Matrix-Shell

CASE STUDY

Strengthening SS7 Security Across a Mobile Network

How Matrix Shell Helped a Telecom Operator Reduce Exposure to Signaling Based Attacks

Executive Overview

SS7 remains a critical protocol for voice calls, SMS delivery, roaming, and subscriber management in mobile networks. However, many SS7 networks were built on trust-based communication models that no longer align with today's threat landscape.

A leading telecom operator engaged Matrix Shell to assess the security of its SS7 signaling environment and identify potential risks that could impact subscriber privacy and service integrity.

The assessment uncovered several high-risk signaling weaknesses that could enable call interception, SMS interception, and subscriber location tracking. By identifying these gaps and recommending stronger signaling controls, Matrix Shell helped the operator improve the security posture of its mobile network.

Challenge

The operator wanted to understand a simple but critical question:

Can unauthorized signaling messages manipulate subscriber services or expose sensitive information?

Because SS7 was originally designed for trusted telecom environments, weak message validation can create opportunities for attackers to:

- Intercept voice calls
- Redirect SMS messages
- Track subscriber locations
- Manipulate subscriber services
- Commit telecom fraud

If left unaddressed, these risks could impact customer trust, regulatory compliance, and overall network security.

Objectives

The assessment was designed to:

- Evaluate the security of the SS7 signaling network
- Identify weaknesses in signaling message validation
- Assess exposure to known SS7 attack techniques
- Verify effectiveness of existing security controls
- Provide actionable recommendations for risk reduction

Solution

Matrix Shell conducted a comprehensive SS7 Security Assessment focused on validating how the network handled signaling requests from external sources.

The assessment focused on three critical attack scenarios:

Voice Call Interception

Validated whether signaling messages could manipulate subscriber service profiles and alter call routing behavior.

SMS Interception

Tested whether signaling procedures could redirect SMS traffic and impact message delivery.

Subscriber Location Tracking

Assessed whether location information could be obtained without authorization.

Rather than focusing on theoretical risks, the assessment validated real-world attack paths and measured the effectiveness of existing security controls.

Testing Process

Phase 1

Information Gathering

- Reviewed signaling architecture
- Identified network entry points
- Mapped signaling routes and interconnects
- Collected key network information required for testing

Phase 2

Network Discovery

- Identified accessible signaling components
- Mapped critical network elements
- Evaluated message routing paths

Phase 3

Security Testing

- Performed controlled SS7 penetration testing
- Simulated real-world attack scenarios
- Validated signaling message filtering and security controls
- Captured evidence for analysis

Phase 4

Analysis & Reporting

- Assessed identified risks
- Evaluated business impact
- Prioritized findings
- Delivered remediation recommendations

Results & Impact

Voice Call Interception Risk Identified

The assessment demonstrated that signaling messages could manipulate call forwarding behavior, creating opportunities for unauthorized call interception.

Business Impact

- Increased privacy risk
- Potential service misuse
- Higher fraud exposure
- Reputational concerns

SMS Interception Risk Identified

Testing showed that location update procedures could influence SMS routing behavior and potentially redirect messages.

Business Impact

- Exposure of OTP messages
- Account takeover risks
- Financial fraud concerns
- Reduced customer trust

Subscriber Location Tracking Exposure

Location-related signaling requests revealed opportunities for unauthorized subscriber tracking.

Business Impact

- Privacy concerns
- Regulatory risk
- Exposure of sensitive subscriber information
- Potential misuse of location data

Overall Outcome

Following the assessment, the operator gained:

- Improved visibility into SS7 security risks
- Better understanding of signaling attack exposure
- Clear remediation roadmap
- Stronger protection for subscriber services
- Enhanced readiness against signaling-based threats

Conclusion

Modern telecom networks still rely heavily on SS7, making signaling security a critical part of protecting subscribers and network operations.Through a structured security assessment, Matrix Shell identified key weaknesses that could impact voice services, messaging, and subscriber privacy.

By implementing stronger message validation, signaling filtering, and continuous monitoring, the operator significantly improved its resilience against SS7-based attacks and strengthened the overall security of its mobile network.

Matrix Shell continues to help telecom operators identify hidden signaling risks and build more secure, resilient networks.