Matrix-Shell

CASE STUDY

Securing Diameter Signaling Against Roaming Threats

How Matrix Shell Helped a Telecom Operator Strengthen Diameter Security and Protect Critical Roaming Services

Executive Overview

Diameter is a core signaling protocol used in 4G and LTE networks to manage subscriber authentication, mobility, and roaming services. Because it connects multiple telecom networks, weak signaling controls can expose operators to fraud, service disruption, and subscriber data breaches.

A telecom operator partnered with Matrix Shell to evaluate the security of its Diameter signaling environment and identify weaknesses that could impact roaming operations.

The assessment revealed critical gaps in message validation, subscriber protection, and signaling controls. By addressing these issues, the operator strengthened its roaming security and reduced the risk of signaling-based attacks.

Challenge

Diameter signaling is responsible for authenticating subscribers and managing roaming between telecom networks. If signaling messages are not properly validated, attackers may manipulate subscriber information, intercept services, or disrupt network operations.

The operator wanted to verify whether its Diameter infrastructure could effectively defend against common roaming threats while maintaining secure and reliable services.

Potential risks included:

- Exposure of subscriber authentication data
- SMS interception
- Service disruption
- Unauthorized signaling requests
- Increased fraud and roaming abuse

Objectives

The assessment was designed to:

- Evaluate the security of the Diameter signaling network
- Validate message filtering and authentication controls
- Assess protection against roaming attacks
- Identify signaling security gaps
- Strengthen subscriber and network security

Solution

Matrix Shell performed a comprehensive Diameter Security Assessment focused on the operator's roaming and signaling infrastructure.

The assessment focused on three high-risk attack scenarios:

Authentication Information Exposure

Validated whether authentication-related signaling messages were properly protected against unauthorized requests.

SMS Interception

Tested whether subscriber location update messages could be manipulated to redirect SMS traffic.

Service Disruption

Assessed whether signaling messages could be abused to interrupt subscriber services or disconnect active sessions.

The assessment combined controlled penetration testing with detailed signaling analysis to validate the effectiveness of existing security controls.

Testing Process

Phase 1

Information Gathering

- Reviewed Diameter architecture and roaming environment
- Identified signaling peers and routing paths
- Collected configuration details required for testing

Phase 2

Network Discovery

- Identified reachable Diameter endpoints
- Validated supported signaling applications
- Evaluated roaming connectivity and routing behavior

Phase 3

Security Testing

- Tested Diameter signaling controls
- Evaluated message validation mechanisms
- Assessed protection against subscriber and service abuse
- Captured evidence to validate findings

Phase 4

Analysis & Reporting

- Analyzed identified security gaps
- Assessed operational and business impact
- Prioritized remediation actions
- Delivered practical security recommendations

Results & Impact

Authentication Information Exposure

The assessment identified weaknesses that could allow unauthorized requests to retrieve subscriber authentication information.

Business Impact

- Exposure of sensitive authentication data
- Increased risk of subscriber impersonation
- Higher fraud potential
- Reduced confidence in roaming security

SMS Interception Risk

Testing showed that subscriber location update procedures could potentially be manipulated, allowing SMS messages to be redirected.

Business Impact

- Unauthorized SMS interception
- Increased account takeover risk
- Subscriber privacy concerns
- Greater exposure to fraud

Service Disruption

The assessment found that certain signaling messages could be used to interrupt subscriber connectivity if proper validation was not enforced.

Business Impact

- Temporary service disruption
- Reduced service availability
- Poor customer experience
- Increased operational risk

Overall Outcome

Following the assessment, the operator achieved:

- Improved visibility into Diameter signaling risks
- Stronger roaming security controls
- Better protection of subscriber information
- Reduced fraud exposure
- Enhanced resilience against signaling attacks

Conclusion

Diameter signaling is a critical part of modern LTE and roaming services, making strong security controls essential for protecting subscribers and maintaining service reliability. Through a structured Diameter Security Assessment, Matrix Shell identified key weaknesses affecting authentication, roaming security, and service availability.

By strengthening message validation, improving signaling controls, and implementing continuous monitoring, the operator significantly enhanced the security and resilience of its Diameter infrastructure.

Matrix Shell continues to help telecom operators secure critical signaling networks with practical, standards-based security assessments.