principles of least privilege to ensure administrators and systems only have the necessary permissions to carry out their tasks, reducing the risks from human errors or malicious access leading to incorrect configurations.

f) **Dedicated jump server:** Implement a dedicated jump server within the private 5G network for administrative access to configurations and sensitive data to add an extra layer of isolation to the actual servers and network functions.

5. Summary of Threats and Recommendations

S/N	Threats	CIA Triad			Key Recommendations
		C	I	A	
1	**Eavesdropping**	🟨			• Subscriber Concealed Identifier • TLS for user plane • Packet Data Convergence Protocol with AES • Network Slicing • Local Breakout of User Plane Function
2	**Radio Jamming**			🟨	• Load balancing • Monitoring and detection • Anti-jamming techniques • MIMO for multiple simultaneous data streams
3	**Exploit of Multi-tenancy Environment**	🟨	🟨	🟨	• Robust hypervisor-based isolation • Strong authentication and authorisation • Strict access control policies • Secure inter-VM and inter-container communication • Monitor resource usage and security events • Secure communication channels • Trusted execution environments
4	**DoS Attack**			🟨	• Robust patch processes • Rate limiting • Incident response plan • Network Slicing
5	**Data Exfiltration**	🟨			• Role-based controls and least privilege principle • Strong data protection measures • Secure erasure or disposal of residual data • Network Slicing • Local Breakout of User Plane Function
6	**Malware**	🟨	🟨	🟨	• Zoning and segmentation based on application requirements • Robust patch management process and verification of digital signatures • Protection of backup images and secure image creation • Security Assurance
7	**Exploit of Misconfigured Network Functions**	🟨	🟨	🟨	• System hardening • Isolation of O&M networks • Change management processes • Secure remote access • Privileged Identity and Access Management (PIAM) • Dedicated jump server

6. Terms and Definitions

Terms	Definitions
Access Control	Access functions, which include identification, authentication, authorisation, and accountability.
Attack Vector	A path or method that a cybercriminal uses to gain unauthorised access to a system, network, or application, exploiting vulnerabilities to carry out malicious activities.
Authentication	Act of confirming the identity of an entity.
Authorisation	Act of specifying the access permissions to a resource.
Availability	Ensuring timely and reliable access to and use of information.
Confidentiality	Property that information is not made available or disclosed to unauthorised individuals, entities, or processes.
Denial of service (DoS)	Prevention of authorised access to a system resource or the delaying of system operations and functions, with resultant loss of availability to authorised users.
Encryption	The process of converting plaintext data into unreadable ciphertext, ensuring confidentiality.
Hardening	The process of securing systems and applications by reducing their attack surface, patching vulnerabilities, and disabling unnecessary services.
Integrity	Guarding against improper information modification or destruction and includes ensuring information non-repudiation and authenticity.
Internet of Things (IoT)	System of physical and virtual entities that are connected with one another allowing interaction anytime & anywhere.
Least Privilege Principle	The concept that dictates user and systems should only have access to the minimum resources and permissions necessary to perform their required tasks, minimising potential for security breaches.
Local Breakout	User Plane Function (UPF) Local Breakout deployment allows user's data traffic to be distributed at edge or node closer to user based on requirements (e.g., privacy or latency).
Mitigation	The proactive or reactive measure taken to reduce the likelihood and/or impact of potential or actual cyber threats, vulnerabilities or risk.
Multi-access Edge Computing (MEC)	The 5G software defined network introduces multi-access edge computing (MEC) which pushes virtualised computing activities outward to the edge of the 5G network (i.e., nearer to the base stations).

Network Slicing	Technology that allows service provider to create multiple, virtualised, logically independent networks (or "slices") on top of the physical network infrastructure.
Operation & Maintenance (O&M) Network	The network infrastructure and systems used for Operation and Maintenance (O&M) activities, critical for ensuring the smooth and secure functioning of a system.
Private 5G network	A mobile network, similar to a public 5G network, but provides restricted access and usage to a specific organisation or entity, allowing them to control and customise the network for their unique needs within a defined area.
Public 5G network	A wireless network that is owned and operated by mobile network operator (MNO) and provides internet connectivity to the public, offering services like voice calling, messaging and video streaming.
Risk Assessment	A systematic process of identifying, analysing, and evaluating potential hazards and risks to determine the likelihood and severity of harm, and then implementing control measures to minimise or eliminate those risks.
Service-Based Architecture (SBA)	A modular framework where core network functions (NFs) are designed as independent, reusable components that communicate via Service-Based Interfaces (SBIs) enabling dynamic network elasticity and scalability.
Sniffing	The process of intercepting and examining data packets as they travel across a network, potentially revealing sensitive data or information.
Subscriber Concealed Identifier (SUCI)	The Subscriber Permanent Identifier (SUPI) enhances subscriber privacy to mitigate against the threats from IMSI catchers. SUPI is encrypted when sent over-the-air as a one-time temporary identifier called the Subscriber Concealed Identifier (SUCI).
Third-Party Application	A software program developed by a company or individual other than the manufacturer of the device or the enterprise deploying it.
Threat Actor	Any individual, group, or entity that intentionally causes harm or poses a risk to computer system, network, data, or information, often with malicious intent.
User Equipment (UE)	A subscriber's device, such as a cell phones, tablets, modems, or any other equipment capable of connecting to 5G services.
Virtualisation	The creation of a virtual version of a physical machine, operating system, server, network or resource, to enable the efficient use of physical resources.
Virtual Private Network (VPN)	A secure, encrypted connection, usually over a less secure network that allows users to send and receive data as if their devices are directly connected to a private network.

7. Abbreviations and Acronyms

Acronym	Meaning
3GPP	3rd Generation Partnership Project
5G	5th Generation Mobile Network
AES	Advanced Encryption Standard
AF	Application Function
AMF	Access and Mobility Management Function
API	Application Programming Interface
APRF	Authentication Credential Repository and Processing Function
AUSF	Authentication Server Function
C2	Command and Control
CIA	Confidentiality, Integrity, Availability
CII	Critical Information Infrastructure
CIIO	Critical Information Infrastructure Owner
CPU	Central Processing Unit
CSA	Cyber Security Agency of Singapore
DDoS	Distributed Denial of Service (attack)
DN	Data Network
DoS	Denial of Service (attack)
EASDF	Edge Application Server Discovery Function
ENISA	European Union Agency for Network and Information Security
gNB	Next Generation Node B
GSMA	Global System for Mobile Communications Association
IDS	Intrusion Detection System
IMSI	International Mobile Subscriber Identity
IP	Intellectual Property
IPSec	Internet Protocol Security
IT	Information Technology
LTE	Long Term Evolution
MEC	Multi-access Edge Computing
MFA	Multi-Factor Authentication
MIMO	Multiple-input and Multiple-output
MITM	Man-In-The Middle
MNO	Mobile Network Operator
NEA	New Radio Encryption Algorithm
NEF	Network Exposure Function
NESAS	Network Equipment Security Assurance Scheme
NRF	Network Repository Function
NSACF	Network Slice Admission Control Function
NSSAAF	Network Slice Specific Authentication and Authorization Function
NSSF	Network Slice Selection Function
O&M	Operations and Maintenance

PCF	Policy Control Function
PFCP	Packet Forwarding Control Protocol
PFICH	Physical Format Indicator CHannel
R&D	Research and Development
RAN	Radio Access Network
RATs	Remote Access Trojans
RBAC	Role-Based Access Control
RRC	Radio Resource Control
SBA	Service-Based Architecture
SCP	Service Communication Proxy
SDR	Software-defined Radio
SEAF	Security Anchor Function
SEPP	Security Edge Protection Proxy
SIEM	Security Information and Event Management
SMF	Session Management Function
SSDLC	Secure System Development Lifecycle
SUCI	Subscriber Concealed Identifier
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UDM	Unified Data Management
UE	User Equipment
UPF	User Plane Function
VLANs	Virtual LANs
VMs	Virtual Machines
VPN	Virtual Private Network
Wi-Fi	Wireless Fidelity

8. References

S/N	Document	Source	Dated
1	Technical Specifications for Security Architecture and Procedures for 5G Systems (TS 33.501)	3GPP	Oct 2018
2	Potential threat vectors to 5G infrastructure	CISA	May 2021
3	Security Guidance for 5G cloud infrastructures Part I: Prevent and Detect Lateral Movement	CISA	Oct 2021
4	Security Guidance for 5G cloud infrastructures Part III: Data Protection	CISA	Dec 2021
5	Guidelines for CII Owners to Enhance Cyber Security for 5G Use Cases	CSA	Apr 2022
6	Private 5G Networks – Secure Connectivity for Industry 4.0	Deloitte	Nov 2022
7	Threat Landscape for 5G Network	ENISA	Dec 2020
8	Security in 5G Specifications	ENISA	Feb 2021
9	Guideline on Security Measures under the EECC	ENISA	July 2021
10	5G Supplement – to the Guideline on Security Measures under the EECC	ENISA	July 2021
11	Exploring 5G Private Network Opportunities in Asia Pacific	GSMA	Feb 2023
12	Best Practices of GSMA Mobile Cybersecurity Knowledge Base	GSMA	Apr 2024
13	FS.40 5G Security Guide V3.0	GSMA	July 2024
14	FS.31 GSMA Baseline Security Controls V4.0	GSMA	Apr 2024
15	FS.31 GSMA Baseline Security Controls V5.0	GSMA	Apr 2025
16	GSMA Mobile Telecommunications Security Landscape 2025	GSMA	Feb 2025
17	5G Security: Analysis of Threats and Solution	IEEE	Sep 2017
18	RAIN: Risk Assessment Framework Based on an Interdependent Input Propagation Network for a 5G Network	IEEE	Jun 2023
19	MITRE FiGHT v2.1.1	MITRE	Feb 2025

QUERIES & FEEDBACK

Questions and feedback on this document may be submitted to:

CSA-TCPO@csa.gov.sg