



WHITE PAPER

Keeping Pace with the Requirements of 5G Security

Keeping Pace with the Requirements of 5G Security

Introduction

The requirements for 5G Security are continually evolving, as is the attack surface. Here, a continuous and growing number of vulnerabilities must be accounted for in a comprehensive testing approach, and with the capability of accelerated speed powered by state-of-the-art automation. Spirent SecurityLabs' years of experience in testing a range of environments, along with Spirent's industry-leading expertise in 5G testing, offer a mature and informed perspective on the best practices of 5G cybersecurity, which are presented in this white paper.

The Rapid Evolution of 5G Security Requirements

Network operators are actively engaged in deploying 5G networks around the globe on a widespread scale. This technology trend is defining and transforming the technological landscape for the foreseeable future. Meanwhile, a myriad of new 5G devices is appearing in the market, with many more to come. As with any new technology, security must be taken into consideration as early as possible in the development process. To face that challenge, 5G security was substantially redesigned to address the known vulnerabilities that existed within the architecture of earlier networks. New cybersecurity frameworks were developed:

- **Zero Trust and Zero Trust Network Access (ZTNA).** Zero Trust eliminates the notion of trust, necessitating that access must be granted for each application transaction
- **Use of encryption on the transport-level.** Targeted at preventing malicious unauthorized altering of transmitted data between endpoints and eavesdropping
- **Mutual authentication.** Where the sender and recipient must verify the other party is genuine and trusted
- **Secure Access Secure Edge (SASE).** A cloud-centric distributed security architecture securing users and applications as opposed to subnetworks and IP resources

Failure to adopt these strategies, or to implement them without comprehensive and continuous execution, can lead to security breaches on varying scales with varying impacts.

Understanding the vulnerabilities in 5G cybersecurity

Telecommunication network carriers, services providers, equipment manufacturers, suppliers, and enterprise organizations have common areas of concern. They reside in the 5G core (NFs, NFVi), telecommunication infrastructure (physical and virtual) and transport security. Cloud security, cloud-native components (containers, Kubernetes, etc.) must also be accounted for, along with applications and application programming interfaces (APIs), edge devices, and network products.

Typical vulnerabilities. Through Spirent SecurityLabs engagements, an array of vulnerability categories has been identified during the assessment phase. They include:

- **Hardware/Firmware/Software.** Misconfigurations (e.g., incorrect access rights); Default or static credentials; Unrestricted access through diagnostic interfaces.
- **Signaling/Control Plane protocols.** Insecure protocols in use; Authentication bypass.
- **Containers/Kubernetes.** Admission controller: no restriction of specific registries; Host OS issues: over-permissive access, outdated software.
- **PKI/NF.** Network function (NF) isolation issues in the platform; Misconfigurations in encryption algorithms used in NF-to-NF communications; Integrity and confidentiality issues on the policy store and routing info (data-at-rest); Protocol support issues at the PKI (Public Key Infrastructure) platform and NFs.
- **Operations, Administration and Management.** Insecure APIs; Various privilege escalations; Various authentication and authorization issues; Outdated software; Missing critical patches.

Potential impact of risk. If the vulnerabilities remain unaddressed, the impact can affect an organization in a host of ways, some more severe than others, yet all impacting the ability to conduct an organization's business operations as planned. The domains these threats occur in include:

- **Core network.** Abuse of remote access; Abuse of user authentication/authorization data; Abuse of third-party hosted network functions; API exploitation; Exploitation of poorly designed architecture and planning (network, services and security, administrative interfaces); Exploitation of misconfigured or poorly configured systems/networks; Fraud scenarios related to roaming interconnections; Memory scraping; Manipulation of network traffic, network reconnaissance and information gathering; Manipulation of network configuration data; Malicious flooding of core network components; Malicious diversion of traffic; Manipulation of the network resources orchestrator; Opportunistic and fraudulent usages of shared resources; Registration of malicious NFs; Traffic sniffing; Side-channel attacks.
- **Access network.** Abuse of spectrum resources; Address Resolution Protocol (ARP) poisoning; Fake access network node; Flooding attack; international mobile subscriber identity (IMSI) catching attacks; Jamming the radio frequency; MAC spoofing; Manipulation of access network configuration data; Radio interference; Radio traffic manipulation; Signaling exploitation.
- **Multi-edge computing.** False or rogue multi-edge compute (MEC) gateway; Edge node overload; Abuse of edge open APIs.
- **Virtualization.** Abuse of Data Centers Interconnect (DCI) protocol; Abuse of cloud computational resources; Network virtualization bypassing; Virtualized host abuse.
- **Physical infrastructure.** Manipulation of hardware equipment; Threat from third parties' personnel accessing mobile network operator's (MNO's) facilities; universal integrated circuit card (UICC) smart card format exploitation; User equipment compromising.
- **Generic.** Denial of service (DoS); Data breach, leak, theft destruction and manipulation of information; Eavesdropping; Exploitation of software and hardware vulnerabilities; Malicious code or software; Compromised supply chain, vendor, and service providers; Exploiting flaws in security, management, and operational procedures; Abuse of authentication; Identity theft or spoofing.



Details on potential threats and their impacts

Having a deeper understanding of the impact and threats helps organizations understand the need for prioritized attention to ensure the threats are managed timely in a comprehensive cybersecurity strategy.

Location	Threat	Risk	Impacts
Hardware	Lack of system isolation	Critical	Shared resources for CNF/VNF*
CNF	Access to namespaces	Critical	Egregious permissions on service accounts
CNF	Secure secrets storage	Critical	Insecure storage of sensitive information
CNF/VNF	Unauthenticated access	Critical	Unauthenticated access to NF functionality
CNF/VNF	Network services	Critical	Services exposed to untrusted segments
CNF/VNF	Logging mechanisms	Critical	Missing information about actions performed
PKI/CNF/VNF	Insecure API request	Critical	Handling of user-controlled variables
SM**/CNF/VNF	Third-party libraries	Critical	All related core functions
CNF/VNF	Default credentials	Critical	Known or insecure credentials in use
CNF/VNF	Authentication bypass	Critical	Unauthorized access to restricted resources
CNF/VNF	Privilege Escalations	Critical	Execute functions with higher permissions
CNF/VNF	Outdated software	Critical	Unpatched or outdated software
CNF/VNF	Improper configuration	Critical	Improper or misconfigurations of services
CNF/VNF	Insecure encryption at rest	Critical	Insecure storage of sensitive data at rest
Network	Firewall	Critical	Unrestricted network port access
Network	Network access controls	Critical	Unrestricted access to networked resources
Network	Insecure protocols	Critical	Weak or insecure communication protocols
Network	Insecure encryption in transit	Critical	Insecure transmission of sensitive data
Network	Lack of network isolation	Critical	Sharing of resources for network functions

* CNF (cloud-native network functions; VNF (virtual network functions)

** SM (service mesh)

Top 5 5G Security Threats Discovered by Spirent SecurityLabs

Through Spirent's extensive global SecurityLabs engagements, the top five 5G vulnerabilities exposed were:

- **Unauthenticated remote code execution (RCE)** – Allows for a full compromise by a remote unauthenticated malicious user
- **Authentication bypass** (Unauthorized User) – Unauthorized direct access to restricted resources
- **Broken access control** – Unauthenticated access leaving compromised access to NF functionality
- **Services running as root user** – Unrestricted access to network resources
- **Information disclosure (pre-auth)** – Insecure encryption at rest leaving insecure storage of sensitive data

If these vulnerabilities remain undiscovered or are unaddressed, they can place an organization's business operations in a position of severe risk from both an operational and data security perspective.

Accounting for the complexity factors of 5G security

A well-designed 5G security testing strategy should address the wide range of needs across numerous dimensions. The testing approach should account for multiple:

- **Approaches**, which tend to fall within three broad categories: Prevention, detection, and remediation
- **Elements and layers** accounting for core, radio access, mobile edge, end-user device, and transport
- **Locations**, including internal networks and devices, remote networks, and devices
- **Supply chain considerations**, such as accounting for the security of new suppliers, supplier network access, equipment supply, and user and network data
- **Processes**, from secure operations, monitoring and auditing procedures to secure design, configuration, hardening, etc.
- **Telecom standards**, including security protocols, algorithms, interfaces, etc.
- **Criticality levels**, ranging from low-criticality use cases such as games and virtual reality; to mid-level criticality such as consumer-grade IoT and smart grid; to high-criticality use cases such as autonomous vehicles, IoT, remote surgery, and more
- **Phases of deployment** ranging from planning, to R&D, to innovation, to actual implementation and ongoing monitoring

Keeping Pace with the Requirements of 5G Security

In addition, any discussion of 5G security must include consideration of new network and device security threats. These range from threat surfaces such as virtualization (NFVi) attacks and multi-vendor weaknesses, cloud edge distribution attacks, massive IoT attacks, and security gateway attacks, to ever-evolving attack risks such as data breach, distributed denial-of-service (DDoS), resource exhaustion, man-in-the-middle, malware, fraud, VLAN hopping, authentication, authorization, and more.

The essentials of a 5G security testing strategy

The optimal starting point in crafting a 5G security strategy is to include 5G security in every business conversation from the outset and work with vendors you can trust to deliver security across all categories, particularly across the supply chain. Building security from the beginning, rather than bolt it on later is key. This facilitates test campaign development, to validate and trust the security measures you put in place. The goal is to not only be capable of implementing trustworthy 5G services, but to also foster innovation and add new value continuously.

Recognizing the magnitude of vulnerabilities, any comprehensive 5G cybersecurity testing strategy must be aimed at ensuring the security of modern complex 5G infrastructure. This should incorporate security analysis and testing at different layers including hardware, firmware, operating system, middleware, application, and protocol stacks (e.g., signaling and control plane). The testing strategy should include:

- **Security Compliance Testing (CST)**. This involves security evaluation of network products against relevant security standards and Security Assurance Specifications (SCAS).
- **Basic Vulnerability Assessment (VA)**. This includes using COTS, FOSS and proprietary tools for scanning and vulnerability assessment of 5G components, devices, and complete systems.
- **Enhanced Security Assessment and Penetration Testing (PT)**. This includes in-depth security analysis using custom tools, fuzzing, robustness testing, scenario-based testing; Controlled simulated DoS; Automation of repetitive assessment through scripting.

Security testing within the wider scope of 5G. A basic 5G security testing strategy should encompass a set of comprehensive cybersecurity testing services, aimed at ensuring the baseline security of modern complex 5G infrastructure, focused on requirements from 3GPP SCAS-3GPP TS 33.117 (General Security Requirements).

3GPP Security Assurance Specifications (SCAS). The core 3GPP standards that should be incorporated into any 5G testing strategy include:

- 3GPP TS 33.116 (MME Security Requirements)
- 3GPP TS 33.117 (General Security Requirements)
- 3GPP TS 33.216 (eNB Requirements)
- 3GPP TS 33.250 (PGW Security Requirements)
- 3GPP TS 33.511 (gNB Security Requirements)
- 3GPP TS 33.512 (AMF Security Requirements)
- 3GPP TS 33.513 (UPF Security Requirements)
- 3GPP TS 33.514 (UDM Security Requirements)
- 3GPP TS 33.515 (SMF Security Requirements)
- 3GPP TS 33.516 (AUSF Security Requirements)
- 3GPP TS 33.517 (SEPP Security Requirements)
- 3GPP TS 33.518 (NRF Security Requirements)
- 3GPP TS 33.519 (NEF Security Requirements)

Incorporating PKI security. Unlike most other communications networks, mobile systems provide no method to verify cryptographically the identity of the other end in the communication. Even newer 5G networks fail to prevent mobile devices from inadvertently camping on a malicious base station. The 5G protocol provides no means to verify cryptographically the identity of base stations and networks to which a mobile device connects. Establishing identity is fundamental to trust and effective security and PKI is a proven technology that enables large-scale device authentication, integrity, and reliable encryption for an extremely high level of trust. PKI certificates also provide a significant level of control. PKI security considerations include:

- Certificates (TLS/mTLS, type, parameters, validity, storage, key size)
- Cryptography in use (hashing and encryption algorithms)
- Assurance (trust validation, protocols, CRL, storage at rest, impersonation)
- Hardening (OS, platform, API, protocols)
- Security of API interfaces
- Network (data in transit protection validation, tampering, impersonation)

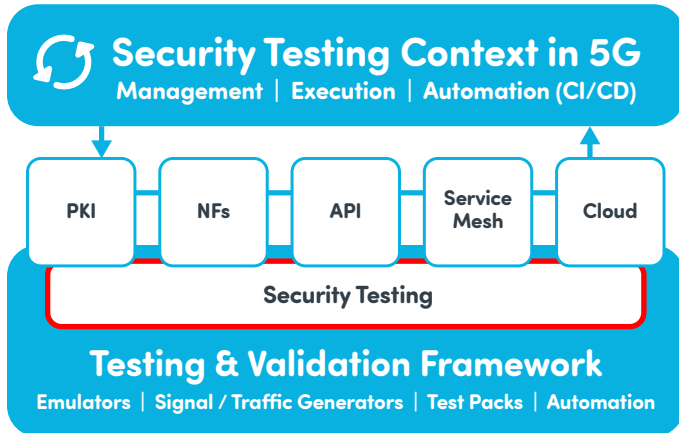


The following is an expanded list of PKI key functional priorities and offer important focal areas for any comprehensive cybersecurity test strategy.

Category	Field	Testing focus
PKI Platform	API	Security testing against the underlying API endpoint
PKI Platform	Security	Security testing against platform
PKI Platform	Network	Reliance and resilience testing against offered services
Cryptography	Issuance	Ensure certificates are issued and signed by CA/ISA
Cryptography	Type	Ensure certificates presented are X.509 compliant
Cryptography	Hashing	Identify if certificate hashing type meets requirements
Cryptography	Validity	Certificate validity and revocation functionality testing
Cryptography	Key Size	Identify if certificate key size meets requirements
Cryptography	Algorithm	Identify if certificate algorithms meet requirements
Cryptography	Validation	Strength and fortification validation against best practices
Assurances	Trust	Validation of root of trust between different network elements
Assurances	Availability	Ensure backup and recovery policies are followed for critical datasets
Assurances	Integrity	Ensure data cannot be manipulated through casual accesses
Networking	Protocols	Validate protocols, incorporate best practices and data protections
Networking	Data	Ensure data in transit is protected from casual inspection
Networking	Services	Ensure only approved services are operational

Having a test plan that incorporates PKI with NFVi/CNF/VNF security requirements, across the entire 5G Core infrastructure, is critical for achieving holistic security.

Taking wider 5G testing requirements into account. An additional and broader scope of requirements should include conducting security analysis and testing at different layers including operating system, NFs/CNFs, NFVi, service mesh, application, and protocol stacks (e.g., transport layer and control plane). Supported by test automation, this testing approach needs to include emulation of complex multi-vector attacks that test and audit the 5G core environment to pre-emptively identify vulnerabilities, misconfigurations and mitigate risks.



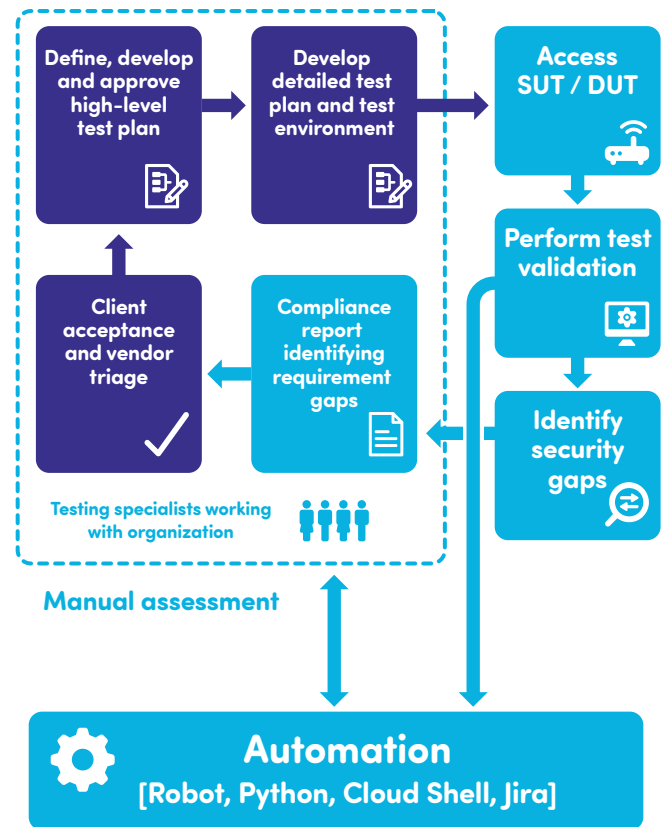
Integrated 5G Security Testing

Ensuring holistic coverage in the 5G testing strategy.

Ultimately, providing a set of comprehensive cybersecurity services, aimed to ensure the security of modern complex 5G infrastructure is the key to success. The services include (but are not limited to):

- 3GPP 5G Security Assurance Specifications Security Validation (SCAS)
- Vulnerability assessment (VA)
- Enhanced security assessment and penetration testing (PT)

Assessment Process



Integrated Testing and Automation

Test Automation for 5G security

The move to 5G Standalone Access (SA) introduces the 5G Core (5GC), reducing the overheads of Non-Standalone Access (NSA) 4G interworking and benefiting from an optimized architecture designed for lower latency and enhanced Quality of Service (QoS). This adoption to new technology requires a new approach to validation. In the networking space, testing of previous generations of network equipment has focused on validation of well-defined physical network elements. With the new 5G Core and its cloud-native architecture, these monolithic network elements are superseded by individual CNFs that may be deployed in traditional centralized locations or closer to the network edge to enhance performance. Likewise, SD-WAN introduces multiple layers to the network with CNFs distributed across the end-to-end network from the core to customer premises.

This flexibility requires that individual CNFs are validated both in isolation and as part of an end-to-end cloud network. To enable rapid collaboration and development, CNF validation must be automated and seamlessly integrated into systems for tracking feature requests, creating new builds, and managing the status of testing and bug fixes. This combined approach is called Continuous Integration / Continuous Development (CI/CD) and is considered a best practice for accelerating cloud software releases.

Adopting CI/CD requires new capabilities:

- Implementing a CI/CD environment for multiple vendors with a constant stream of releases
- Integrating automated CNF isolation and end-to-end validation tests into the CI/CD environment
- Emulating the network to perform realistic validation including interoperability testing of vendor CNFs

Ensuring CI/CD expertise. Organizations struggle to build their own CI/CD environments. Too often, they don't have the internal expertise or toolsets to do this on their own, nor do they have the time or budget to acquire them. On top of this, 5G brings diverse new testing demands that span cloud environments, network functions and security. Building automated test suites that cover these diverse needs, especially security, is a challenge for many providers. On top of this, test suites must be automated and integrated with CI/CD test environments, so that as new CNFs become available, they are rapidly validated. A mature testing strategy should be designed to address this complex range of technology challenges and requirements. At times, this entails bringing in third-party expertise.

The importance in lab automation in any 5G testing strategy. To achieve maximum efficiency, testing automation capabilities must be supported by workflows in a next-generation test lab. This entails cloudification, unification of and centralization of physical, virtual and hybrid lab environments. Most companies operate multiple labs in geographically dispersed areas. In scenarios such as these, a partner with advanced lab automation expertise and technology capabilities can help eliminate outmoded internal and external siloed workflows, by consolidating multiple labs into a single shared, web-accessible resource which may be delivered in whole, or part, as a service.


Key Security KPIs for 5G


With the right testing strategy in place, a number of the KPIs to assure are in place in a testing campaign should include:

- Number of pass/fail compliance requirements per network element
- Average time between the test and the re-test, measuring how quickly vulnerabilities were remediated
- A difference between the number of pass/fail compliance results in test and the re-test, measuring the efficiency of remediation
- How often the same issue appears in the next tests – Rate of Defect Recurrence
- The length of time from when the issue is identified (e.g., in test 1) and when it is closed (e.g., in test 3) – defect remediation window (DRW)
- Number of issues per category, e.g., authentication, authorization, transport security, encryption, misconfiguration, logging, user management, system hardening, unpatched system, caused by lack of secure coding best practice, etc.

5G Security Case Study

Different organizations have a range of security challenges and must address them according to the specifics of their 5G architecture. Having a real-world example of one organization's addressing their challenge provides insight into the process of resolution. In this case study, Spirent SecurityLabs provided a solution that addressed a number of concerns.

 **CHALLENGE:** North American Tier 1 carrier was struggling to establish comprehensive 5GC security testing across multi-vendor 5G Core environment. The carrier needed help evaluating an in-house vs. a third-party PKI platform and PKI implementation for 5GC transport security.

 **SOLUTION:** Spirent SecurityLabs developed detailed test plans against the carrier's enhanced 3GPP SCAS security requirements.

- They conducted security validation against the test plan and automated test cases to ensure compliance and repeatability.
- The test plan for PKI/NFVi/CNF/VNF helped the carrier validate 100s of security requirements across the entire 5G Core infrastructure. Spirent conducted 100+ automated tests over 12 different NFs.
- Spirent helped evaluate the carrier's in-house PKI platform vs. the third-party PKI platform as a service for 5GC transport security.

 **IMPACT:** Spirent provided 5G Security Testing for the carrier, aligned with 3GPP standards and security best practices for hardening of their environment.

- Spirent SecurityLabs identified over 75 security gaps in areas such as authentication, authorization, encryption, system hardening. These issues would have resulted in unauthorized access to restricted resources, insecure transmission of sensitive data, services exposed to untrusted segments and unauthenticated access to NF functionality.
- Spirent worked with the carrier to triage these issues, so the identified gaps were addressed quickly.
- Spirent provided automation capabilities to proactively monitor and alert on an ongoing basis to identify any future security issues.

Recommendations for a sound 5G security strategy

As a general guideline, organizations working to optimize the cybersecurity of their 5G networks, should ensure adoption of the following actions:

- Use and appropriate configuration of the security functions specified by 3GPP
- Implement additional solutions available on the market that improve the security of networks offering:
 - A continuous security audit and monitoring of the security configurations and security policies
 - A multi-vendor system that provides single-sign-on with privileged identity management, user-behavior analytics, and compliance-logging capabilities
 - Automated holistic security orchestration and management combined with automated, intelligent security controls

Conclusions and Takeaways

Understand the vulnerabilities and severity of risks in 5G cybersecurity. These cover hardware, firmware, software; Signaling and Control Plane protocols; containers and Kubernetes; PKI and NF; operations, administration, and management.

Adopt a proactive 5G security testing strategy. Building security from the beginning, rather than bolt it on later is key.

Align with 3GPP Security Assurance Specifications (SCAS). The core 3GPP standards should be incorporated into any 5G testing strategy.

Account for PKI security implementation. Having a test plan that incorporates PKI with NFVi/CNF/VNF security requirements, across the entire 5G Core infrastructure, is critical for achieving holistic security.

Incorporate next-gen test automation. Utilize CI/CD environments for 5G's diverse new testing demands that span cloud environments, network functions and security, and build automated test suites that cover these diverse needs, especially security.

Utilize key security KPIs for 5G. This includes the number of pass/fail compliance per test, as well as the DRW – the length of time from when the issue is identified and when it is closed.

Consider an expert testing partner. Organizations struggle building automated test suites that cover 5G's diverse requirements, where effective testing must also account for test lab automation which entails cloudification, unification of and centralization of physical, virtual and hybrid lab environments often in geographically dispersed areas to eliminate outmoded internal and external siloed workflows.

To learn more about Spirent's Managed Solutions and SecurityLabs, go to:
<https://www.spirent.com/products/securitylabs-cybersecurity-services>

About Spirent

Spirent Communications (LSE: SPT) is a global leader with deep expertise and decades of experience in testing, assurance, analytics and security, serving developers, service providers, and enterprise networks. We help bring clarity to increasingly complex technological and business challenges. Spirent's customers have made a promise to their customers to deliver superior performance. Spirent assures that those promises are fulfilled.

For more information visit:
www.spirent.com

Americas 1-800-SPIRENT

+1-800-774-7368 | sales@spirent.com

Europe and the Middle East

+44 (0) 1293 767979 | emeainfo@spirent.com

Asia and the Pacific

+86-10-8518-2539 | salesasia@spirent.com