FORWARD DEFENSE

Telco Security Testing

ACTIVE TELCO CYBER DEFENSE

SS7 Penetration Test SS7 Forensics SS7 Intelligence Reports Diameter Penetration Test Telco Cyber Security Training

Active Telco Cyber Defense

Forward Defense conducts off-premises Signaling System No. 7 (SS7) penetration tests and telecom network security audits for corporate, government and military clients. We can assess your vulnerabilities and in short time give remediate actions to these vulnerabilities.

Whilst SS7 networks have been vulnerable since inception it has only been the explosion in growth and power of everyday telecoms equipment that these deficits have been able to be exploited.

SS7 Penetration Test

What is an SS7 penetration test?

A SS7 penetration test, or SS7 security audit, is very similar in concept to a PCI compliance test. Through our partnership with multiple mobile operators, we have access to worldwide SS7 connectivity. We will fire various SS7 messages at you from various external sources (trying when possible to test across your multiple SCCP providers, just in case one of them has implemented a cloud-based SS7 firewall solution). Sources of the messages will not be disclosed to you in advance, in order to maintain the independence of the test. Messages will replicate dozens of different types of attacks that are known to us, but will only be directed at specific single-purpose test subscriptions on your network, in order not to disrupt or breach privacy of any real subscriber.

We will not perform any network-wide DOS testing, for obvious reasons, unless you have a lab setup against which we can run these more involved tests.

Typically, no direct SS7 connection needs to be established with your network in order to conduct an audit, which keeps audits relatively inexpensive and quick, when compared to the cost and implementation time of a full-blown on-premises firewall solution.

After the test has been concluded, we will provide you with a report of the those vulnerabilities that have been detected on your network, and we will provide directions as to how they can be eliminated. At your option, we can interact with your mobile node vendors in order to facilitate the production and deployment of patches to address the various issues, and perform a rescan at a later time, to confirm that the vulnerabilities have been eliminated.

SS7 Forensics

Has your network been attacked or hacked via SS7? Or perhaps an attack is ongoing?

We can help with a forensic analysis of SS7 traces (or setup traps, probes, decoys or honeypots to capture information on ongoing attacks and mislead attackers) to determine the target of the attack, the goal, and possibly shed some information on the origin of the attack by using techniques involving correlation, OSINT or fingerprinting of the sending node. More importantly, we can help fast! Possibly today.

We will also recommend ways in which to prevent these attacks going forward, and look for other SS7 vulnerabilities on your network that need to be closed down by running an external SS7 penetration test.

Please contact us using the form below and we will discuss the best course of action for your problem, which may include remote or onsite resources.

Diameter is an authentication, authorization, and accounting protocol for computer networks.

SS7 Intelligence Reports

Forward Defense provides its clients with regular SS7 intelligence reports, providing mobile operators and regulators valuable information about the SS7-based threat landscape and the bad actors that are attacking subscribers through the worldwide SS7 network.

While recent years have seen a lot of attention from telecom regulators on the subject of SS7-based vulnerabilities, and some mobile operators have begun securing their networks, the vast majority of worldwide mobile networks remain vulnerable to SS7-based attacks against their subscribers. Using the SS7 network, an attacker can accurately geo-locate mobile phone, intercept text messages, record phone conversations and much more on unprotected mobile networks.

Through a strategic partnership with The Telecom Defense Limited Company in USA, Forward Defense offers an SS7 intelligence report, updated monthly and sold via annual subscription, that provides a mobile operator or regulator with valuable information regarding the identity of currently active attackers on the SS7 network, new attackers, volumes of attacks and trends, origins, types and signatures of attacks.

The reports are produced using anonymized SS7 metadata provided by various partner mobile operators around the world, which creates a representative and realistic picture of the worldwide threat landscape and its trends month after month.

The monthly report contains:

- Current list of GTs originating malicious SS7 traffic
- Correlation between attacking GTs and patterns
- Types of attacks per GT
- Activity patterns
- OSINT information on the originating networks to help determine possible attribution
- Volume of activity and trends

Diameter Penetration Test

For a basic understanding of what Diameter is, you may want to start *here.*

We are currently concluding the R&D on our Diameter penetration testing methodology and Diameter network audits, and will be offering off-premises Diameter penetration testing shortly.

CDMA PENETRATION TEST

For an over of CDMA is, you may want to start *here.*

Code division multiple access (CDMA) is a channel access method used by various radio communication technologies.

Vulnerabilities for CDMA operators are very similar than those found on GSMA networks. CDMA signaling also use SS7, just a different flavor of it.

Our CDMA penetration test is currently in R&D and we are looking for CDMA networks interested in this subject to serve as initial test targets.

If you are a CDMA network concerned about security vulnerabilities over the signaling interface, please contact us using the form below.

Telco Cyber Security Training

We provide trainings / courses that covers various aspects of telecom network security and fraud, for your engineering, fraud prevention and billing teams. The course contains many real life examples of security breaches and fraud cases in both fixed and mobile networks, as well as a complete training on SS7 based vulnerabilities, and can be eye opening for upper management as well.

We also provide training to country regulators who wish to learn about security issues that may affect mobile operators in their countries, such as SS7 vulnerabilities.

The training can be tailored to your audience in content and length, from one to five days, and will be conducted onsite anywhere in the world.

Some of the contents include:

- Why security is particularly important for telecom operators.
- Proper security starts with internal accountability.
- Internal fraud.
- Internal mistakes that can cost millions.
- External toll fraud in fixed networks, including with wholesale voice transit operations.
- External fraud in mobile networks.
- Roaming fraud.
- SS7 vulnerabilities. How they work, how to find them, and how to prevent them.
- Who is attacking by SS7 and why?
- Sim OTA vulnerabilities.
- Local intercept challenges with multi-IMSI subscribers.

Optionally, an SS7 penetration test of your network can be conducted live during the training session, and the results discussed immediately with the audience. This is particularly effective if the engineers responsible for your SS7 connectivity and various network nodes are part of the audience.