adaptivemobile™
SECURITY

AdaptiveMobile Signalling Penetration Testing

Product Overview

SS7 networks have been vulnerable since their inception, with the risk of SS7 based attacks on mobile networks recently gaining a lot of attention in the public media.

The SS7 network was created decades ago when the only parties connected to it were government owned telecom companies. There was never any protection or authentication built into the protocol, because it was simply not needed then. Several decades on, a typical mobile operator network "talks" to hundreds of other networks in dozens of countries, to facilitate international roaming, still without any protection or authentication. In addition, Diameter security standards are no better than that of SS7.

The GSM Association's (GSMA) Fraud and Security Group has recently categorized SS7 vulnerabilities in a document named FS.11. Mobile operators can obtain this from the GSMA's Fraud and Security Group.

AdaptiveMobile offers a range of penetration testing services to enable operators to understand the specific signalling security risks their networks face and so understand the most appropriate countermeasures to put in place to protect their subscribers and business.

Types of SS7 attacks caused by vulnerabilities in mobile networks

- **Denial of service attack:** a malicious attacker can bring down mobile services for a specific subscriber, a group of subscribers, random subscribers, or in some cases, for the entire network.
- **Geolocation:** a malicious attacker can locate the cellphone of a subscriber, knowing only their phone number, with an accuracy of a few meters.
- **Call interception:** a malicious attacker can intercept and record calls from a subscriber, without the subscriber or operator's knowledge.
- **Toll fraud:** a malicious attacker can purchase retail subscriptions from an operator, and make outbound toll calls without being charged for these calls. This can cause a significant loss to the operator within a short amount of time, when premium numbers are being targeted.
- **Wholesale SMS fraud:** a malicious attacker can use a mobile operator's network to terminate or relay large amounts of wholesale SMS messages. This practice can go on for years undetected. Good intentioned operators have deployed SMS firewalls, but some of the first generation firewalls can be bypassed by malicious attackers.
- **Information Harvesting:** a malicious attacker can get subscriber details such as IMSIs/MSISDNs, device type, who they forward calls to, account status, etc.

Additional abuses emerge continuously, imagined by more and more creative attackers.

Why Should Operators Act Now

- You have noticed your network is under threat, or your subscribers are complaining about privacy issues.
- You suspect your network is being impersonated/ abused at your brand's expense.
- You wish to assess your network's security status as part of your evolution to clamp down on signalling threats.
- You have limited time and resources to self-assess the overall security grading.

Signalling Penetration Testing Services Overview

AdaptiveMobile provide the following range of penetration testing services:

1. Exploratory or Rapid Penetration Testing
2. Full Penetration and Security Testing
3. Repeat Security Auditing
4. Training Workshops
5. Traffic analysis

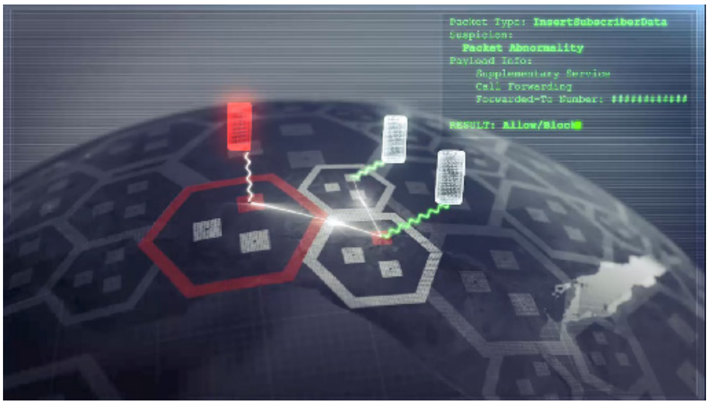

Figure 1: Visualization of real life example of SS7 based message interception

AdaptiveMobile Signalling Penetration Testing Services

1. Exploratory or Rapid Penetration Testing

What we do

- Measure your defences against the most popular 2G, 3G and 4G network interconnect attacks, using penetration tests with the attacker's mind set.
- Subscriber Location tracking, Information gathering and Service/Call manipulation attack types are in scope.

Value for you: A report including:

- What the penetration tests were along with their pre-prerequisites
- A summary report per simulated attack and security assessment/score
- Recommendations arising from the test

Next steps for you

The report and recommendations may lead to one of the following:

- Progress with the comprehensive full penetration test
- Progress to a repeat auditing to monitor severity and frequency of attacks

2. Full Penetration and Security Test

What we do

- Measure your defences against the full suite of 2G, 3G and 4G network interconnect attacks, using penetration tests with the attacker's mindset.
- All Subscriber Location tracking, Information gathering, Service/Call manipulation, Fraud, subscriber and network DoS attack types are in scope.

Value for you: A report including:

- What the penetration tests were along with their pre-prerequisites
- A detailed report per simulated attack and security assessment/score
- Detailed evidence gathered during the test execution
- Recommendations arising from the test

Next steps for you

The report and recommendations may lead to one of the following:

- Progress to a repeat auditing to monitor severity and frequency of attacks
- Implement counteracting measures in the network, e.g. Signalling Firewall

3. Repeat Security Auditing

What we do

- Automatically and at regular intervals, conduct the Full Penetration and Security Test
- All Subscriber Location tracking, Information gathering, Service/Call manipulation, Fraud, subscriber and network DoS attack types are in scope.

Value for you: A report including:

- What the penetration tests were along with their pre-prerequisites
- A detailed report per simulated attack and security assessment/score
- Detailed evidence gathered during the test execution
- Recommendations arising from the test

Next steps for you

The report and recommendations may lead to one of the following:

- Change the frequency of the repeat auditing
- Engage our training services to inform you and/or assess next steps
- Implement counteracting measures in the network, e.g. Signalling Firewall

4. Training/Workshop

What we do

- We provide an overview of mobile network security principles.
- In conjunction with the audience, we analyse and clarify any penetration test results and recommendations.

Value for you: A report including:

- Optimal awareness and knowledge to evolve signalling threat prevention.

Next steps for you

The above may lead to one of the following:

- Change the frequency of the repeat auditing
- Implement counteracting measures in the network, e.g. Signalling Firewall

5. Traffic Analysis

What we do

- We provide an analysis of customer traffic.
- In conjunction with the audience, we analyse and clarify any unwanted packets in a customer trace from your network.

Value for you: A report including:

- Awareness of what threats are coming in and out of your network.
- Also awareness of lost revenue via messages coming from non agreed paths.

Next steps for you

The above may lead to one of the following:

- Agree for an analysis to be completed on a trace from your network.
- Implement counteracting measures in the network, e.g. Signalling Firewall

Sophisticated Signalling Attacks

AdaptiveMobile's range of Signalling Penetration Testing Services can help you defend your network against some of the more sophisticated attacks currently being perpetrated against mobile subscribers.

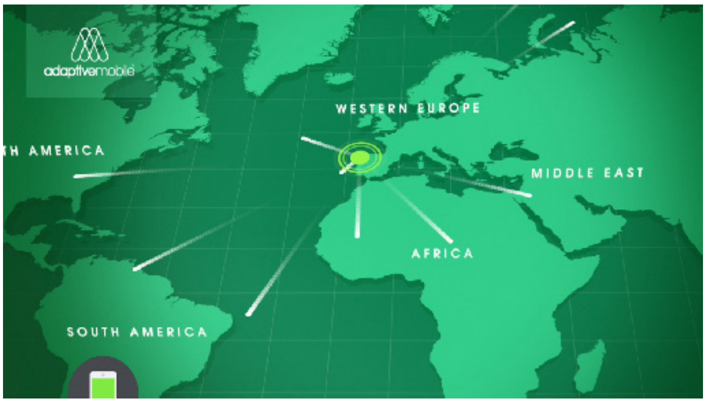

Figure 2: Visualization of real life example of SS7 based attack. Packet combinations and multiple origination points used to track one subscriber in 2 minutes and 20 second window

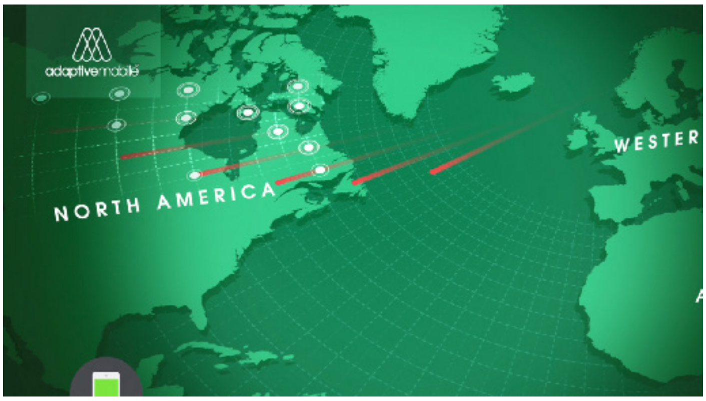

Figure 3: Visualization of real life example of SS7 based attack. Attacker performed scanning of an operator's entire switching infrastructure

Corporate Headquarters:
Ferry House, 48-52 Lower Mount Street, Dublin 2
Tel: +353 1 524 9000
Fax: +353 1 524 9001

Regional Sales Contact Numbers:
US, Canada, Latin America Sales: +1 972 377 0014
UK Sales: +44 207 049 0421
Middle East Sales: +97144 33 75 83
Africa Sales: +27 875502315
Asia Sales: +65 31 58 12 83
European Sales: +353 1 524 9000

Regional Support Contact Numbers:
UK: +44 208 114 9589
Ireland: +353 1 514 3945
France: +33 975 180 171
India: 000-800-100-7129
US, Canada: +1 877 267 0444
Latin America: +52 5584211344

www.adaptivemobile.com

For discussion of typical use cases, overview of AdaptiveMobile's existing deployments or a full walkthrough of our customer experience, contact your local office: **www.adaptivemobile.com/contact-us**

About AdaptiveMobile

AdaptiveMobile is the world leader in mobile network security protecting over one billion subscribers worldwide and the only mobile security company offering products designed to protect all services on both fixed and mobile networks through in-network and cloud solutions. With deep expertise and a unique focus on network-to-handset security, AdaptiveMobile's award winning security solutions provide its customers with advanced threat detection and actionable intelligence, combined with the most comprehensive mobile security products available on the market today. AdaptiveMobile's sophisticated, revenue-generating security-as-a-service portfolio empowers consumers and enterprises alike to take greater control of their own security. AdaptiveMobile was founded in 2003 and boasts some of the world's largest mobile operators as customers and the leading security and telecom equipment vendors as partners. The company is headquartered in Dublin with offices in the North America, Europe, South Africa, Middle East and Asia Pacific.

MAAWG MESSAGING ANTI-ABUSE WORKING GROUP GSMA GSM World oma Open Mobile Alliance IWF Member DO the right thing