Matrix-Shell

CASE STUDY

Strengthening Mobile Network Security Across the Radio Access Network

How Matrix Shell Helped a Telecom Operator Secure Its RAN Against Fraud and Unauthorized Access

Executive Overview

The Radio Access Network (RAN) is the first point of connection between mobile devices and a telecom network. If security controls at this layer are weak, attackers may gain unauthorized access, misuse subscriber services, or expose critical network infrastructure.

A telecom operator partnered with Matrix Shell to evaluate the security of its 2G, 3G, 4G, and 5G Radio Access Network.

The assessment uncovered several high-risk weaknesses related to subscriber authentication, device identity validation, and network exposure. By addressing these issues, the operator strengthened its security posture and reduced the risk of fraud and infrastructure attacks.

Challenge

The operator wanted to ensure that only legitimate subscribers and trusted devices could access its mobile network. As mobile networks evolve, weaknesses in authentication or device validation can allow attackers to impersonate subscribers, bypass security controls, or gain visibility into internal infrastructure.

The operator needed to verify whether its RAN was protected against common attack techniques that could impact both customers and network operations.

Potential risks included:

- Subscriber identity impersonation
- Device identity spoofing
- Unauthorized network access
- Exposure of internal infrastructure
- Increased fraud and operational risk

Objectives

The assessment was designed to:

- Evaluate the security of the Radio Access Network
- Validate subscriber authentication mechanisms
- Assess device identity verification
- Identify unnecessary network exposure
- Strengthen protection against unauthorized access and fraud

Solution

Matrix Shell conducted a comprehensive RAN Security Assessment across the operator's mobile network.

The assessment focused on three critical attack scenarios:

Subscriber Identity Impersonation

Validated whether subscriber identities could be misused to access network services.

Fake Device Registration

Tested whether the network properly verified device identities before granting access.

Network Infrastructure Exposure

Assessed whether internal systems and services were unintentionally exposed through mobile data connectivity.

The assessment combined controlled penetration testing with detailed security analysis to identify practical risks affecting day-to-day network operations.

Testing Process

Phase 1

Information Gathering

- Reviewed the mobile network architecture
- Identified authentication mechanisms
- Collected information about network services and access points

Phase 2

Network Discovery

- Mapped accessible network components
- Identified exposed services
- Evaluated subscriber connectivity paths

Phase 3

Security Testing

- Performed controlled penetration testing
- Tested authentication and identity validation
- Assessed infrastructure exposure
- Collected technical evidence for validation

Phase 4

Analysis & Reporting

- Evaluated identified security gaps
- Assessed operational and business impact
- Prioritized remediation activities
- Delivered practical security recommendations

Results & Impact

Subscriber Identity Impersonation Risk Identified

The assessment demonstrated that subscriber identities could potentially be misused to place calls and send messages under another user's account.

Business Impact

- Unauthorized use of subscriber services
- Increased fraud risk
- Financial losses
- Reduced customer trust

Device Identity Validation Weakness

Testing showed that the network accepted modified or invalid device identities without sufficient verification.

Business Impact

- Difficulty identifying unauthorized devices
- Increased opportunity for fraudulent activity
- Reduced visibility into connected devices
- Higher operational risk

Internal Network Exposure

The assessment identified internal IP addresses and network services that were accessible through mobile data connections.

Business Impact

- Larger attack surface
- Increased risk of infrastructure compromise
- Potential exploitation of exposed services
- Greater operational and security risk

Overall Outcome

Following the assessment, the operator achieved:

- Better visibility into RAN security risks
- Stronger subscriber authentication
- Improved device validation
- Reduced exposure of internal infrastructure
- Enhanced protection against fraud and unauthorized access

Conclusion

The Radio Access Network is the foundation of every mobile service. Protecting it is essential for maintaining subscriber trust and ensuring secure network operations. Through a structured RAN Security Assessment, Matrix Shell identified critical weaknesses that could impact authentication, device validation, and infrastructure security.

By strengthening security controls and reducing unnecessary network exposure, the operator significantly improved the resilience of its mobile network against evolving threats.

Matrix Shell continues to help telecom operators build secure, resilient Radio Access Networks that protect both subscribers and critical infrastructure.