

Securing SS7 Telecommunications Networks

G. Lorenz, T. Moore, G. Manes, J. Hale, S. Shenoi*

Abstract— Signaling System 7 (SS7) defines the network architecture, configuration and message transport protocol for Public Telephone Networks (PTNs). SS7 was originally designed for a closed telecommunications community, and therefore possesses limited authentication facilities. Deregulation coupled with PTN convergence with the Internet and wireless networks significantly increase vulnerabilities, enabling attackers to perpetrate fraud, interception and interruption on a potentially massive scale.

This paper analyzes vulnerabilities in SS7 networks and presents an attack taxonomy. The architecture of a system for detecting and responding to SS7 network attacks is also described.

Keywords— Public telephone networks, SS7 networks, vulnerabilities, critical infrastructure protection

I. INTRODUCTION

Public Telephone Networks (PTNs) are massive heterogeneous networks comprising three overlapping sub-networks: a PTN backbone, the Internet and wireless networks [4,9,13]. The PTN backbone employs signaling, transmission and operations equipment. Signaling equipment sets up and tears down calls; it includes databases and adjunct processors for number translation and call routing. Transmission equipment carries the actual telephone conversations. Operations equipment, including the operations support system (OSS), performs management, inventory, engineering and repair functions [12].

The older in-band signaling technique combined signaling and transmission over “homerun” copper wires. But this solution was inefficient and did not support advanced PTN services [2]. The newer – and widely used – out-of-band signaling separates voice transmission from the data that manage calls. Out-of-band communication between central-office switches occurs via dedicated (private and public) X.25 data networks using special protocols, most notably Signaling System 7 (SS7), to set up calls, establish billing and return busy signals [2,12].

The global standard for telecommunications, SS7 defines procedures by which PTN elements exchange information over a digital signaling network. The SS7 standard governs network architecture, configuration and message transport. The network architecture supports base communications, routing and database access across PTNs. Dedicated out-of-band SS7 networks also help prevent in-band fraud while

conserving telecommunications resources.

Although SS7 reduces in-band attacks, it introduces other vulnerabilities [8,11]. The protocol was originally designed for a closed telecommunications community; therefore, it possesses limited authentication facilities. However, deregulation now requires phone companies to provide SS7 connections to any entity for a modest fee. The Internet-PTN convergence allows attackers inroads via entities with poorly secured SS7 networks. ISDN connections are also points of unauthorized entry.

Once access to a PTN is gained, an attacker can perpetrate modification, fabrication, interception and interruption on a potentially massive scale. For example, during a terrorist bombing incident, an attacker can modify entries in a call forwarding database to re-route all phone calls to emergency services, disrupting them and possibly increasing the number of casualties.

Very few systems exist for securing SS7 networks. SecureLogix produces Telewall, a firewall for private branch exchanges (PBXs) that controls unauthorized access [14]. Sevis Systems has developed the IntelGuard Signaling Firewall for controlling access to central office switches [15]. Apart from these efforts, published research on defending SS7 networks against attacks is virtually non-existent.

This paper focuses on the problem of securing SS7 networks. The SS7 architecture and protocol are described, and their vulnerabilities are analyzed in detail. A taxonomy of attacks on SS7 networks is presented, and the architecture of a system for systematically detecting and responding to these attacks is described.

II. SIGNALING SYSTEM 7 (SS7) NETWORK

Public Telephone Networks (PTNs) typically are composed of a PTN backbone, the Internet and wireless networks (Figure 1) [4,9]. The PTN backbone primarily uses the Signaling System 7 (SS7) protocol, the Internet employs the TCP/IP protocol suite, and wireless networks use the CDMA, TDMA and GSM protocols [5,7]. As shown in Figure 1, the PTN backbone is connected to the Internet and wireless networks via IP and wireless gateways, respectively. In addition, the PTN backbone maintains diverse connections to entities ranging from large organizations to individual users. For example, individuals and small organizations use xDSL, Dial-Up and ISDN connections to access the PTN (or Internet) [6]. Large organizations em-

* To whom correspondence should be addressed (email: sujeet@utulsa.edu).

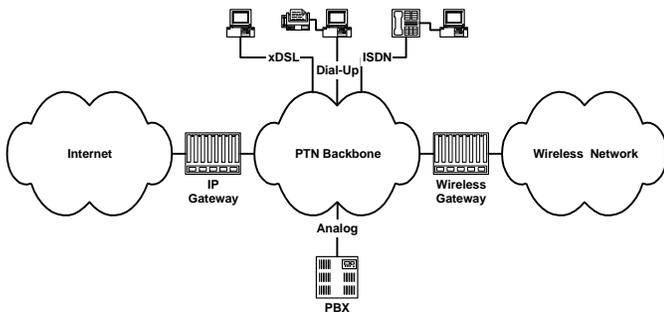


Figure 1. Public telephone network schematic.

ploy analog trunks to connect PBXs (Private Branch Exchanges) to the PTN.

The SS7 network controls many PTN features, e.g., basic call setup, management, tear down, billing and returning busy signals. It also supports advanced services such as local number portability (LNP), toll-free (800/888) and toll (900) services. Enhanced call features such as call forwarding, calling party name/number display, and three-way calling are also controlled. SS7 not only facilitates these and other new services, but also provides a more efficient and secure telecommunications network.

The SS7 standard defines the signaling architecture and protocols employed for message transport. This section describes these components in detail.

A. SS7 Architecture

The SS7 architecture comprises three signaling points: service switching points (SSPs), signal transfer points (STPs) and service control points (SCPs) (Figure 2). Each signaling point is identified by a unique point code that facilitates the routing of signaling messages. Signaling points are connected via signaling links, typically 56 or 64 kbps bi-directional X.25 data links. SSPs are the entry and exit points for SS7 networks, i.e., they strictly originate, terminate and tandem telephone calls. They are analogous to border routers on the Internet and are the primary entry points for attackers.

Figure 2 shows an SSP (1) connected to two pairs of STPs via access (A) links, the primary channels for all STP-SSP communications. A links simultaneously support up to 9600 connections [12]. If the number of connections exceeds 9600, the SSP diverts traffic to extended (E) links (shown connecting SSP (1) to an alternative STP in Figure 2). The architecture does not demand that SSPs be deployed with E links. Therefore, some SSPs, e.g., SSP (2) in Figure 2, cannot handle large volumes of traffic. SSPs communicate by sending signaling messages over A and E links to other SSPs via STPs. They send queries to SCPs via STPs using separate links.

Figure 2 shows the four primary line types connecting

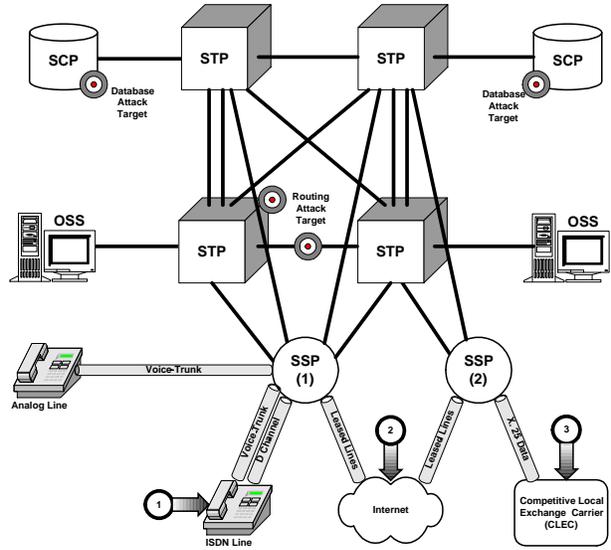


Figure 2. SS7 network architecture.

SSPs to end users: analog lines, ISDN lines, X.25 data lines and leased lines. Voice trunks are analog lines directly connected to SSPs. Analog signals received by SSPs are converted to digital signaling messages to handle the call. ISDN lines represent the next stage of PTN evolution by removing analog signals from the loop [1]. These connections contain a digital (D) channel that generates digital signaling messages (resembling SS7 packets) at customer telephones, interfacing directly to SSPs. The D channel of an ISDN connection architecturally resembles the X.25 connections used by competitive local exchange carriers (CLECs), typically small start-up companies offering services ranging from long distance to voice mail [12]. In addition, much of the Internet is connected to SSPs via leased lines. Therefore, all data passing over these lines also passes through SSPs.

Once a call has been initiated by an SSP, it is routed using a matching set of STPs. All SSPs are connected to at least one mated pair of STPs. STPs are the routers of a PTN, receiving and then routing SS7 network traffic between signaling points. Messages to outside destinations must travel through dedicated STPs. STPs facilitate database access by detecting and routing queries to SCPs. They also connect call requests between SSPs. As shown in Figure 2, STPs often link to the operations support systems (OSSs), remote maintenance centers that monitor and manage PTNs. Using signaling links, OSSs connect to STPs, introducing SS7 messages throughout the PTN.

SCPs provide database access needed for advanced services. They directly connect to STPs (like SSPs). SCPs respond to queries with information necessary to process calls, accessing information sources that maintain consumer and call information, including call management service databases (CMSDBs), local number portability (LNP)

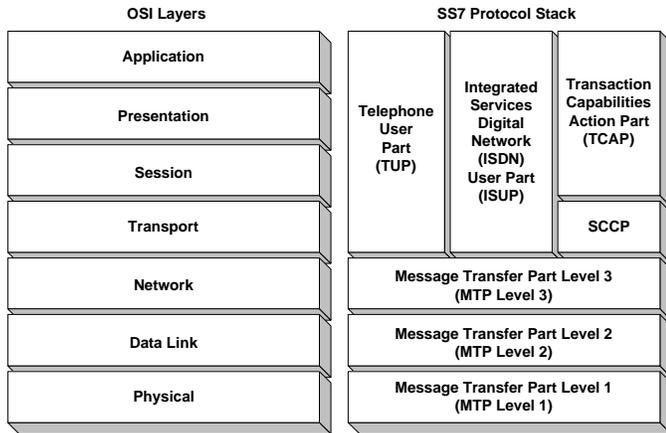


Figure 3. SS7/OSI protocol stacks.

and line information databases (LIDBs) [12].

B. SS7 Protocol

The SS7 protocol defines the procedures for operating and communicating over SS7 networks. The protocol resembles the popular OSI model (see Figure 3) [12]. The SS7 message transfer part (MTP) Levels 1 – 3 correspond directly to the physical, data link and network layers of the OSI model. The user and application parts of the SS7 protocol loosely correspond to OSI Layers 4 – 7; they define the connection/disconnection protocol and the remote database access protocol.

MTP Level 1 defines the electrical characteristics of signaling links and the types of interfaces used in the network, e.g., Digital Signal 0 (DS0A) and V.35. DS0A is a 56/64 kbps channel within a DS1 (1.544 Mbps) facility, often used in ISDN networks and T-1 trunks [12]. DS0As are the most commonly used interfaces in the United States. V.35 interfaces also support 56/64 kbps links, but they were designed to interface analog modems with digital lines and are no longer recommended.

MTP Level 2 ensures the sequenced delivery of all SS7 messages and provides the tools necessary for reliable transport throughout the network. MTP Level 3 routes and distributes messages to the proper destinations. Using routing tables that store point codes, the routing function finds the correct destination point codes and delivers the messages. Link, routing and traffic management of network elements all occur at the network level. Link management oversees the error levels at each link and sends messages advising of a link’s failed or restored status. In cooperation with link management, routing management facilitates the re-routing of traffic around failed or congested nodes. When certain functions of a node fail, traffic management notifies other signaling points about the failure, and only re-routes those signals that are affected by the failure. The similarities between the SS7 and OSI protocols fade at this point.

Once MTP ensures reliable signaling between adjacent nodes, SS7-specific protocols define cross network communications such as telephone call connections, disconnections and remote function control. The ISDN user part (ISUP) provides connection-oriented services in SS7 networks, setting up and tearing down circuits for voice and data between exchanges [1,12]. ISUP also offers supplementary services for the circuits carrying the transmission, e.g., sending caller information between the end points during calls. International networks employ the telephone user part (TUP) to handle call setup and teardown. TUP is compatible with ISUP, but it does not facilitate the needs of modern digital networks, especially advanced services. Consequently, ISUP is the predominant protocol while TUP is being phased out worldwide.

The signaling connection control part (SCCP) provides connectionless and connection-oriented services, although it has only been implemented for connectionless services. While MTP provides routing between adjacent nodes, SCCP performs end-to-end routing for the transaction capabilities application part (TCAP) protocol. TCAP employs SCCP connectionless service to transport non-circuit related information between signaling points. End users in the SS7 network use TCAP for peer-to-peer communication. Since TCAP allows signaling points to remotely access each other, TCAP also supports database access. In addition, SCCP enables STPs to provide global title translation, i.e., allow originating messages to only indicate general digits, not point codes. Subsequently, STPs use SCCP to transport messages to their destinations, effectively preventing outsiders from obtaining internal network point codes.

III. SS7 NETWORK VULNERABILITIES

Major SS7 network vulnerabilities, as with the Internet, arise from the number and complexity of interfaces between distinct SS7 entities. Moreover, advanced services like call forwarding have intrinsic vulnerabilities – attackers can create havoc by modifying SCPs containing forwarding destinations.

Additional vulnerabilities arise from the increasing interdependence and interconnectivity between SS7 networks and the Internet [4,6,9]. Large portions of the Internet use leased phone lines. Conversely, SS7 systems are networked using Internet technologies, and often, the Internet itself. Thus, SS7 vulnerabilities can affect the Internet, and Internet vulnerabilities can affect SS7 networks. Furthermore, SS7 incorporates limited authentication procedures (because it was originally designed for a closed telecommunications community). Consequently, anyone capable of generating SS7 messages and introducing them into a network can disrupt PTN services. Figure 2 identifies potential entry points for attacks (Attackers 1, 2 and 3).

Users with ISDN connections can introduce digital mes-

sages into the SS7 network [1]. Attacker 1 in Figure 2 exploits this relationship by spoofing the source telephone number and introducing malicious packets onto the network. Additionally, PTN-Internet convergence gives Attacker 2 new entry points to the network. While large regional Bell operating companies (RBOCs) have significant security staff and resources, competitive local exchange carriers (CLECs) – typically small startup companies – often have limited budgets and may be relatively insecure. Thus, Attacker 2 can gain access to SSPs by compromising networked computers at a CLEC.

The Telecommunications Act of 1996 grants an SS7 network connection to any entity (including a possibly malicious one) for a modest fee (currently \$10,000) [13]. Traffic on SS7 networks is therefore suspect (Attacker 3 in Figure 2).

Because STPs and SCPs use front-end computer systems, hacker exploits that seize control of network operating systems pose serious threats. Local number portability (LNP), another service mandated by the 1996 Telecommunications Act, allows telephone users to switch local providers without having to change telephone numbers. LNP is another point of vulnerability. Once access is gained to SS7 networks, attackers have it easy. Virtually no systems exist for detecting and responding to attacks.

A. SS7 Attack Taxonomy

The vulnerabilities described in the previous section enable a slew of attacks on SS7 networks. An attack taxonomy is presented in Figure 4. The targets are SSPs, STPs and SCPs. Four types of attacks are possible: modification, interception, interruption and fabrication [10].

B. SSP Attacks

SSPs constitute the SS7 network perimeter and are the gateways for attack. Most attacks exploit SS7's weak authentication. For example, ISDN was designed to connect the edges of SS7 networks to end users, enabling ISDN users to introduce traffic directly into an SS7 network [1]. Malicious ISDN users can modify or fabricate ISUP messages. Indeed, ISDN connections are similar in design to SS7 connections used by CLECs. ISDN connections, however, are available at a much lower cost (less than \$100 per month).

All SS7 network elements are susceptible to packet sniffing. However, an SSP is a prime target for sniffing specific users, because each user's traffic must flow through the corresponding SSP. Attackers can also intercept services intended for a user by appending the attacker's destination to the original destination in the message.

SSPs, like all network elements, have a maximum operating capacity. Overloading an SSP-STP connection can interrupt SSP service, denying service to a segment of users. For example, one distributed denial of service (DDoS) at-

tack introduces large numbers of initial address messages (IAMs, i.e., ISUP messages that start call setups) and direct them at a single SSP. Attackers could also intercept all traffic at a compromised signaling point, and modify IAMs to request connections with a targeted user on the same SSP. Since message sources of ISUPs can be spoofed quite easily, SSPs cannot trace the sources of such attacks.

C. STP Attacks

STPs perform routing and all messages must pass through them. Therefore, attacks that exploit routing protocols are a major concern.

SSP traffic travels directly through STPs. Thus, attackers who compromise an STP can view all traffic to and from the corresponding SSPs. A more sophisticated attack remotely compromises an STP, and then creates a transparent bogus STP that filters traffic and re-routes it to the STP. Thus, it is possible to eavesdrop on selected conversations. Modifying the destinations of SCCP (end-to-end) messages allows corresponding telephone calls (and database queries) to be re-routed at will.

Since OSSs connect to STPs, toll fraud can be perpetrated by seizing control of the OSS via the STP. Global title digits are the digits provided by the called party address. These digits do not give the point code or subsystem number, although SCCP translates the global title digits to the appropriate point code. SCCP messages with a global title (e.g., 800 number) must be routed through an STP, which then translates the global title to the actual point code, usually an SCP. Point codes are sensitive information, and global title translation protects the information by requiring an originating message to only provide general information that the STP can then translate to specific point codes. However, if an STP is compromised, the point codes of internal network nodes can be determined by accessing the corresponding SCPs. Another attack can modify the global title translation database maintained within the STP.

As with all routers, STPs can be overloaded with traffic, although, this is more difficult because STPs are usually deployed in redundant mated pairs. Denial of service attacks are still possible, however, if multiple SCP databases are modified to re-route large numbers of calls to telephone numbers on a specific SSP. Additionally, an attacker compromising multiple STPs could re-route all received messages to a target STP, in effect, overloading the STP and rendering the connected SSP useless.

The OSS is susceptible to traditional computer attacks. These include viruses, worms and Trojan horses since the OSS is typically a collection of computers.

STPs and SCPs maintain local number portability (LNP) databases that hold information for routing calls. Queries of LNP databases require considerable system resources. Therefore, LNP overload is a real threat – an at-

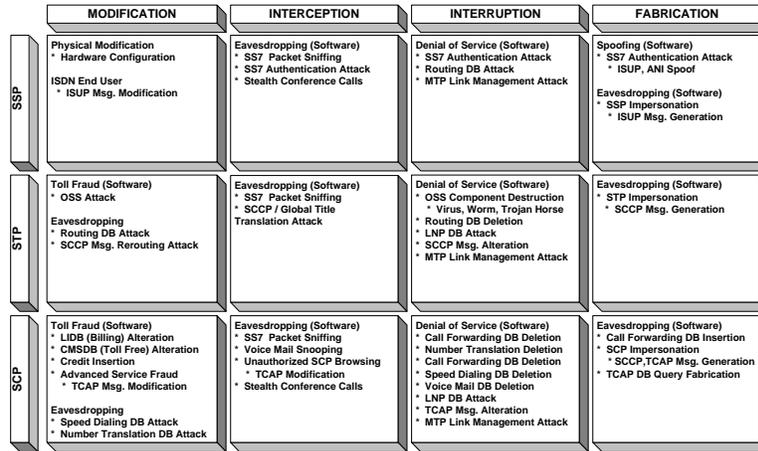


Figure 4. SS7 attack taxonomy.

tacker generating massive amounts of LNP queries can shut down STPs and/or SCPs maintaining the LNP databases. Additionally, telephone numbers in LNP databases can be modified or erased.

MTP Level 3 of the SS7 protocol provides sophisticated link traffic management [11]. Message signaling units (MSUs) can notify surrounding signaling points of a node failure, causing traffic to be re-routed around the failed node. Fabricated MSUs could render operational signaling points useless, resulting in congestion and possible crippling of the network.

D. SCP Attacks

SCP databases that store sensitive information are highly vulnerable. Consider, for example, call management services databases (CMSDBs) that process toll-free calls [12]. Toll-free numbers do not represent the actual telephone number dialed. Instead, the toll-free number is mapped to an actual telephone number and the billing information is maintained separately. The CMSDB provides routing instructions that map the call and the billing information for the call. An attacker could fraudulently change the destination number to some other number, thus removing all charges for calls made to destination number. Alternatively, the owner of a toll-free number could also change the billing information to avoid charges.

Similar modifications are possible with billing databases, LNP databases, line information databases (LIDBs) and others. An LIDB maintains subscriber information, including billing, collect call service, calling card service and validation, and personal identification numbers (PINs). Access to this database facilitates malicious activities ranging from identity theft to toll fraud. For example, attackers could modify the billing amounts, intercept, and even modify PINs.

Many SCP attacks utilize TCAP messages that support access and modification of SCP databases. For example,

an attacker could modify the subscriber account number in a TCAP message destined for an LIDB and so avoid billing. Likewise, subscribers' PINs could be obtained by generating the appropriate TCAP requests.

Voice mail databases have similar vulnerabilities. An attacker could send a TCAP message query for a certain user's password and gain full access to his/her voice mailbox.

SCP databases are also vulnerable to interruption or denial of service attacks. A compromised SCP could simply have its databases deleted, disrupting all advanced services. Additionally, a business could interrupt a competitor's toll-free number by associating it with an unrelated, even illicit, telephone number (e.g., a phone sex company.) More seriously, an attacker could modify all the destination numbers in a call-forwarding database and route them to a single number, e.g., emergency services (911), completely shutting it down.

The fabrication of TCAP messages also permits unauthorized SCP database access and modification. Such attacks can severely disrupt SS7 network services.

IV. SS7 ATTACK MANAGEMENT SYSTEM

Attack management in an SS7 network requires the coordination of diverse platforms, operating systems and applications. The subsystems and tools constituting the attack management system, currently under development, must be strategically positioned throughout the SS7 network (Figure 5).

The heterogeneous, distributed architecture requires a secure communication infrastructure that provides authentication, encryption and access control mechanisms. The infrastructure employs a combination of a private (back-side) network and a VPN-style public network. Secure communication will be implemented using public/private key cryptography and secure broadcasting (with capabilities).

V. CONCLUSIONS

During the fall of 1997, telephone systems in Puerto Rico were sabotaged by physically cutting lines [3]. The convergence of information and communications into a single global network makes it possible to conduct similar attacks from afar with software. Sophisticated systems are required to address a spectrum of cyber threats – ranging from emergency service disruption to coordinated strikes designed to destroy the communications infrastructure and cripple American society [16].

While substantial attention has been directed at securing computer networks, little work has focused specifically on public telephone networks (PTNs). This paper is among the first to analyze vulnerabilities in SS7 networks and present an attack taxonomy. It is hoped that this taxonomy and the system for detecting and responding to SS7 network attacks, currently under construction, will spur efforts to develop and deploy sophisticated systems for safeguarding telecommunications networks.

ACKNOWLEDGMENTS

This research is supported by the National Institute of Justice through the Memorial Institute for the Prevention of Terrorism (MIPT), Oklahoma City, Oklahoma.

REFERENCES

- [1] U. Black, *ISDN and SS7: Architectures for Digital Signaling Networks*, Prentice Hall, Upper Saddle River, New Jersey, 1997.
- [2] J. Bosse, *Signaling in Telecommunication Networks*, John Wiley and Sons, New York, 1997.
- [3] D. Denning, *Information Warfare and Security*, Addison-Wesley, Reading, Massachusetts, 1999.
- [4] I. Faynberg, et al., *Converged Networks and Services: Internet-working IP and the PSTN*, John Wiley and Sons, New York, 2000.
- [5] S. Glisic, et al., *Wireless Communications: TDMA v. CDMA*, Kluwer Academic Publishers, Boston, 1997.
- [6] P. Kuhn, et al., *Broadband Communications: Convergence of Network Technologies*, Kluwer Academic Publishers, Boston, Massachusetts, 1999.
- [7] Y. Lin, et al., *Wireless and Mobile Network Architectures*, John Wiley and Sons, New York, 2000.
- [8] G. Lorenz, et al., Characterization of attacks on public telephone networks, *Proceedings of the SPIE Conference on Technology on Law Enforcement*, Boston, Massachusetts, November 5-8, 2000.
- [9] N. Muller, *IP Convergence: The Next Revolution in Telecommunications*, Artech House, Norwood, Massachusetts, 1999.
- [10] C. Pfleeger, *Security in Computing*, Prentice Hall, Upper Saddle River, New Jersey, 1997.
- [11] M. Rozenblit, *Security for Network Telecommunications Management*, IEEE Press, Piscataway, New Jersey, 2000.
- [12] T. Russell, *Signaling System #7*, McGraw-Hill, New York, 2000.
- [13] F. Schneider (Ed.), *Trust in Cyberspace*, National Academy Press, Washington, D.C., 1999.
- [14] SecureLogix Corp., San Antonio, Texas (www.securelogix.com)
- [15] Sevis Systems, San Antonio, Texas (www.sevis.com)
- [16] The White House, *Defending America's Cyberspace: National Plan for Information Systems Protection (Version 1.0)*, Washington, D.C., 2000.

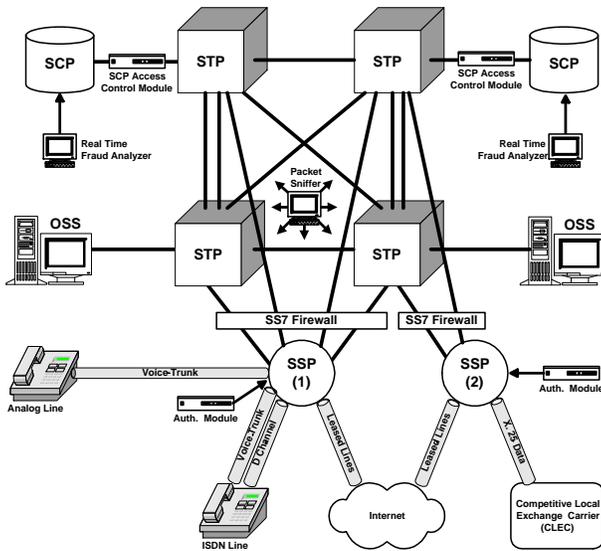


Figure 5. SS7 attack management system.

Since SSPs represent the SS7 network perimeter, authentication modules are positioned at each SSP to certify all entries. The modules detect attempts at spoofing and identity subversion by comparing SS7 messages with signatures of spoofing attacks.

SS7 packet sniffers, specially designed to read and interpret SS7 messages, are the primary information gatherers of the attack management system. The sniffers are positioned to passively monitor all signaling channels (Figure 5). They continuously transmit information to the other tools in the network.

SS7 firewalls are designed actively filter SS7 messages. As shown in Figure 5, they are positioned between SSPs and STPs to control traffic at all switching points. The firewalls screen traffic for attack signatures that are maintained in a special database.

SCPs interface with databases supporting advanced PTN services. Therefore, a real time fraud analyzer is located at each SCP. The analyzers examine SCP queries (TCAP messages) for suspicious patterns. For example, they check successive TCAP messages that seek to modify telephone numbers in call forwarding databases.

SCP access control modules work in conjunction with fraud analyzers. Positioned in front of SCPs to regulate entrance, the control modules determine whether or not TCAP messages destined for SCPs are “safe” based on their source data and information received from the corresponding fraud analyzer.

Each of the tools comprising the attack management system represents a systematic response to known SS7 vulnerabilities. Obviously, the tools and system will not completely secure SS7 networks. They will, however, help address many of the major problems facing modern public telephone networks.