Matrix-Shell

CASE STUDY

Critical Security Gaps in 5G SBA APIs

How Matrix Shell Helped a Telecom Operator Identify High-Risk Exposure Inside Their 5G Core Network

Executive Overview

During a targeted security assessment of a major 5G Core deployment, critical structural vulnerabilities were identified in the Service Based Architecture (SBA). The absence of standard API security controls specifically OAuth2.0 and mutual TLS (mTLS) has led to the unauthorized exposure of the Network Repository Function (NRF) and Service Communication Proxy (SCP).

This exposure allows any entity within the network segment to enumerate, register, and manipulate Network Functions, breaking the fundamental zero-trust requirements of modern 3GPP standards.

Challenge

Modern 5G networks rely heavily on APIs for communication between core network functions.

These APIs are designed to work only between trusted systems. But during testing, Matrix Shell discovered that several critical security controls were either missing or not properly enforced.

The biggest concerns included:

- NRF APIs accessible without authentication
- No OAuth2.0 token validation
- Missing mutual TLS (mTLS) verification
- Internal SBA traffic trusted automatically
- Exposure of internal network topology and node information

In simple terms, the network trusted requests that should never have been trusted automatically.

This meant an attacker with access to the environment could potentially:

- Register rogue network functions
- Modify core network behavior
- Delete active network instances
- Query internal services
- Cause service disruption for subscribers

For a telecom operator, this creates both operational and security risks at a very high level.

Objectives

The assessment was designed to:

- Evaluate the security posture of the 5G SBA environment
- Validate OAuth2.0 and mTLS enforcement
- Test external and internal API exposure
- Identify trust boundary weaknesses
- Assess lateral movement possibilities between network functions
- Measure operational impact of potential exploitation
- Provide practical remediation guidance

Solution

Matrix Shell Technologies conducted a focused 5G core security assessment targeting both external exposure and internal SBA communications. The team simulated real-world attack scenarios to understand how far an attacker could interact with the environment.

The assessment included:

External API Security Validation

Matrix Shell tested externally reachable NRF interfaces to verify:

- Authentication enforcement
- API access control
- Network exposure
- Discovery protections

Internal SBA Communication Testing

The team also validated communication flows through the SCP layer to assess:

- Peer authentication
- Trust validation
- Internal API authorization
- Lateral access possibilities

Controlled Exploitation Simulation

To demonstrate real business impact safely, Matrix Shell validated several high-risk scenarios, including:

- Rogue NF registration
- Network function modification
- Unauthorized discovery requests
- Internal API querying
- Service disruption simulations

Testing Process

The engagement followed a structured assessment approach to ensure minimal operational impact while achieving deep visibility into the environment.

Phase 1

Environment Reconnaissance

- Identified reachable SBA components
- Evaluated exposed interfaces
- Mapped communication flows

Phase 2

Authentication & Trust Validation

- Tested OAuth2.0 enforcement
- Verified mTLS implementation
- Checked peer validation mechanisms

Phase 3

Controlled Security Testing

- Unauthorized API requests
- Rogue NF onboarding
- Internal service interactions
- Network function manipulation

Phase 4

Risk Analysis & Reporting

- Exposure severity
- Operational impact
- Attack paths
- Root causes
- Remediation priorities

Results & Impact

The assessment uncovered multiple critical trust and authentication gaps inside the 5G core environment.

Key Findings

Critical Exposure Identified

- NRF APIs accepted unauthenticated requests
- Internal SBA communication lacked proper trust validation
- OAuth2.0 enforcement was incomplete
- mTLS certificate verification was missing

Operational Risks Demonstrated

Matrix Shell successfully validated the ability to:

- Register unauthorized network functions
- Modify active NF states
- Delete active NF instances
- Query internal SBA services
- Expose internal topology and infrastructure details

Business Impact

The operator gained immediate visibility into risks that could potentially lead to:

- Subscriber service disruption
- Unauthorized signaling activity
- Core network instability
- Increased attack surface exposure
- Internal lateral movement opportunities

Security Improvements Enabled

Following the assessment, the operator received a prioritized remediation roadmap focused on:

- Restricting NRF exposure
- Enabling mTLS enforcement
- Implementing OAuth2.0 validation
- Strengthening SBA trust boundaries
- Adopting a zero-trust communication model

Conclusion

5G networks depend heavily on trusted communication between core services. This assessment showed that network segmentation alone is no longer enough to secure modern telecom infrastructure. Strong authentication, verified trust, and application-level security controls are now essential.

By identifying these gaps early, Matrix Shell Technologies helped the operator strengthen their 5G security posture before the issues could become operational threats.The result was improved visibility, stronger trust enforcement, and a clearer path toward secure and scalable 5G core operations.