Positive Technologies SS7 Attack Discovery<sup>™</sup>



# DATA SHEET

POSITIVE TECHNOLOGIES



As is shown in the SS7 network analysis performed by Positive Technologies in 2014\*, even hackers with a minimal knowledge of how to launch security attacks against a telecom company can:

- + Disclose a subscriber location
- + Wiretap phone calls
- Intercept SMS messages and passwords
- Steal money from subscriber accounts
- + Affect availability of service

The research also discovered that:

- Even the top 10 telecom operators are vulnerable to these attacks
- + Hacker location and network type are of no significance
- + Hackers only need a Linux-based PC
- + Required software is available on the Internet
- Attacks involve valid SS7 messages: rough filtration can negatively affect your entire service

## **CELLULAR NETWORK SECURITY COMPLICATIONS**

Our society is more reliant than ever on telecommunications. There are at least 4bn subscribers worldwide and 70% of firms rely on the SS7 network for Internet-of-Things (IoT) and Machine-to-Machine (M2M) solutions for the provision of their own services. Everything from ATMs to GPS navigation devices already transmits data over cellular networks.

But there is a significant weakness at the heart of this mobile revolution: the widely-used SS7 signaling protocols were developed decades ago with no protection provided or even planned. Though recently introduced, SIGTRAN specifications for SS7 protocols inherited all the weak points of SS7.

Mobile communications further evolved to provide mobile carriers and service providers with wider access to SS7 networks. Overall roaming connectivity adds to the pressure on mobile carriers to ensure network security and continuity of service. This lack of security enables hackers to send, intercept, and alter SS7 messages attacking cellular networks and subscribers.

Recently, SS7 security has become very topical:

- When Edward Snowden, a former contractor for the CIA, first talked about the total surveillance by the NSA, many infosec experts showed evidence that the main technique the NSA could have used was exploitation of SS7 vulnerabilities.
- + There are private companies offering SS7 attack services at reasonable rates, and as more companies enter the market, the rates continue to fall.
- Celebrities' private conversations posted on the Internet by hackers have become more frequent.
- + Current SS7 filtering systems (firewalls) are weak as they fail to analyze signaling traffic flows in detail without causing a loss of speed and connectivity.

\* www.ptsecurity.com/library/whitepapers/

# PT SS7 ATTACK DISCOVERY<sup>™</sup>: DETECTING MOBILE ATTACKS

PT SS7 Attack Discovery<sup>™</sup> — a new telecom security solution from Positive Technologies — detects intrusions via an SS7 network online and immediately informs infosec departments for early incident response. The system also performs a retrospective analysis of signaling traffic and assists in forensics tasks while not interfering with SS7/SIGTRAN interaction. Key features:

- + Detection of all SS7 attack vectors including: examination of the network and collection of subscriber data (IMSI, MSC/VLR, HLR), user location tracking, interception of SMS messages, sending of spoofed SMS and USSD messages, subscriber or cellular segment DoS, billing by-pass, alteration of subscriber profiles in VLR and subscriber categories.
- + Low impact on signaling traffic. The PT SS7 AD<sup>™</sup> system is implemented at the border of the SS7 network avoiding a negative effect on signaling traffic. Only an IP connection is required. There is no need to assign special addresses to SS7 in the form of Signaling Point Codes (SPC) or Global Titles (GT). Quick attack identification and its thorough analysis enhances protection avoiding impact on the speed of the network and its services.
- Message correlation. This is available in systems with load balancing over several Signal Transfer Points (STPs), ensuring the whole SS7 perimeter is covered and preventing false positives.
- + Regularly updated knowledge base. PT SS7 AD<sup>™</sup> benefits from the expertise of the specialist Positive Technologies Telecoms Research Lab, ensuring it reflects the very latest research on SS7 security.
- + **Dynamic analysis.** This approach rapidly determines which SS7 network activity is irregular by monitoring traffic changes and comparing its characteristics at different times.
- + Data visualization. User-friendly dashboards display information about all interactions with external SS7 networks; attacks and fraud attempts. These dashboards are configurable for ease of data analysis.



#### ADDITIONAL FEATURES

PT SS7 Attack Discovery<sup>™</sup> is used to create a single SS7 stream database in a carrier's network. In addition to detecting attacks, its in-depth analysis of signaling traffic and call flows enables carriers to:

- + Investigate fraud
- Gather evidence of malicious activity
- + Detect equipment errors
- + Find bottlenecks in the carrier's infrastructure

## ATTACK VECTORS: HOW TO DETECT AND PREVENT

**Example Nº1: Network investigation and collection of subscriber data** (IMSI, MSC/VLR, HLR). A hacker examines an operator's network **(1)**, finds core hosts, determines their functional roles **(2, 3)**, and collects information that the network discloses **(4)**.



Meanwhile, PT SS7 AD<sup>™</sup> logs his actions identifying illegal use of such messages as SRI4SM, SRI, SRI4LCS, SendIMSI, etc. Recognizing attacks while they are being planned helps to prevent their execution.

**Example Nº2: Disclosure of subscriber location and control over his moves.** With necessary data on the network and its subscribers gathered, the hacker directly addresses the main hosts (1, 2) requesting information about the subscriber via ATI, PSI, and SRI messages (3).



Using signature analysis, PT SS7 Attack Discovery<sup>™</sup> singles out illegal messages from the traffic and registers an attack attempt. Rapid response to the attack can block and prevent the hacker from monitoring subscriber moves.

**Example №3: Interception of SMS messages** is one of the most perilous attacks because it exploits SMS messages that often include sensitive information such as payment confirmation (3D Secure codes) and recovery data for email, social network, and payment service passwords. The attacker only needs to register a victim subscriber on a fake MSC/VLR **(1, 2)**. If successful, the hacker will receive all subscriber's SMS messages **(3–6)**.



#### POSITIVE TECHNOLOGIES



Analyzing subscriber registration outside the home network, PT SS7 AD<sup>™</sup> checks its integrity and detects suspicious and unfinished procedures that prove attack attempts. With this attack detected, you can be sure there was an attempt to compromise a subscriber and obtain his data. Therefore, prevention of such attacks and notification of clients of such attempts is a necessity.

**Example №4: DoS for MSC.** A hacker can directly attack an operator's network and its services. The most severe are DoS attacks because they cause network unavailability and many other negative implications. The attack is based on the procedure of assigning a roaming number (MSRN) when receiving a voice call. If an attacker sends multiple roaming number requests (1), then the pool of available numbers will soon be exhausted (2). As a result, the switch will not be able to process terminating calls (3).



Studying valid call flow sequences, PT SS7 AD<sup>™</sup> detects attacks at the very beginning, identifies and helps to block attack sources. Detection of other DoS attacks — exploitation of HLR Reset and SCCP Management, denial of service via SSN Prohibit and TID Flood — has the same algorithm.

PT SS7 Attack Discovery<sup>™</sup> can also discover redirection and wiretapping of voice calls, sending of fake SMS and USSD messages, subscriber DoS, spoofing of a subscriber's profile in a VLR, alteration of a subscriber's category, and many other attacks. For details, see the SIGNALING SYSTEM 7 (SS7) SECURITY REPORT at <u>http://www.ptsecurity.com/upload/ptcom/SS7\_WP\_A4.ENG.0036.01</u>. <u>DEC.28.2014.pdf</u>



# PT SS7 ATTACK DISCOVERY<sup>™</sup> IN USE

#### Modularity

PT SS7 Attack Discovery<sup>™</sup> includes two types of modules. SS7 Sensor collects raw SS7 traffic from the STP, singles out useful data, and sends messages to Attack Detector. Attack Detector aggregates processed SS7 traffic from all SS7 Sensors in the network, creates dialogs, discovers intrusions using its knowledge base, and examines signaling traffic for unusual behavior.

#### Full view

PT SS7 Attack Discovery<sup>™</sup> obtains data from all required links, either international or local, and places it in separate dialogs on Attack Detector to avoid loss of system messages and false positives.

#### In-depth protocol analysis

PT SS7 AD<sup>™</sup> studies all-layer protocols and checks address information, address and subscriber ID compliance, and operation codes. Based on the complete view of the signal exchange, the system comes to a conclusion about the attack and immediately informs the infosec department about it.

#### **Call flow inspection**

With a vast knowledge of mobile systems, PT SS7 AD<sup>™</sup> identifies suspicious messages from external networks, unusual message sequences, and wrong equipment responses to outside actions. The system renders all data on anomalies to information security staff for analysis.

#### Flexible classification of attacks

With a custom event classification system, PT SS7 AD<sup>™</sup> signals an attack if a message comes from a blacklisted address. There is also the option to create white lists — a limited number of addresses whose actions will be recognized as valid.

## **DEPLOYMENT AND OPERATION MODES**

PT SS7 Attack Discovery<sup>™</sup> is deployable both as hardware and as a virtual solution. Depending on the client's tasks and technical specifications, the system can run in a variety of modes:

1. External traffic analysis on the STP. PT SS7 AD<sup>™</sup> receives all incoming and outgoing traffic on an "external" STP interface and detects attacks against telecom carriers.



2. Traffic analysis after the border STP. To detect intrusions into a border device, PT SS7 AD<sup>®</sup> examines a copy of traffic from an internal SS7 network on any aggregating host.



PT SS7 Attack Discovery" processes the copy of signaling traffic and keeps away from the SS7/SIGTRAN interaction between operators avoiding any damaging impact on the network and its services speed.

**3.** Traffic analysis before network elements. If PT SS7 AD<sup>™</sup> cannot obtain a traffic copy from an aggregating host, it studies traffic before key network elements (MSC/VLR, HLR, SMSC).



**4.** Analysis of specific message types. SIGTRAN must be connected to the STP. The STP must be able to copy traffic depending on specific features of signaling messages.



### ADDITIONAL SERVICES: TELECOM SECURITY ANALYSIS

PT SS7 Attack Discovery<sup>™</sup> enhances detection of real-time intrusions via the SS7 network. Nonetheless, you can prevent many attacks beforehand discovering vulnerabilities and noncompliance with security standards on all the levels of the telecommunications infrastructure. Positive Technologies provides telecom companies with:

- SS7 security audit service that includes MAP/CAP attack simulation, assessment of impact on CS Core (MSC/VLR/HLR/AuC), forensic investigation of possible fraud or SS7-based security incidents.
- + Cell network security assessment to examine various vulnerabilities and configuration weakness in the radio access network that could allow illegal use of services and disruption or degradation of services delivered through 2G, 3G, and 4G.
- Mobile application security service to reduce the risk of security breaches that could cause significant financial losses and damage to reputation. We provide both client- and server-side application analysis using gray- and white-box testing to identify vulnerabilities and find ways to neutralize them.
- Penetration testing to detect hidden system flaws; evaluate the potential impact on operations if those flaws are exploited; verify the efficiency of current security tools and evaluate the level of security awareness among staff.
- Vulnerability research into new technologies, protocols, and applications to check whether security mechanisms are missing or employed incorrectly; to identify vulnerabilities and security issues that arise as a result and reduce associated risk.
- + Security and compliance audit (ISO 27001, 27002, and 27011; TIA, ITU, NIST, ETSI recommendations) as a basis for development of an adequate and comprehensive action plan for information security enhancements. Such plans help to mitigate the financial and reputational risk related to information security.

#### **About Positive Technologies**

Positive Technologies is a leading provider of vulnerability assessment, compliance management, and threat analysis solutions to more than 1,000 global enterprise clients. Our solutions work seamlessly across your entire business: securing applications in development; assessing your network and application vulnerabilities; assuring compliance with regulatory requirements; and blocking real-time attacks. Our commitment to clients and research has earned Positive Technologies a reputation as one of the foremost authorities on SCADA, banking, telecom, web application, and ERP security, and distinction as the #1 fastest growing Security and Vulnerability Management firm in 2012, as shown in an IDC report\*. To learn more about Positive Technologies please visit ptsecurity.com.

\*Source: IDC Worldwide Security and Vulnerability Management 2013-2017 Forecast and 2012 Vendor Shares, doc #242465, August 2013. Based on year-over-year revenue growth in 2012 for vendors with revenues of \$20M+.

© 2016 Positive Technologies. Positive Technologies and the Positive Technologies logo are trademarks or registered trademarks of Positive Technologies. All other trademarks mentioned herein are the property of their respective owners.

POSITIVE TECHNOLOGIES

pt@ptsecurity.com ptsecurity.com