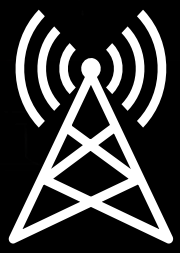
Palindrome Technologies

ASSURANCE | TRUST | CONFIDENCE

# Private 5G Security uncovered



## Lessons from Industrial Automation

Peter Thermos, Shashank Murali

PALINDROME TECHNOLOGIES

www.palindrometech.com

The Challenge: Securing Private 5G Networks in a Multifaceted Threat Landscape ..... 2
Solution: A Holistic, Standards-Aligned Security Assessment ..... 3
Testing Methodology ..... 3
Key Test Areas: Understanding the Security Assessment ..... 5
Results: Critical 5G-Specific Vulnerabilities Identification ..... 7
Measurable Outcomes: Enhancing Security Posture and Fostering Stakeholder Trust ..... 8
Conclusion and Next Steps ..... 9

## The Challenge: Securing Private 5G Networks in a Multifaceted Threat Landscape

The global telecommunications infrastructure is undergoing a radical transformation, spearheaded by the deployment of Fifth Generation New Radio (5G-NR) technology. 5G enables a diverse ecosystem of real-time applications, including enhanced Wireless Priority Services (eWPS), Internet of Things (IoT), Massive Machine Type Communications (mMTC), enhanced Mobile Broadband (eMBB), Virtual Reality (VR), and Augmented Reality (AR). This ecosystem leverages technologies such as high-speed mobile connectivity, distributed cloud environments, virtualized network functions (SDN/NFV), open-source software components, and machine-learning algorithms for automated service orchestration and Operations, Administration, Management, and Provisioning (OAM&P).

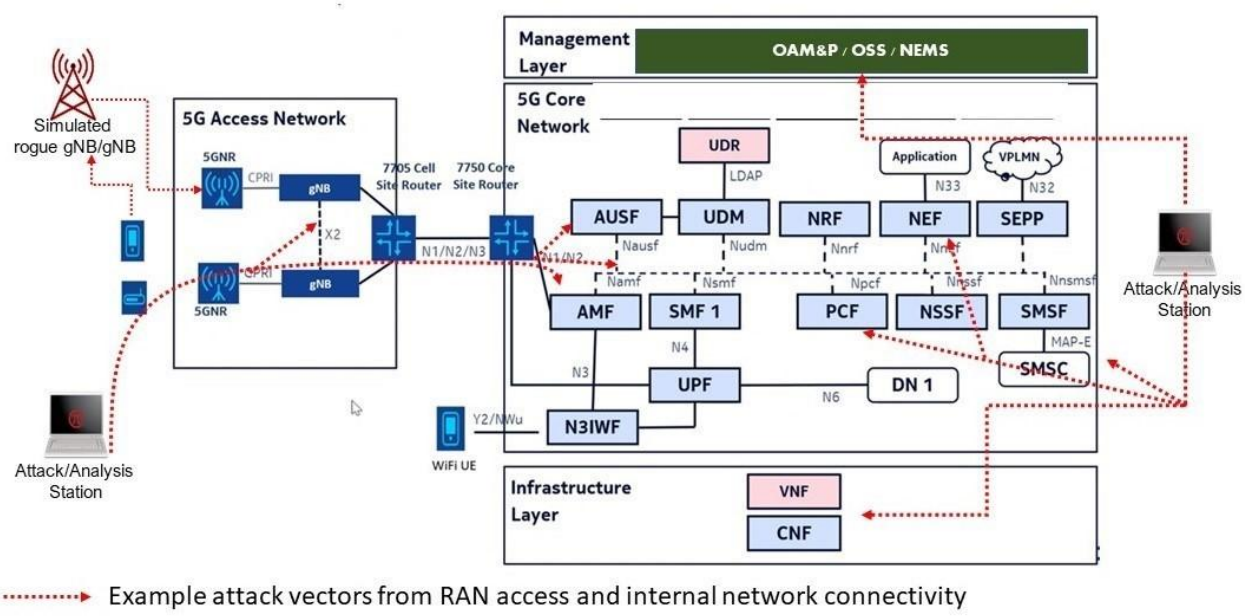
While 5G offers enhanced system capacity, data rates, reduced latency (under 10 milliseconds), massive device connectivity, and improved security, its inherent complexity introduces new attack vectors. Unlike 4G LTE, 5G leverages cloud computing technologies, including software-defined networking (SDN), network function virtualization (NFV), virtualization, and multi-access edge computing (MEC).

Furthermore, the 5G ecosystem leverages several standards and protocols (e.g., NAS, DIAMETER, SIP, HTTP/2/TLS) to support a variety of use cases for both consumers and enterprise organizations (e.g., Industry 4.0/M2M, Telemedicine, AV/VR, smart cities). The diverse technologies used to support 5G, the multitude of interactions, and interdependencies between the various architectural elements (e.g., radio access, core network elements, network functions, and protocols) increase the level of complexity and consequently introduce new attack vectors. This mandates rigorous security assessments, drawing on expertise and guidance from organizations such as 3GPP, NIST, ISASecure, GSMA, IEEE, CISA, and ENISA.

The stringent requirements of industrial automation, necessitating real-time performance, ultra-reliability, and robust security, amplify the security risks.

A compromise can lead to data breaches, disruptions in critical processes, potentially resulting in physical damage, safety incidents, and significant financial losses. This case study details a security assessment of a private 5G Standalone (SA) network designed to support industrial automation. The objective is to identify vulnerabilities, assess the risk and impact of relevant threats, and determine the viability of applicable attacks, including eavesdropping, disruption, rogue base stations, and unauthorized access to network elements and operational technology (OT).

## Example Private 5G Network

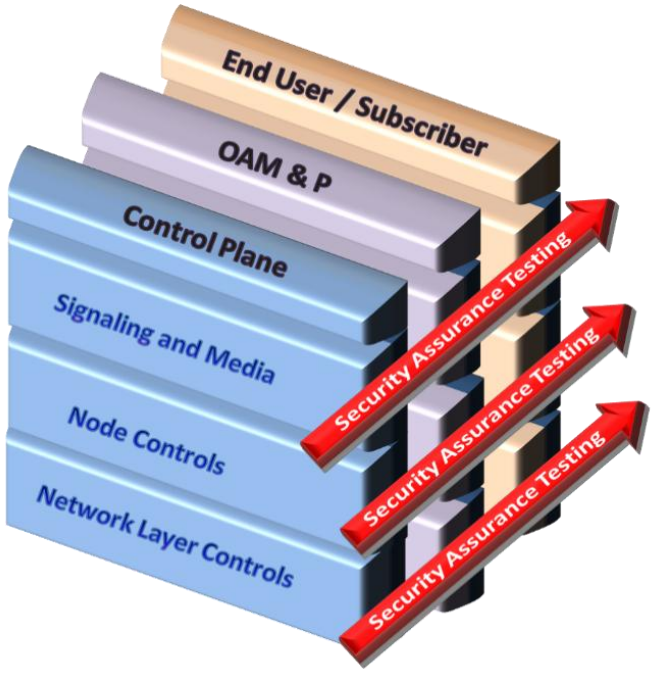



## Solution: A Holistic, Standards-Aligned Security Assessment

Palindrome adopted a holistic and layered approach, aligning with 3GPP specifications and industry best practices to evaluate the security posture of the private 5G network. This involved validating component security, end-to-end service flows, and adherence to relevant security standards. The assessment scope encompassed platform software, signaling protocols, control plane protocols, OAM&P interfaces, applications, services, and device hardware.

## Testing Methodology

The security assurance testing is part of an organization's continuous efforts to minimize security risks in the operational infrastructure including organizational data and impact to operations. Palindrome's security assurance testing methodology leverages techniques and methods that focus on validating the target component's security along with end-to-end service flows to determine proper alignment with industry standards and best security practices.




The evaluation approach comprises the following phases:

- **Phase I: Information gathering and scope refinement**: This phase involves a comprehensive review of the target environment, including network diagrams, system configurations, and security policies. The goal is to establish a clear understanding of the assessment scope and objectives and to identify key stakeholders and communication channels.

- **Phase II: Conduct a focused Threat Modeling exercise**: This phase entails creating a detailed threat model specific to the 5G implementation. This includes identifying potential threat actors, attack vectors, and the assets at risk. The threat model is used to prioritize testing efforts and ensure that the assessment addresses the most critical security concerns. Threats associated with the target solution (TOE), in this case Private 5G, are identified and classified along with recommendations on validating controls to minimize risk.

- **Phase III: Security Analysis and Penetration Testing**: This phase involves executing a comprehensive suite of security tests based on the threat model developed in Phase II and the information gathered in Phase I. This includes both automated and manual testing techniques to identify vulnerabilities in the 5G network infrastructure, applications, and services. Specific testing activities may include performing penetration tests against network elements, analyzing signaling protocols for vulnerabilities, assessing the security of APIs and web

interfaces, and evaluating the effectiveness of security controls such as firewalls, intrusion detection systems, and access control mechanisms. Results from the testing are carefully documented, with vulnerabilities categorized and prioritized based on their severity and potential impact. The security testing evaluates the solution's controls to protect against the identified threats and consists of performing a security baseline and penetration testing using various techniques, including, but not limited to, service and protocol enumeration, application mapping, vulnerability scans, exploitation of vulnerabilities, and signaling protocol analysis. The penetration testing comprises a Deterministic phase and a non-Deterministic phase. The Deterministic phase evaluates the TOE's ability to properly enforce the designed security controls against known attacks and vulnerabilities. The non-Deterministic phase explores novel attack vectors and identifies 0-day vulnerabilities associated with the TOE's implementation.

## Key Test Areas: Understanding the Security Assessment

To provide a comprehensive security assessment of the private 5G network, our testing methodology focused on several critical areas. These areas were chosen to address the most likely attack vectors and vulnerabilities, ensuring a robust and secure deployment.

1. **RAN (Radio Access Network) Signaling / Call Flow Security Analysis**
    a. *Why this is important*: The RAN is the entry point to the 5G network. Securing it is paramount to prevent unauthorized access and malicious activities.
    b. *What we tested:* Palindrome performed test cases to verify the security controls that prevent attacks on the RAN access such as Rogue Base Stations, Man-in-the-Middle (MitM) attacks, and eavesdropping.
    c. *Examples of specific tests*:
        i. Integrity protection of RRC signaling
        ii. Integrity protection of user data between the UE and gNB
        iii. Ciphering of RRC signaling
        iv. Ciphering of user data between the UE and the gNB
        v. Replay protection of user data between the UE and gNB

2. **5G Core Network Function - Call Flow Security Analysis**
    a. *Why this is important*: The 5G core is the brain of the network, responsible for authentication, authorization, and session management. A compromised core can have catastrophic consequences.
    b. *What we tested:* Palindrome evaluated the security of the 5G core Network Functions individually and in end-to-end scenarios to prevent unauthorized access and ensure proper data handling.

c. *Examples of specific tests*:
    i. Impersonated PDU session establishment
    ii. Rogue NF discovery authorization
    iii. SMF API Analysis
    iv. UDM API Analysis
    v. AMF API Analysis
    vi. NRF API Analysis

3. **Infrastructure – Operating System, application servers, virtualization/cloud (i.e., VMs, Kubernetes, Docker)**
    a. *Why this is important*: The underlying infrastructure (OS, virtualization, cloud) provides the foundation for the 5G network. A vulnerability at this level can compromise the entire system.
    b. *What we tested*: Palindrome validated the security controls enforced by the virtualization/cloud environment and operating systems to prevent unauthorized access to Network Elements and the management platform(s).
    c. *Examples of specific tests*:
        i. OS Configuration Analysis
        ii. Orchestration (Kubernetes) analysis
        iii. Container Analysis

4. **Management Web interfaces (OAM&P)**
    a. *Why this is important*: OAM&P interfaces are used to manage and monitor the 5G network. A vulnerability here could allow attackers to take complete control of the system.
    b. *What we tested*: Palindrome focused on testing the security of Operations, Administration, Management, and Provisioning functions, ensuring that only authorized personnel can access sensitive data and perform critical operations.
    c. *Examples of specific tests*:
        i. Session Management
        ii. Role Based Access
        iii. Data Validation
        iv. Network Protocols
        v. Configuration
        vi. Auditing and Logging
        vii. OWASP Top 10

5. **Hardware security analysis of the Radio Nodes (i.e., gNB/eFemto)**
    a. *Why this is important*: Physical access to radio nodes can allow attackers to tamper with the hardware, extract sensitive data, or compromise the entire network.

b. *What we tested*: Palindrome explored various areas applicable to the device configuration, focusing on unauthorized access and potential hardware vulnerabilities.
c. *Examples of specific tests*:
    i. Unauthorized access to local Admin/Debug interface (e.g., USB, RS232, RJ45, HDMI)
    ii. Boot sequence protection evaluation (Secure boot/TPM)
    iii. Hardware Root of Trust verification

## Results: Critical 5G-Specific Vulnerabilities Identification

The penetration testing exercise produced a detailed report of vulnerabilities, categorized and prioritized based on severity, exploitability, and potential impact.

Key findings included:

- **NAS Authentication Vulnerabilities**: Implementation flaws in NAS authentication procedures (as specified in 3GPP TS 33.501) could allow attackers to impersonate legitimate users or gain unauthorized access to the network. These vulnerabilities could be exploited by attackers using rogue gNBs to intercept and manipulate authentication traffic.
- **PFCP Signaling Exploits**: Misconfiguration or vulnerabilities in PFCP signaling could enable attackers to disrupt user plane traffic or gain control over data forwarding paths.
- **Kubernetes Misconfigurations**: Improperly configured network policies and RBAC settings in the Kubernetes environment could allow attackers to compromise containers and gain unauthorized access to network elements.
- **Unsecured OAM&P Interfaces**: Vulnerabilities in OAM&P interfaces could allow attackers to gain administrative access to the network, potentially leading to complete system compromise.
- **Hardware Tampering Risks**: Insufficient hardware security controls on radio nodes could allow attackers to tamper with firmware, extract cryptographic keys, or disable the devices.

## Measurable Outcomes: Enhancing Security Posture and Fostering Stakeholder Trust

The security assessment of the private 5G network yielded tangible and measurable outcomes, demonstrating the value of a proactive and comprehensive security approach:

- **Prioritized Vulnerability List**: A comprehensive list of 7 critical and 23 high-severity vulnerabilities was identified, categorized, and prioritized based on exploitability and potential business impact. This list included detailed technical descriptions, attack vectors, and remediation recommendations aligned with industry best practices (e.g., 3GPP, GSMA, NIST, OWASP, DHS-CISA).
- **Improved Security Awareness**: The client's security team gained enhanced understanding of 5G-specific security threats and vulnerabilities, resulting in a 30% increase in their ability to recognize indicators of attack and respond to potential incidents during simulated attack scenarios.
- **Strengthened Security Controls**: Implementation of recommended security enhancements led to 75% reduction in exposed attack surface by hardening configurations and patching vulnerabilities. The remaining 25% is associated with potential exposure of edge devices and external service providers (i.e., Spectrum Management/CBRS).
- **Enhanced Stakeholder Confidence**: Increased confidence among stakeholders (including operations, engineering, and executive management) in the security of the private 5G network. This resulted in:
    - Approval for expanding 5G deployment to additional industrial automation plant operations.
    - Improved compliance with industry requirements (e.g., DHS-CISA, ISASecure, NIST GSMA) related to data security and privacy.
- **Demonstrated Commitment to Security Assurance**: A clear demonstration of a commitment to continuous security assurance through proactive identification and mitigation of potential security risks. This commitment:
    - Positions the organization as a leader in 5G security within the industrial automation sector.
    - Provides a competitive advantage by demonstrating a proactive approach to risk management.

## Conclusion and Next Steps

This case study demonstrates the critical need for robust security assessments of private 5G networks, especially in demanding industrial automation environments. Palindrome's multi-layered approach, adherence to industry standards, and in-depth technical expertise provide a clear path for organizations to secure their 5G deployments.

As part of our efforts helping organizations improve their cybersecurity posture, we have compiled the top 10 areas that security teams should consider when deploying private 5G.

### Private 5G – Top 10 Security Prioritization Areas

| | |
|---|---|
| 1 | Hardware : UE, IoT devices, gNB/eFemtos/extenders |
| 2 | RAN Signaling |
| 3 | 5G Core Signaling |
| 4 | Network Slicing |
| 5 | Network Infrastructure : Fronthaul/mid-haul/backhaul |
| 6 | Virtualization / Cloud Infrastructure : MEC (Multi-access Edge Computing) |
| 7 | Management and Network Orchestration Applications (MANO/OAM&P/OSS) |
| 8 | Supply Chain : Product security verification and attestation |
| 9 | Network Peering Functions – Security Edge Protection Proxy (SEPP) : Partner networks |
| 10 | Network Exposure Functions (NEF) : API's for device telemetry and Artificial Intelligence workloads |

To discuss your specific private 5G security requirements and explore how Palindrome can help you achieve a robust security posture, you may contact us for an exploratory discussion. We're ready to help you navigate the complexities of 5G security and ensure a safe and reliable foundation for your future innovations.

## Contact Information

services@palindrometech.com

www.palindrometech.com

## About Palindrome Technologies

Palindrome's organizational philosophy is built upon three fundamental principles

***Assurance***

***Trust***

***Confidence***

Founded in 2005, Palindrome Technologies Inc. is a leading applied information security research firm and analysis laboratory having expertise in emerging technologies, embedded systems, communication networks, software, and cloud platforms.

Prior forming Palindrome, the principals of the company worked for Bellcore (Bell Communications Research) in the Security & Fraud group where they supported security assurance efforts for telecommunication providers, product vendors and the US government.

Since its inception Palindrome has been providing a range of high-tech services related to securing emerging technologies, global enterprise organizations (I.e., healthcare, financial, energy, government) and carrier-grade networks.

Palindrome is an accredited ISO/IEC 17025 testing laboratory as well as a FCC, GSMA, CTIA and IEEE designated Cybersecurity Testing Lab. Palindrome has been helping global enterprise organizations, service providers and product vendors with deploying and maintaining secure networks, services, and products. The Palindrome team is also known for its contributions to industry standards bodies (e.g., IEEE, GSMA, CTIA and ATIS), and branches of the US government such as FCC CSRIC VII, CSRIC IX and NIST.