



GSMK Network Security

Interconnect Security Assessment

Core Network Security

Interconnect Security Assessment

Protect your Core Network's Achilles Heel

Today's increasing core network complexity requires strict policies and new tools to prevent fraud, hijacking or service disruption and espionage.

The once secure 'walled' world of trusted operator members is in danger of now facing an onslaught of fraud and hacking. Countless threats in the SS7 Diameter and GRX topology can lead to serious consequences for operators and customers.

As a renowned industry leader in the field of strong encryption (GSMK CryptoPhone®) and core network security, GSMK has over 12 years of proven, extensive experience in mobile telecommunications security.

GSMK developed a range of products and services to enable comprehensive detection of core network anomalies and reliable protection of SS7, Diameter and GRX interconnections.

Our penetration tests are performed by experienced senior experts within our high-security facilities in the center of Berlin. We are a GSMA associate member with access to SS7, Diameter and GRX on a global scale.

Operational Risk Management

For every network operator, MVNO, hub operator, and signalling service provider operational risk management is essential to avoid severe legal consequences and financial impact.

Insufficient protection of critical infrastructure is the number one risk within the industry. Even if a firewall has already been installed, it can initially be circumvented in most cases.

Confidence Level

With our core network penetration test we can offer the most comprehensive interconnect vulnerability assessment in the industry.

The test suites executed during the assessment are custom-tailored to the respective operator's network topology, based on our extensive experience with global tier 1 and tier 2 operators.

We will provide a comprehensive test report with detailed recommendations on how to improve your interconnect security. Discounted retests are available to assess the effectiveness of new security measures.

Key Features

- Carrier-grade penetration testing
- Most extensive SS7, Diameter and GTP interconnect vulnerability assessment in the industry
- Custom-tailored test suites (manual and automated tests)
- Tests include, but are not limited to GSMA FS.11, FS.19 and FS.20 recommendations
- Required for MNO risk management
- GSMA associate member
- Comprehensive final report with found vulnerabilities and detailed recommendations
- Re-testing for maximum safety
- Flexible pricing models according to your needs
- Optional on-site workshop to work out best ways to implement security mitigations

Threats

The tremendous growth of independent entities with SS7, Diameter and GRX access, including MVNOs and certain micro-operators, has made it easier for malicious actors to purposefully exploit the protocols' weaknesses.

Investigations commissioned by major network operators have shown a rapid increase in interconnect-based attacks on a global scale.

Basic filtering of messages to counteract intruders is neither sufficient for protecting operators from the financial impacts nor can it guarantee the network's integrity in terms of data security and availability.

The increasing number of M2M or IoT applications with critical data connections relying on mobile infrastructure will be the target of the future.

Below we list some typical attacks and vulnerability tests performed. All tests are including but not limited to the GSMA recommendations (e.g. FS.11 / FS.19 / FS.20).

► **Illegal interception of calls, messages and data theft**

- intercept phone calls made or received by subscriber (man-in-the-middle)
- intercept SMS messages sent or received by subscriber (including two-factor authentication messages and mTANs sent by banks or online services)
- intercept and re-route Internet and other data connections

► **Billing fraud**

- transfer pre-paid balance to other subscribers
- make calls to premium rate numbers at the expense of subscriber
- make calls to premium rate numbers at the expense of operator
- setup data sessions at the expense and in the name of other subscribers
- disable billing of pre-paid subscribers (all calls and SMS free for subscriber)
- buy premium content in the name and at the expense of subscriber
- send SMS messages in the name and at the expense of subscriber
- remove pre-paid credit of subscriber with simulated calls

► **Subscriber privacy violations**

- track subscribers (worldwide, street level precision in cities, reading out geo coordinates directly)
- monitor when subscriber uses phone (SMS, call)
- retrieve authentication vectors for subscriber (enables decryption of over-the-air-traffic)
- find out phone numbers of subscriber
- show all caller IDs for incoming calls, even if they were suppressed by calling party
- compile detailed logs of all calls made or SMS sent or received by subscriber
- identify phone model in use by subscriber (via IMEI)
- read out call status

► **Denial of service (DoS)**

- denial of service against operator network elements via specially crafted messages (only tested upon request by operator)
- disable calls, SMS and data for subscriber
- denial of service against all subscriber's using a network element (only tested upon request by operator)

► **Manipulate network settings**

- simulate subscriber roaming in foreign network
- Subscriber profile modifications in HLR/HSS
- override network settings made by subscriber (e.g. call forwarding, call barring, CLIP/CLIR, ...)
- enable functions normally blocked by operator (e.g. calls or call forwarding to foreign / premium rate numbers)
- execute USSD codes on behalf of subscriber (e.g. SIM Toolkit functions, subscriber menus, transfer pre-paid credit, execute banking commands, modify subscriber contract, execute M2M functions)
- unauthorized use of APNs
- change outgoing caller ID to any number
- send official looking spam or phishing messages to subscriber

► **Further tests performed**

Bypassing existing security measures/firewall

- check if network accepts messages from spoofed/faked addresses (Global Titles)
- check if network elements accept messages with illegal formatting
- check if network elements accept unusual message combinations
- check if network accepts unusual addressing
- check for network services and interfaces which are accidentally exposed to the interconnect

Four real-world attacks that our penetration tests can help to prevent:



Stealing money from online banking accounts

Fraudsters oftentimes already retrieved credentials for the online banking account of their victim. But to actually transfer money, they need to access the SMS message with the 'second factor' (e.g. TAN, transaction number) being sent by the bank to their victim's mobile phone.

- the fraudster retrieves the victim's IMSI by sending SS7/Diameter requests to the Core network's HLR/HSS
- the fraudster uses the IMSI to simulate that the victim is currently roaming abroad in the fraudster's "fake" network
- the fraudster initiates a bank transfer from the victim's online banking account to his own account
- this triggers the TAN SMS message being sent by the bank to the victim's mobile phone number
- the bank's SMS provider asks the victim's MNO's HLR/HSS where to route the message
- the HLR/HSS answers with the address of the fraudster's "fake" network
- the SMS message is being sent to the fraudster's "fake" network instead of the victim's mobile phone
- the fraudster receives the SMS message, enters the TAN into the online banking and completes the theft of the victim's money, without ever touching the actual mobile phone

This happened to German bank customers because they were using a badly protected MNO.

With the same method for example Facebook, Twitter, Google, Microsoft and Amazon accounts as well as those of many other online services can be stolen.



Intercepting phone calls (man-in-the-middle attacks)

Corporate espionage or nation state actors - there are many reasons why shadowy entities want to listen to other people's phone conversations. The current core network protocols make it easy to intercept phone calls from half a world away without anybody noticing.

- the malicious actor retrieves the victim's IMSI by sending SS7/Diameter requests to the core network's HLR/HSS
- using the IMSI, the actor manipulates the subscriber profile in the VLR/MSC to make his "fake" network an authority on what should happen with the victim's phone calls
- the victim dials a phone number
- the VLR/MSC now asks the actor's "fake" network what should happen with the call
- the actor tells the VLR/MSC to re-route it to his own recording bridge
- when the call arrives at the recording bridge, the actor will connect it from there to the destination previously dialed by the victim
- the victim can now talk to the person he called, but the whole conversation is being recorded by the malicious actor

Among the victims of this kind of attack were Ukrainian subscribers whose calls were being intercepted by a neighbouring country.

It is reasonable to expect that this happens all the time on many networks without being noticed, as subscribers don't experience any service degradation.

The same techniques can be used for intercepting/re-routing SMS messages and also internet data connections.



Premium rate fraud with pre-paid contracts

Pre-paid contracts do not allow calls or SMS messages when the balance is depleted, and most of the time they don't allow calls to premium rate numbers at all. But fraudsters found a way to disable billing completely using the core network. This makes it possible for them to call their own premium rate lines and earn money while the MNO has to pay for the call.

- *the fraudster reads out the IMSI from the pre-paid SIM(s) he purchased*
- *using the IMSI, the fraudster manipulates the subscriber profile in the VLR/MSC to disable billing and lift any restriction on the type of calls that can be made*
- *the fraudster dials his own premium-rate number and the MSC completes the call even though there is no balance on the pre-paid SIM*
- *the fraudster earns money from the call and the MNO has to pay for it*

Various South American network operators were subject to fraud cases employing this technique.



Uncovering secrets by tracking executives' movements

By monitoring high-level employees' movements, fraudsters can gain insights into a corporation's future, still secret, plans. They never need to be in the vicinity of the people they monitor.

- *the fraudster sends an SS7/Diameter command to the MSC/MME which tells it to send the location of the victim to the fraudster's "fake" network periodically*
- *the MSC/MME sends the geo coordinates of the subscriber's current location to the address of fraudster's "fake" network*
- *it will repeat this indefinitely, at intervals set by the fraudster*

The fraudster can monitor the location of many people this way. This also goes completely unnoticed most of the time, but our analysis of network traffic shows that it is extremely common.

Steps to a secure Interconnect

- Kick-off meeting
- Exchange of legal documents (letter of indemnity)
- Agreement on testing schedule and tests to be performed
- Purchase order (PO)
- Exchange of technical data
- Testing stage (2 weeks per signaling type)
- Post processing stage (1 week)
- Presentation of findings or workshop (either remote or on site, 1 day)
- Infrastructure update on client side
- Retest (3 weeks max.)

Our Service Options


1. **Comprehensive custom-tailored Interconnect security assessment including a full report and presentation of findings via conference call or in person**
 - a) SS7 MAP/CAP
 - b) Diameter
 - c) SS7 MAP/CAP , Diameter and GRX
2. **Comprehensive assessment as described in 1., including one full retest after the implementation of new security measures**
 - a) SS7 MAP/CAP
 - b) Diameter
 - c) SS7 MAP/CAP , Diameter and GRX
3. **Comprehensive assessment as described in 1., including three further retests within a year, full reports and updates**
 - a) SS7 MAP/CAP
 - b) Diameter
 - c) SS7 MAP/CAP , Diameter and GRX
4. **Fuzzing services on site or remote for up to 3 network elements**
 - a) remote (via VPN)
 - b) on site (on site, min. 4 days)

Optional features

- all tests can be performed as black-box tests.
- fuzzing of network elements in operator or vendor lab, or off-site at GSMK's premises
- offline analysis of interconnect traffic

For further technical questions or your personal quote, please get in contact with your local distributor or call our network security team.

Notes



GSMK - Gesellschaft für Sichere Mobile Kommunikation mbH
Marienstrasse 11
10117 Berlin
Germany

Phone + 49-30-24 62 500-0
Telefax + 49-30-24 62 500-1
www.gsmk.de

This document is provided for information purposes only, and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document, and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

The product names and logos mentioned in this document are trademarks or registered trademarks of their respective owners. CryptoPhone ist a registered trademark of GSMK • © V1.8_12.2018.

This document includes GSMK Proprietary Information.



Regional Representative / Distributor