Matrix-Shell

CASE STUDY

Securing Roaming Services Against GTP Signaling Threats

How Matrix Shell Helped a Telecom Operator Strengthen GTP Security and Reduce Fraud Risks

Executive Overview

GTP (GPRS Tunnelling Protocol) plays a critical role in mobile data services and roaming connectivity. It helps establish and manage subscriber data sessions across telecom networks worldwide.

A telecom operator approached Matrix Shell to evaluate the security of its GTP signaling environment and identify any weaknesses that could be exploited by external roaming networks.

The assessment uncovered several gaps in subscriber validation and session handling that could lead to fraud, unauthorized data usage, and revenue leakage. By identifying these risks and providing targeted recommendations, Matrix Shell helped the operator strengthen roaming security and improve trust in its signaling infrastructure.

Challenge

Roaming services depend on trusted communication between telecom operators. However, if incoming GTP requests are not properly validated, attackers may be able to create unauthorized data sessions or misuse subscriber identities.

The operator wanted to determine whether its existing controls could effectively prevent:

- Unauthorized data usage
- Subscriber identity abuse
- Roaming fraud
- Revenue leakage
- Signaling-based service disruption

Without proper controls, these risks could impact both network security and business operations.

Objectives

The assessment was designed to:

- Evaluate security controls within the GTP environment
- Validate subscriber verification mechanisms
- Identify opportunities for roaming fraud
- Assess exposure to unauthorized session creation
- Strengthen overall signaling security posture

Solution

Matrix Shell conducted a comprehensive GTP Security Assessment focused on how the network processed and validated signaling requests from roaming environments.

The assessment focused on three high-risk attack scenarios:

Unauthorized Data Usage

Validated whether data sessions could be established using another subscriber's identity.

Subscriber Enumeration

Tested whether attackers could discover valid subscriber identities through repeated signaling requests.

Invalid Session Creation

Assessed whether the network would accept session requests for non-existing subscribers.

The goal was to verify whether existing security controls could effectively prevent abuse of roaming services.

Testing Process

Phase 1

Information Gathering

- Reviewed roaming architecture and GTP infrastructure
- Identified key network components
- Collected subscriber and connectivity information required for testing

Phase 2

Network Discovery

- Validated GTP connectivity paths
- Assessed routing behavior
- Identified supported signaling procedures

Phase 3

Security Testing

- Performed controlled GTP penetration testing
- Evaluated subscriber validation mechanisms
- Tested session establishment procedures
- Verified protection against signaling abuse

Phase 4

Analysis & Reporting

- Analyzed findings and security gaps
- Assessed technical and business impact
- Prioritized risks
- Delivered remediation recommendations

Results & Impact

Unauthorized Data Session Creation Identified

Testing showed that data sessions could be established without sufficiently validating whether the subscriber was legitimately roaming on the requesting network.

Business Impact

- Unauthorized data consumption
- Fraudulent service usage
- Subscriber account abuse
- Increased revenue leakage risk

Subscriber Enumeration Exposure

The assessment found that multiple subscriber identities could be tested through signaling requests without adequate rate limiting.

Business Impact

- Exposure of valid subscriber information
- Increased targeting opportunities for attackers
- Additional load on signaling infrastructure
- Elevated security risk

Invalid Subscriber Session Requests Accepted

Testing demonstrated that session requests containing invalid subscriber information were not always properly rejected.

Business Impact

- Unauthorized session creation attempts
- Unbillable network traffic
- Increased fraud exposure
- Misuse of roaming infrastructure

Overall Outcome

Following the assessment, the operator achieved:

- Better visibility into roaming security risks
- Stronger subscriber validation controls
- Reduced fraud exposure
- Improved protection against signaling abuse
- Enhanced confidence in roaming operations

Conclusion

As roaming ecosystems continue to expand, strong GTP security controls are essential for protecting both subscribers and operator revenue. Through a structured GTP Security Assessment, Matrix Shell identified critical weaknesses that could lead to unauthorized usage, fraud, and revenue loss.

By improving validation processes, enforcing stronger filtering controls, and continuously monitoring signaling traffic, the operator significantly enhanced the security and reliability of its roaming environment.

Matrix Shell continues to help telecom operators secure critical signaling infrastructure and stay ahead of evolving telecom threats.