Matrix-Shell

CASE STUDY

Securing VoLTE Services Against IMS Security Risks

How Matrix Shell Helped a Telecom Operator Strengthen VoLTE Security and Protect IMS Infrastructure

Executive Overview

Voice over LTE (VoLTE) has transformed mobile communication by delivering voice calls over high-speed IP networks. While it improves call quality and user experience, it also introduces new security challenges if IMS (IP Multimedia Subsystem) controls are not properly enforced.

A telecom operator partnered with Matrix Shell to assess the security of its VoLTE environment and identify weaknesses that could impact subscriber privacy, network integrity, and revenue.

The assessment uncovered several critical gaps in traffic policies, routing controls, and information protection. By addressing these issues, the operator strengthened its IMS security and reduced the risk of service abuse and infrastructure exposure.

Challenge

VoLTE relies on IMS infrastructure to manage voice services over IP networks. If traffic policies or routing rules are not properly configured, subscribers may communicate in unintended ways, internal systems may become exposed, and sensitive information could be leaked.

The operator wanted to verify whether its VoLTE environment was adequately protected against common security risks before they could impact customers or business operations.

Potential risks included:

- Unauthorized subscriber communication
- Revenue loss from unbilled services
- Exposure of internal network infrastructure
- Leakage of subscriber and device information
- Increased attack surface

Objectives

The assessment was designed to:

- Evaluate the security of the VoLTE environment
- Validate IMS traffic policies
- Assess network segmentation and routing controls
- Identify information disclosure risks
- Strengthen overall IMS security

Solution

Matrix Shell conducted a comprehensive VoLTE Security Assessment focused on the operator's IMS infrastructure and signaling environment.

The assessment focused on three critical attack scenarios:

Unauthorized Subscriber Communication

Validated whether traffic policies prevented direct communication between subscribers outside approved IMS services.

Internal Network Exposure

Tested whether VoLTE data paths exposed internal IP addresses or critical network services.

Information Disclosure

Assessed whether sensitive subscriber or device information was visible within IMS signaling traffic.

The assessment combined controlled penetration testing with detailed traffic analysis to validate how effectively the network enforced its security controls.

Testing Process

Phase 1

Information Gathering

- Reviewed IMS architecture
- Identified signaling components and connectivity paths
- Collected network configuration details required for testing

Phase 2

Network Discovery

- Validated IMS connectivity
- Observed traffic flow between subscribers and IMS components
- Evaluated routing behavior across VoLTE services

Phase 3

Security Testing

- Tested IMS traffic policies
- Evaluated routing and bearer restrictions
- Assessed information exposure
- Captured evidence for detailed analysis

Phase 4

Analysis & Reporting

- Reviewed assessment findings
- Evaluated business impact
- Prioritized security improvements
- Delivered actionable recommendations

Results & Impact

Weak IMS Traffic Policies Identified

The assessment showed that subscribers could communicate directly over the IMS environment without appropriate restrictions, creating opportunities for unauthorized data exchange.

Business Impact

- Unauthorized subscriber communication
- Unbilled data usage
- Revenue leakage
- Reduced control over IMS services

Internal Network Exposure

Testing identified internal IP addresses and network services that were accessible through VoLTE data routes.

Business Impact

- Increased infrastructure exposure
- Larger attack surface
- Higher risk of unauthorized access
- Potential impact on network stability

Subscriber Information Disclosure

The assessment found that subscriber and device-related information was visible within IMS signaling messages.

Business Impact

- Exposure of sensitive subscriber information
- Increased privacy risks
- Potential misuse of device information
- Regulatory compliance concerns

Overall Outcome

Following the assessment, the operator achieved:

- Improved visibility into IMS security risks
- Stronger VoLTE traffic controls
- Better protection of subscriber information
- Reduced infrastructure exposure
- Enhanced security across VoLTE services

Conclusion

VoLTE has become a core service for modern mobile networks, making IMS security more important than ever. Through a structured VoLTE Security Assessment, Matrix Shell identified key weaknesses affecting traffic control, routing policies, and subscriber data protection.

By strengthening IMS policies, improving network segmentation, and enhancing signaling security, the operator significantly reduced its exposure to service abuse, privacy risks, and infrastructure attacks.

Matrix Shell continues to help telecom operators secure next-generation voice services with practical, standards-driven security assessments.