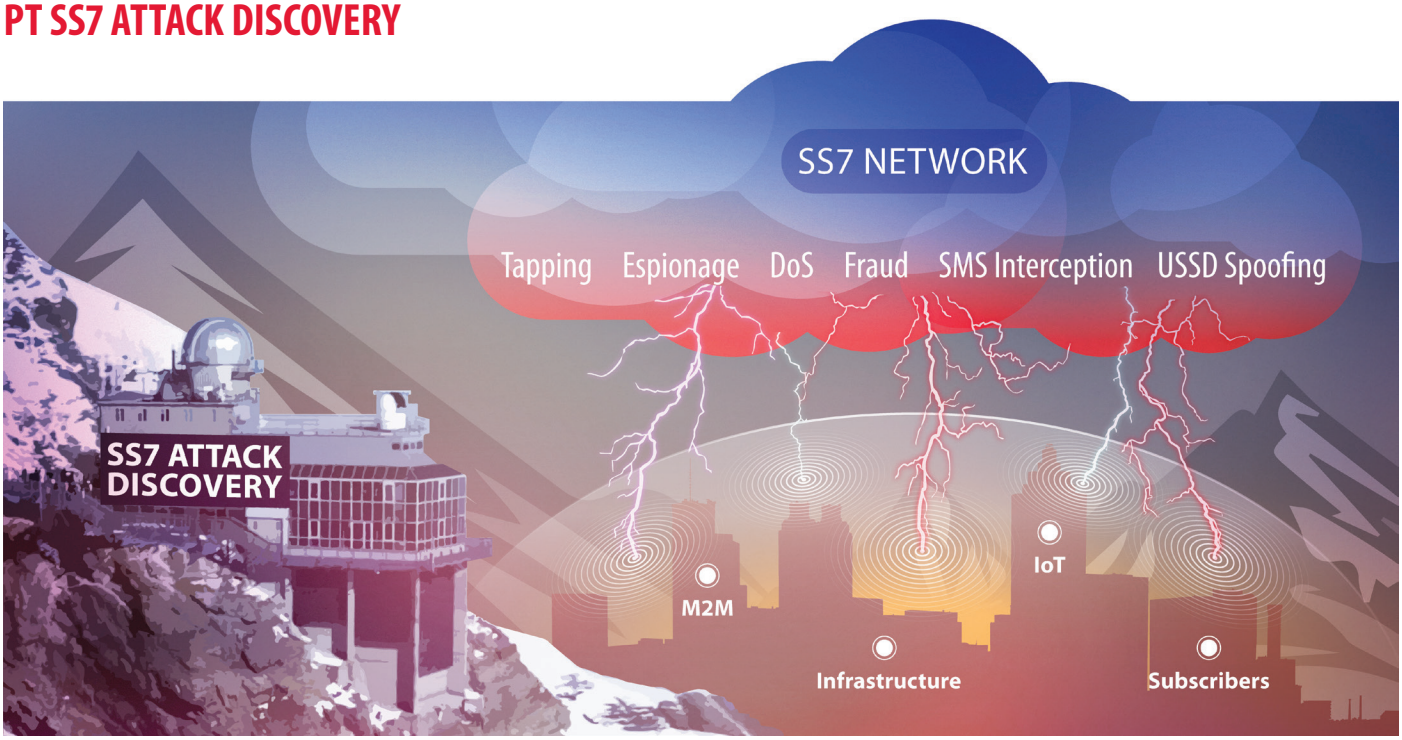
A FAST AND PAINLESS ROUTE TO SAFER SIGNALING TRAFFIC: PT SS7 ATTACK DISCOVERY



HIGHLIGHTS

PT SS7 Attack Discovery can detect many types of malicious activity, including

- **Monitoring networks and harvesting** subscriber data (IMSI, MSC/VLR, HLR)
- **Tracking** a subscriber's location
- **Redirection and wiretapping** of voice calls and SMS
- **Sending fake** text messages and data (USSD) from a subscriber's number
- **Denial of service** to a subscriber or a network segment
- **Bypassing** the carrier's billing system to make free calls
- **Editing** subscriber profiles in VLR, e.g. switching anonymous prepaid SIMs to function as post-pay and provide free calls

Our society is more reliant than ever on telecommunications. There are at least 7.4bn active mobile phone subscriptions worldwide, a figure that's likely to top 9bn by 2021*. The Internet of Things (IoT) and the growing use of Machine to Machine (M2M) solutions add to the pressure on mobile carriers to ensure network security and continuity of service. Everything from ATMs and payment terminals to GPS navigation devices already transmits data over mobile networks and the trend is rapidly gathering pace. In a 2013 Economist survey across 19 industries, 75% of business leaders said they were already exploring IoT and 96% expected to be using it by 2016**.

But there is a significant weakness at the heart of this mobile revolution: the widely-used SS7 signaling protocols. SS7 was developed decades ago, before the Internet was invented and hackers became a threat. Today, research from Positive Technologies*** shows that even low-skilled intruders with cheap equipment can exploit vulnerabilities in SS7/SIGTRAN networks to commit fraud, steal sensitive data, and interrupt services. Telecommunications companies cannot afford to ignore this threat.

PT SS7 Attack Discovery (PT SS7 AD) from Positive Technologies gives telcos the ability to detect, identify, and analyze attacks on their SS7 networks, without having a negative impact on services. It analyzes irregular activities on SS7 networks, performs retrospective analysis of signaling traffic and helps to investigate fraud.

Detection Without Damaging Effects

Several vendors offer specialist SS7 firewalls, but they have never been 100% effective, largely because of fears that any in-depth analysis of signaling streams could impair network speed and availability. With SS7 attacks based on legitimate messages, it's hard to filter malicious activity without a negative impact on communications.

Pressure on carriers to find a more practical solution grows rapidly from all sides: regulators, shareholders, consumers, and enterprise customers. PT SS7 AD meets this need with a no-impact deployment model on the border of the SS7 network. Only an IP connection is required to begin detecting and investigating the most critical and common forms of malicious activity.

* Ericsson's Mobility Report, November 2015: http://www.ericsson.com/res/docs/2015/mobility-report/ericsson-mobility-report-nov-2015.pdf
** The Internet Of Things Business Index, 2013: http://www.economistinsights.com/analysis/internet-things-business-index/fullreport
*** Positive Technologies SS7 Security Report, 2014: http://www.ptsecurity.com/upload/ptcom/SS7_WP_A4.ENG.0036.01.DEC.28.2014.pdf

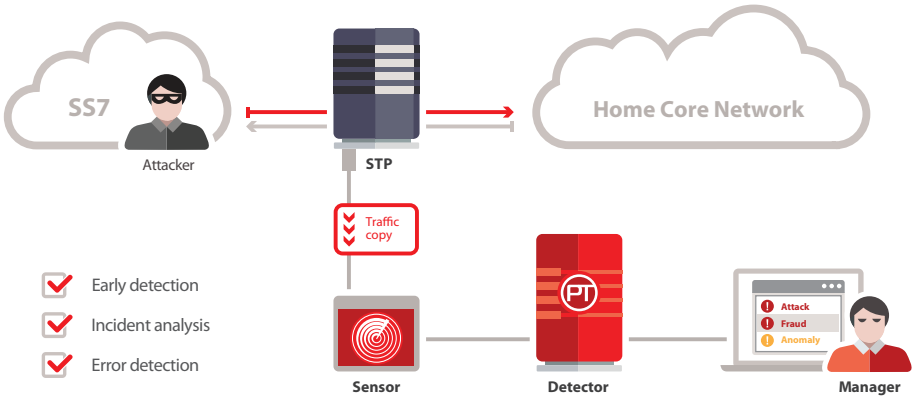
ENHANCED NETWORK INTELLIGENCE FROM PT SS7 ATTACK DISCOVERY

PT SS7 Attack Discovery 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:

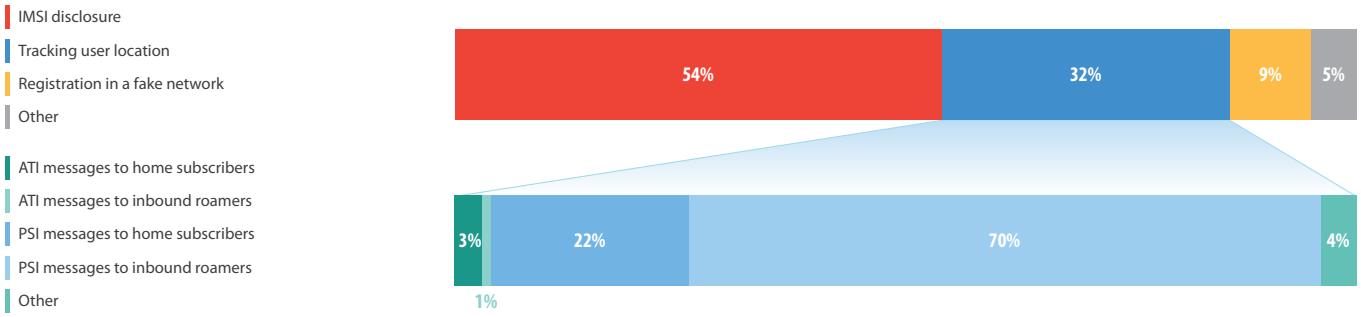
+ Investigate fraud
+ Gather evidence of malicious activity
+ Detect errors in equipment
+ Find bottlenecks in the carrier's infrastructure

PT SS7 ATTACK DISCOVERY KEY FEATURES

+ **No impact on signaling traffic.** The PT SS7 AD 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).



+ **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 benefits from the expertise of the specialist Positive Technologies Telecoms Research Lab, ensuring it reflects the very latest research on SS7 security.
+ **Heuristic analysis.** This approach rapidly determines which SS7 network activity is irregular; helping to detect emerging attacks not already included in the PT SS7 AD knowledge base.
+ **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. The example dashboard image below shows the distribution of attacks by type and gives detailed information on the methods used to perform subscriber tracking.



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+.

POSITIVE TECHNOLOGIES

pt@ptsecurity.com ptsecurity.com