SS7 Over IP: Signaling Interworking Vulnerabilities

Hemant Sengar, George Mason University
Ram Dantu, University of North Texas
Duminda Wijesekera and Sushil Jajodia, George Mason University

Abstract

Public telephony — the preferred choice for two-way voice communication over a long time — has enjoyed remarkable popularity for providing acceptable voice quality with negligible connection delays, perhaps due to its circuit-switched heritage. Recently, IP telephony, a packet-based telephone service that runs as an application over the IP protocol, has been gaining popularity. To provide seamless interconnectivity between these two competing services, the Internet Engineering Task Force (IETF) has designed a signaling interface commonly referred to as SIGTRAN. This seamless intersignaling provided by SIGTRAN facilitates any subscriber in one network to reach any other subscriber in the other network, passing through any heterogeneous maze of networks consisting of either of these. Unfortunately, the same intersignaling potentially can be exploited from either side to disrupt the services provided on the other side. We show how this can be done and propose a solution based on access control, signal screening, and detecting anomalous signaling. We argue that to be effective, the latter two should consider syntactic correctness, semantic validity of the signal content, and the appropriateness of a particular signal in the context of earlier exchanged messages.

Until recently, public telephones — the overwhelming choice for two-way voice communication — has provided acceptable voice quality with negligible connection delays. However, Voice over IP (VoIP) telephony is emerging as an alternative to public telephones, due to its convenience, cost effectiveness, and the ease of designing new services. Consequently, there has been a need to interoperate signaling and media between these two competing services. The signaling interoperation, made possible by using the signaling transport (SIGTRAN) [1] protocol suite proposed by the Internet Engineering Task Force (IETF), allows any subscriber in either network to transparently call another subscriber in either network. The malusability of the signaling interoperation and mechanisms, and possible prevention mechanisms, comprise the subject matter of our article.

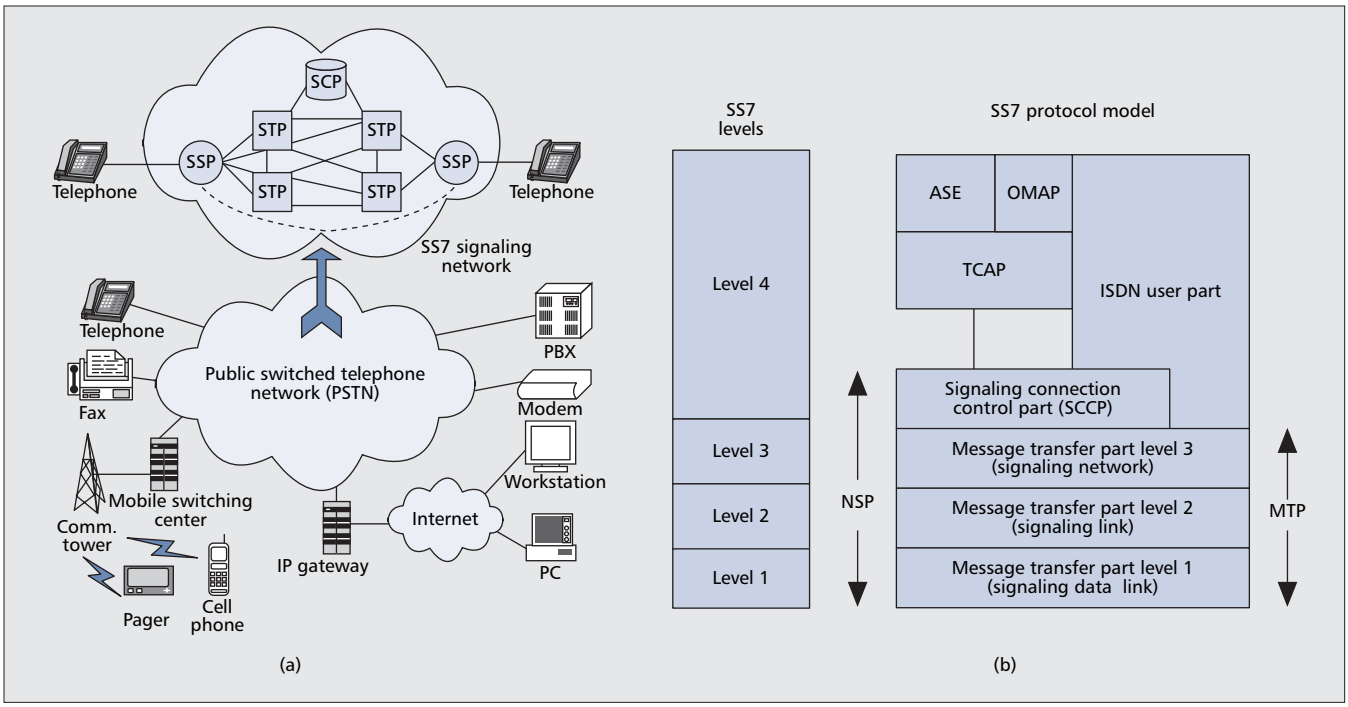
Designed in two different eras, the infrastructure of public and VoIP telephones have different networking architectures. Public telephony uses a signaling network known as Signaling System 7 (SS7) to set up and tear down connections for circuit-switched voice trunks, whereas VoIP telephony is an application running over the popular Internet Protocol (IP) — a packet switched network. Being born in an era where a few large enterprises owned and controlled the public telephony infrastructure, the SS7 network has been engineered with performance and failure tolerance in mind, but not security as a design objective. Telecommunication deregulation in 1996 [2] and liberalized economies have introduced many new players, known as competitive local exchange carriers (CLECs), thus increasing the number of access points to SS7, and thereby exposing new points for attacks. As we show herein, one such interface to both networks, SIGTRAN, can be exploited as well unless care is taken. We summarize the PSTN and VoIP infrastructures before describing how their interoperation can be exploited.

This material is based upon work supported by the National Science Foundation under grants CT-0627493, IIS-0242237, IIS-0430402, CNS-0516807, and CNS-0551694. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

Preliminaries

Public Switched Telephone Network — Current public telephone systems use separate networks for signaling and voice streams, where the former controls (itself and) the latter, referred to as common channel signaling. The combination of these two networks are commonly referred to as the public switched telephone network (PSTN), in which the control part is commonly known as Signaling System 7 (SS7). SS7 is the out-of-band signaling standard used by PSTN to control circuit-switched voice and data transmission, Integrated Services Digital Network (ISDN) services, and optionally for, cellular mobile telephony and network management. SS7 provides both circuit-related and non-circuit-related signaling. As shown in Fig. 1a, the PSTN network is connected to the wireless network through the mobile switching center (MSC) and

0890-8044/06/$20.00 © 2006 IEEE



■ Figure 1. *SS7 network architecture: a) SS7 signaling network; b) SS7 protocol stack.*

the Internet through IP gateways. Individual users and organizations access the PSTN network using dial-up, telephone, PBX, and ISDN connections.

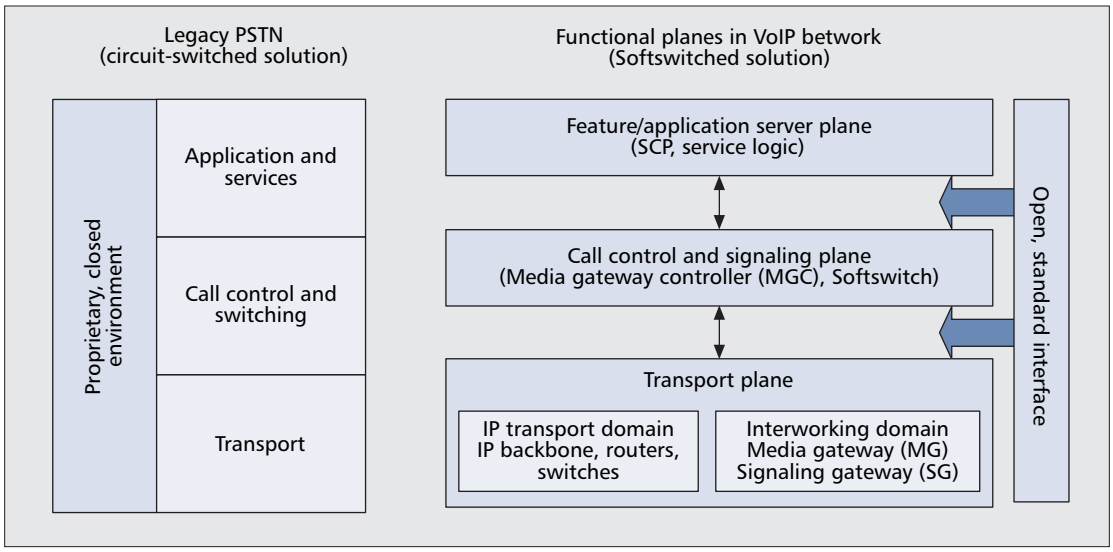
The interior of SS7 consists of three main network elements, referred to as signaling points (SPs). SPs are identified by a numeric address known as point codes, like the IP addresses of the Internet. SPs are classified as service switching points (SSPs), signaling transfer points (STPs), and service control points (SCPs), depending upon their functions in the SS7 network, as shown in the top half of Fig. 1a. In SS7 terminology, the addresses of senders and receivers are known respectively as originating point codes (OPC) and destination point codes (DPC), and are carried in a part of the SS7 message's header referred to as a routing label (RL).

SSPs are (end offices or tandem) telephone switches that originate, terminate, or switch calls. An SSP may also send a query message to an STP for logical to physical address translation, referred to as *global title translation*. SCPs contain centralized databases that store information pertinent to call-processing capabilities such as calling cards, subscriber's profiles, and mobile-station profiles. Similar to an IP-based router, based upon their DPC, STPs route incoming messages to outgoing links. STPs can also be used to screen signals and perform global title translations — mapping global mnemonic addresses to point codes.

The SS7 Protocol Stack — The SS7 protocol stack consists of four functional levels, as shown in Fig. 1b. Levels 1 through 3 together form the message transfer part (MTP) and are used for reliable point-to-point signal transfers. In addition, Level 3 provides network management functions. Level 4 represents various services (known as user parts) of MTP Level-3 (MTP3), such as telephone user parts, ISDN user parts, and signaling connection control parts. MTP is implemented at each signaling point, but the user part's implementation depends upon the services supported at that particular signaling point. STPs provide routing functions and therefore user parts are absent. The MTP3 layer routes messages across sets of MTP Level-2 (MTP2) links, controls network congestion, balances loads, and reroutes MTP2 traffic from failed links. MTP3 functions are divided into two areas, *signaling message handling*, ensuring proper delivery of messages, and *signaling network management*, managing the signaling network. The signaling connection control part (SCCP) complements MTP with the network service part (NSP) that is a functional equivalent of the Open Systems Interconnection Reference Model's network layer. SCCP supports both connectionless and connection-oriented services while enhancing the addressing scheme. The transaction capabilities application part (TCAP) is a non-circuit-related remote procedure call mechanism offering four types of transactional services: request-response, response only upon success, response only upon failure, and responseless service. Its most common use is in 800-number calling. TCAP uses SCCP as a transport layer to exchange non-circuit-related data between applications. ISDN User Part (ISUP) provides functions to support basic bearer services and supplementary services for voice and non-voice applications in an ISDN. ISUP defines messages and protocols for the controlling interexchange calls (i.e., setting up and releasing of voice trunks) between two subscribers. Further details of the SS7 protocol stack can be found in [3].

Functional Components of PSTN, VoIP and Softswitch — PSTN consists of two network planes (a plane represents a logical grouping of communication procedures), one for signaling and the other for voice transportation, that has lead to a high-level system architecture consisting of call control and media transport, which are being used to implement other applications, as shown in Fig. 2. Although legacy systems have implemented all these functional units (as shown in the left side of Fig. 2) in one physical location, the *International Packet Communications Consortium* [4] and the IETF [1] have redesigned a distributed architecture referred to as the *softswitch architecture*, as shown in the right side of Fig. 2.

The softswitch architecture has three main components: media gateway (MG), media gateway controller (MGC), and signaling gateway (SG). The MG operates at the transport plane of PSTN and is responsible for transferring voice streams from the PSTN to VoIP networks and vice versa. The MGC is responsible for call control functionality such as set-



■ Figure 2. *Softswitch architecture.*

ting up, tearing down, and monitoring end-to-end call connections, whereas MGCs control MGs using a master-slave relationship, mostly using the *Megaco* [5] protocol. SGs interface between the signaling part of the PSTN and the VoIP networks by translating between SS7 signals and (to be described below) SIGTRAN signals — namely, an adaptation layer that transports SS7 signals over IP networks.

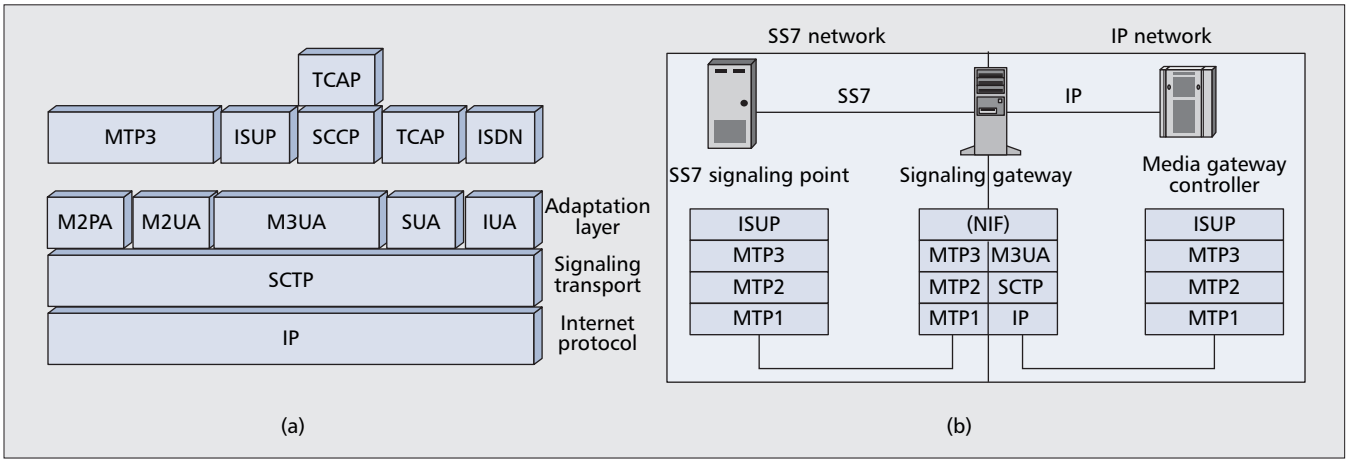
The SIGTRAN Protocol Suite: Transporting SS7 Signals over IP Networks — The SIGTRAN protocol suite proposes a new common signaling transport protocol the Stream Control Transmission Protocol (SCTP), and its adaptation sublayers that support specific primitives required by a particular application protocol of SS7 or ISDN. Figure 3a shows the SIGTRAN architecture, which consists of three components: the IP protocol, common signaling transport, and adaptation modules. By maintaining SS7 service levels with an IP routing architecture, network elements can take advantage of the cost benefits of the IP network in attempting to provide the reliability of the SS7. Many adaptation modules operating on top of SCTP provide the lower-layer services of SS7 and ISDN by means of interfaces to the upper-layer protocols and applications, and are summarized as follows.

MTP2 User Adaptation Layer (M2UA) [6]: M2UA transports MTP3 signals over SCTP and IP, instead of SS7's MTP2, and provides a way to use standard MTP3 of SS7 in IP networks. As a benefit, IP-based MGC could exchange signaling network management messages in the same way as any other network element (i.e., STP, SCP, or SSP) in the SS7 network. Figure 3a shows how MTP3 sits over M2UA in the IP-based MGC.

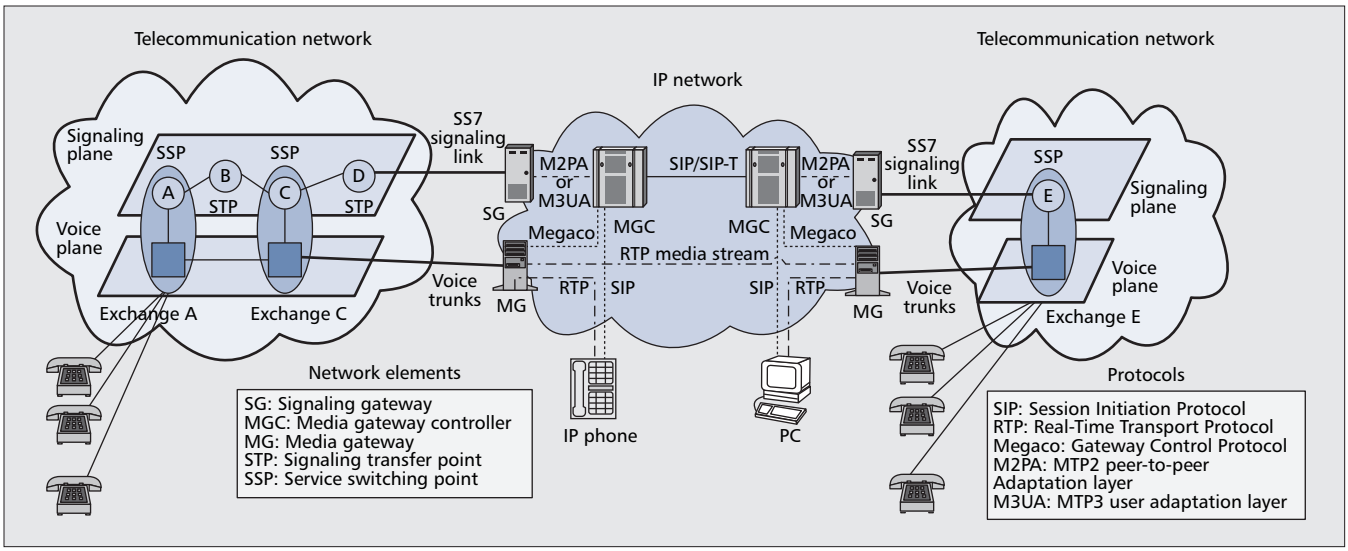
MTP2 Peer-to-Peer Adaptation Layer (M2PA) [7]: M2PA allows SS7 links to be IP-based while maintaining SS7 link topology. Service providers can maintain their SS7 network topology while taking advantage of SS7 over IP. M2PA resembles M2UA in aspects, such as allowing network management message transmission, and so on. The differences are in the network design, where SG using M2PA has its own signaling point code and acts as an IP-based STP with the flexibility of performing global title translation operation.

MTP3 User Adaptation Layer (M3UA) [8]: M3UA allows MTP3 user applications (e.g., ISUP and SCCP) in IP networks to participate at the corresponding services in the SS7 network. M3UA passes the same primitives to upper layers as MTP3 in SS7 but does not provide the total functionality of MTP3. Generally, M3UA is used between SG and MGC. Besides the user-part messages, some network management messages (M3UA does not provide full network management capability) are also delivered to the local M3UA-resident management functions of respective MGCs.

SCCP User Adaptation Layer (SUA) [9]: SUA carries transactional signaling messages (i.e., query and response type



■ Figure 3. *SS7 transportation over IP network: a) SS7 over IP (the SIGTRAN architecture); b) SS7 ISUP message over IP using M3UA.*



■ Figure 4. *Interworking of VoIP and PSTN.*

messages of the database) such as SCCP user applications, including TCAP. SUA replaces MTP and SCCP of the SS7 protocol stack for better use of IP routing. Figure 3a shows the placement of SUA on top of IP-based SCTP. Mobile Application Part (MAP), a TCAP application, uses the services of SUA in an IP-based network in the same way as SCCP is use in an SS7 network.

PSTN, VoIP Interworking Using SIGTRAN — As an example, Fig. 3b shows SS7 ISUP signaling message transportation from the SS7 SP to IP-based MGC using the M3UA SIGTRAN adaptation layer. As shown, SG implements the nodal interworking function (NIF) that exchanges IP-based MGC signals with the PSTN-based SPs. At the SG, the NIF acts as the interface between MTP3 and M3UA. SS7 messages destined to the MGC are received at the SG, the local MTP3's upper-layer interface delivers message parameters to NIF, and after translation the NIF delivers it to the M3UA's message distribution function for the final IP-based destination. Similarly, NIF reverse translates signals from MGC destined to the SS7 SP.

In addition to signaling messages, voice packets belonging to communication sessions need to be routed through the MG where PSTN's time-division-multiplexed (TDM) voice circuits are converted to an IP's packetized voice. Figure 4 shows the interworking of VoIP and PSTN networks. As shown, there are three demarcation points:

- SGs that translate signals
- MGCs that manage sessions and translate VoIP-based SIP messages to ISUP messages
- MGs that translate IP-based RTP voice streams to PSTNs voice trunks and vice versa.

Problem Statement and Organization of the Rest of the Article

Due to worldwide telecommunication deregulation, today's PSTN is open to all for a nominal fee. Therefore, telephone service providers with various levels of experience and ethics can become CLECs and subsequently have the capability to generate and inject SS7 messages. Similarly, the exponential growth of IP-based telephony will encourage Internet service providers (ISPs) to attach themselves to SS7 networks and provide IP telephony services. The adaptation layers of SIGTRAN (e.g., SUA, M3UA, M2PA, etc.) allow the possibility for an SG (Fig. 4) to appear as an STP (with its own point code) at the interface connecting IP and SS7 networks. Thus, the threats arising in either of the networks due to misprovisioned or malicious (e.g., hijacked) signaling nodes are not confined to that network alone, but may affect the other network as well.

The main contribution of this article is the identification of security threats in the interoperation of PSTN and VoIP signaling through SIGTRAN. To the best of our knowledge, this is the first effort that addresses signaling vulnerabilities in the integrated signaling network outside of the industrial sphere. Out of many adaptation modules available in the SIGTRAN protocol suite, we have chosen SUA, M3UA, and M2PA as case studies. Nevertheless, our discussion is general enough and can be extended to other adaptation modules as well.

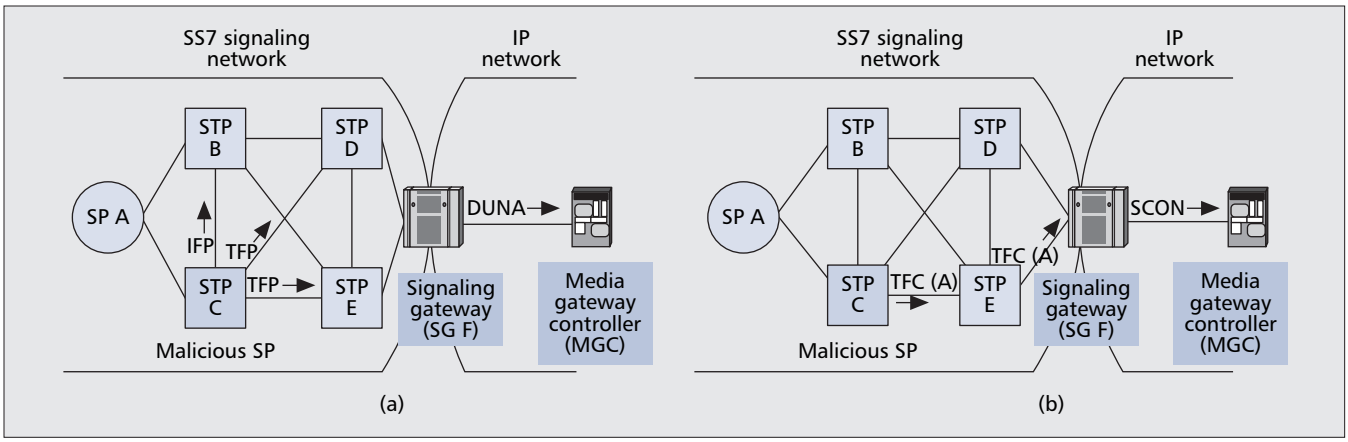
SUA is primarily used to carry transactional (i.e., TCAP) content and replaces protocol layers in the SS7 stack up to and including SCCP, thereby reducing the implementation and management complexity. M3UA is the most popular and widely deployed adaptation module used to carry SCCP, ISUP, and TCAP messages. M2PA is chosen because it maintains the SS7 network topology over IP network and acts as an SS7 link replacement. M2PA-based signaling nodes are symmetric in nature, whereas SUA and M3UA are examples of asymmetric signaling nodes.

The rest of the article is organized as follows. We present various security threats, and then describe the current status of security solutions developed so far for securing SS7 signaling network and IP-based signaling nodes. We propose a layered security solution before concluding the article.

Signaling-Message-Related Threats

In this section, we first describe various signaling messages of the SS7 network and how these are mapped into SIGTRAN messages in the IP network. Subsequently we describe various signaling-message-related threats.

Within SS7, a signal unit (SU), that is, an ordered set of parameters, is an information block that is exchanged between the SPs. Out of three types of SUs, the link-status signal units (LSSUs) and fill-in signal units (FISUs) are exchanged between MTP2 modules of adjacent SP pairs. The LSSU messages convey link-status (i.e., recovery or initialization of the link) information, whereas the FISU messages monitor the health of the links. A third type, a message signal unit (MSU), is used to carry network-management information (i.e., a message originated by MTP3 at Level-3) or MTP3 user's data



■ Figure 5. *M3UA network management messages threats originating from an SS7 network: a) DUNA message attack; b) SCON message attack..*

(i.e., a message originated by MTP3-User at Level-4) between SPs.

Within an IP network, various SIGTRAN adaptation layers follow a very generic packet format consisting of a *common header* followed by zero or more parameters that depends upon the message type, but using the standard *TLV* notation where the *tag* (i.e., an identifier of the type of the parameter), *length* (i.e., size of the parameter), and *value* (i.e., the actual information) are specified. The common header contains the adaptation layer *version*, *message class*, *message type*, and *message length*. SG maps SS7 signaling messages into a message class and a message type-5 of the common header and their parameters into relevant TLV format parameters. For the M2PA messages, the header is followed by a M2PA-specific message header and data. The *user data* type of the M2PA message contains SS7 MSU information in the message data field.

Signaling-message-related threats are due to the lack of authentication and integrity mechanism in the SS7 network, leaving open the possibility of unauthorized message content (i.e., parameters and their values) and structure manipulation.

Threats Due to Compromised Signaling Nodes

The possibility of hijacked (or compromised) signaling nodes in the SS7 or IP network can exploit the signaling messages to disrupt telephone services. In this section we describe potential threats due to various signaling messages at different levels of the SS7 protocol stack.

Level 2: Threats Due to Link-Status Messages of the M2PA Adaptation Layer — The LSSU (i.e., signaling-link control message) of the SS7 and link-status message (LSM) of IP-based signaling links are used to convey the link status between adjacent signaling nodes. LSSUs are exchanged between directly connected SPs, and in IP network, LSMs are sent between M2PA peers using SCTP associations over IP. SCTP associations are created between two IP-based signaling points (IPSPs), but are not as direct as in SS7, because there can be many devices such as routers connected between two peers. Hence in an IP network, link-status messages also need to be secured. Spoofed link-status messages such as Processor Outage, Busy, Out of Service, and so on may pose a security threat and possibly resulting in suspending signaling-link operation.

Level 3: Exploiting MTP3 Signaling Network Management (SNM) Messages — Signaling Network Management (SNM) messages are used to ensure the proper functioning of the SS7 network under abnormal conditions such as congestion, link failures, and so forth. We show how to exploit the absence of message integrity and authentication in the SS7 network. Integrity and authentication services could be provided by IP Security (IPsec), but those terminate at the SGs. Network level IPsec security services are not good enough to protect against vulnerabilities at the application level. Hijacked or misbehaving SS7 signaling nodes can still inject spurious SNM messages addressed to MGCs, aimed at disrupting VoIP services. Similarly, SNM messages generated at misbehaving SGs may affect the functioning of SS7 nodes. In this section, we discuss the vulnerabilities of SNM messages for M3UA and M2PA adaptation layers. Even with IPsec running between SGs and MGCs, IP-based signaling nodes can be compromised with some coordination between the malicious (or hijacked) signaling nodes (SS7 nodes or SGs), and the SNM messages may be used to make selected signaling links or routes unavailable, thereby causing traffic diversion to a selected route. Next we describe some sample attacks that can originate inside the SS7 signaling network targeting M3UA and M2PA-based IPSPs.

M3UA: Network Management Messages Attack — The SNM messages carrying SS7 network conditions received at an SG are conveyed to appropriate application server processes (ASPs), that is, an SCTP association's other end point configured to process signaling traffic running at IP-based signaling nodes. Some examples of ASPs are the signal handling processes running at MGCs and IP-based SCPs. The SS7 native SNM messages are converted to appropriate ASP management messages at the SGs, before being transported over the IP network. The SS7 signaling network management messages related to ASPs are defined as destination unavailable (DUNA), destination available (DAVA), destination state audit (DAUD), signaling congestion (SCON), destination user part unavailable (DUPU), and destination restricted (DRST) messages. Hijacked SS7 nodes or compromised SGs can exploit the network management messages to affect the proper functioning of a signaling network.

DUNA Message Attack: DUNA messages are sent from an SG to all concerned ASPs (i.e., MGCs) to signal the unreachability of an SG by some destinations within the SS7 network. If an MTP3-user does not find an alternate route via another SG, signal traffic (and therefore voice services) to the affected destination is suspended, thereby denying voice services. Figure 5a shows a scenario in which this message can be used to launch a denial-of-service attack. In Fig. 5a, the target SG-F has active links to STP-D and STP-E. Signaling traffic from MGC destined to SP-A can be routed through STP-D or STP-E, depending upon the employed load balancing algorithm. Now suppose a malicious SP (say, STP-C) sends a transfer prohibited (TFP) SNM signal to its neighbors STP-B, STP-D,

and STP-E, indicating its inaccessibility to SP-A. If STP-C is in their access control list, then it is authorized to initiate this process and in turn respective STPs will make appropriate modification to their routing tables, resulting in traffic diversion. Moreover, if the malicious STP-C sends another TFP signal to STP-D and STP-E on behalf of STP-B, indicating its inability to reach SP-A, then there are no routes available for SG-F to reach the destination SP-A. SG-F, being unaware of this attack, informs the MTP3-user parts about the unavailability of SP-A. Consequently, TFP and DUNA signals can be exploited to isolate SPs, divert traffic and overload routes.

SCON Message Attack: An SG realizing a route congestion to some destination in SS7 sends an SCON signal to all concerned ASPs. In response, these ASPs send a *MTP-status indication* to its local MTP3-users. The MTP3-users reduce their traffic rate towards the affected point code. In Fig. 5b we show how this can be turned into an attack scenario. Suppose that malicious STP-C sends a transfer controlled (TFC) SNM message to SG-F, indicating its route to SP-A is congested. On receipt, SG-F sends an SCON message to concerned ASPs so that M3UA passes a MTP-status primitives to its users, thus resulting in resource underutilization.

M2PA: Network Management Messages Attack — M2PA-based IPSPs have the MTP3 layer and are thus allowed to perform their *message handling* and *network management* functions as other SS7 nodes. Compromised IPSPs, hijacked SS7 nodes, or fabricated management messages are equally threatening to the functioning of the integrated signaling network.

Changeover Order Attack: Changeover procedure diverts signaling traffic from a currently unavailable (due to failure, blocking, or inhibiting) signaling link to an available alternative signaling link without loss, duplication, or missequencing of messages. This initiates changeover actions by the signaling nodes (say, SP-A and SP-B in the case of a SS7 network and IPSP-X and IPSP-Y in the case of an IP network) at both ends of the signaling link. For example, suppose SP-A sends changeover order (COO) or extended changeover order (XCO) message to SP-B. These messages say that the signaling link identified by the particular DPC/OPC/signaling-link code (SLC) parameter combination is unavailable. COO messages are used by the SS7 SPs, whereas XCO messages are used between IPSPs because M2PA uses 24 bit sequence numbers in contrast to MTP2's COO message with seven bit sequence numbers. The receiving signaling node has no mechanism in place to check the origination of this message other than to believe its RL. Currently, the only known security measure in place is an access control mechanism that specifies whether the OPC contained in messages's RL is authorized to perform such an operation. On arrival, the OPC of the message is compared with the available access control list (ACL), maintained manually by network operators at the node specifying which network management procedures are allowed and by which nodes. If the RL contains the OPC of SP-A (or IPSP-X), then it is assumed to be originating at the correct and authorized node, or else it will not be allowed to perform such network management operations. This access control mechanism is still devoid of solving fabricated message attacks towards SP-B (or IPSP-Y). For example, suppose a malicious or hijacked node SP-M (or IPSP-M) can send a fabricated network management message towards SP-B (or IPSP-Y) by spoofing the OPC of SP-A (or IPSP-X) that is authorized to send network management messages. SP-B (IPSP-Y), believing that the RL of the message will start the changeover procedure, stops sending the messages to the link specified in COO (XCO) message, thereby making the signaling link unavailable. If the victimized node is attacked with some coordination between malicious nodes, then it is possible to make believe that the selected link is unavailable, thus resulting in diverting traffic to other links and thereby wasting resources.

Level 4: Exploiting SCCP Management Messages — The SCCP management (SCMG) function maintains the smooth transferring capability of SCCP messages during network failures and SCCP subsystems downtimes. SCMG messages inform the SCCP users to stop sending any further messages and, if possible, advise SCCPs to reroute messages to other backup subsystems. At the SG, SUA layer interworks with SCMG function to interoperate between SS7 and IP networks. The SS7 SCMG messages pertaining to SS7 network conditions received at an SG are conveyed to application server processes (ASPs) running at IP-based signaling nodes after converting them to appropriate ASP management messages (such as DUNA, DRST, DUPU, and SCON messages), before being transported over the IP network.

Loss of integrity or lack of authentication of SCMG messages at SGs may be used to isolate an ASP or an SS7 node and its subsystem from an SG. For example, a DUNA message is sent from an SG to its local SUA-user at an ASP when a destination or SCCP-user becomes unreachable. The SUA-user at the ASP stops sending traffic to the affected destination or SCCP-user through the SG that sent the DUNA message. At the SG, SCMG messages originating at the SS7 side are not authenticated and therefore could be used by a hijacked SS7 node to launch a DoS attack against an ASP running at an IPSP. Similarly, a misbehaving SG at the interface or an ASP (residing at an IPSP) may be used to generate spurious management messages to affect a SS7 nodes or its SCCP subsystems.

There are various other network management procedures that may pose threats to the signaling network. The underlying problem of the lack of integrity and authentication check is common among most of them. Table 1 lists some critical management messages used by the SS7 and IP-based signaling nodes.

Threats Due to Spoofed or Fabricated Signaling Messages

SS7 network's *gateway screening* [10] is the only widely deployed security solution available today, but does not check the actual content and structure of the signaling messages. Therefore, the responsibility of parsing and interpreting the message parameters falls upon the SSPs/SCPs and IPSPs, where higher layers of the SS7 protocol stack (i.e., TCAP, ISUP, etc.) reside. Inability to interpret or properly parse messages with inappropriate contents may cause problem at the signaling node and thereby affect telephone services. As an example, consider ISUP's initial address message (IAM) populated with the multilevel precedence and preemption (MLPP) parameter that identifies the network resources to which the MLPP supplementary service is applicable. MLPP service is used by the government and emergency services on government's signaling networks. Therefore, such IAMs coming to a commercial switch may not be properly parsed. Another example is the populating circuit identification code (CIC) of the IAM message with value 0000, which may arise due to a misprovisioned CLEC's switch. Other threats affecting individual subscribers may also arise by modifying message parameters. Parameters such as automatic number identification (ANI) and *caller ID* provide essential services to the subscribers and, if spoofed, may deny these services.

Another set of potential threats arises in the environment where a part of the call involves PSTN interworking with the

SS7 protocol layer and its management messages	SS7 network management messages in IP networks	Security features
SS7 level 4: SCCP SCCP management messages: • Subsystem prohibited networks • Subsystem out-of-service request • Subsystem status test **SIGTRAN layer: SUA**	At SG, SUA layer interworks with SCCP management function and provides indications to appropriate ASPs (i.e., IP signaling nodes) by using existing ASP management messages such as: • Destination restricted (DRST) • Destination unavailable (DUNA) • Signaling congestion (SCON) • Destination user part unavailable	• Integrity and authentication mechanism across SS7 and IP networks • Protocol behavior monitoring
Message transfer part level 3 Signaling network management (SNM) messages: • Emergency changeover order • Changeover order • Transfer prohibited • Transfer controlled • Transfer restricted **SIGTRAN layer: M3UA**	At SG, M3UA layer provides interworking with MTP3 management function by using ASP management messages such as: • Destination restricted (DRST) • Destination unavailable (DUNA) • Signaling congestion (SCON) • Destination user part unavailable	• Integrity and authentication mechanism across SS7 and IP networks • Protocol behavior monitoring
M3UA message transfer part level 3 Signaling network management (SNM) messages: same as above **SIGTRAN layer: M2PA**	M2PA-based SGs and IPSPs have their own MTP3 layer, and therefore can perform all message handling and network management functions. SS7 nodes and M2PA-based IPSPs are equally vulnerable to fabricated MTP3 SNM messages.	• Integrity and authentication mechanism across SS7 and IP networks • Access control on nodes • Protocol behavior monitoring
Message transfer part level 2 Signaling link management messages • Out of alignment • Emergency alignment • Out of service • Processor outage • Busy **SIGTRAN layer: M2PA**	M2PA-based peers exchange MTP2 link status messages (similar to LSSU of SS7 network). The M2PA link is not as direct as the MTP2 signaling link. There may be many other network elements lying in the path between two M2PA peers. Fabricated link status messages pose serious threats to IPSP signaling links and nodes.	• Integrity and authentication mechanism between IPSP peers • Protocol behavior monitoring

■ Table 1. *Some critical management messages in IP and SS7 networks.*

session initiation protocol (SIP) or H.323 (an international standard for multimedia communication over packet-switched networks). For example, MGCs are used to bridge SIP and ISUP networks so that calls originating in the PSTN can reach IP telephone endpoints and vice versa, or calls originating and terminating in PSTN may go through MGCs and a SIP network in between, as shown in Fig. 4 [11]. In all these cases, SS7 to VoIP interworking is facilitated by mapping ISUP messages into SIP messages where corresponding ISUP parameters are translated into SIP headers. Consequently, lack of ISUP security can cause harm if embedded ISUPs are blindly interpreted. Directly mapping SIP headers to ISUP parameters may lead to SIP users accessing invalid or restricted numbers or selecting some carrier identification code that are restricted by PSTN policy. Unlike a traditional PSTN phone, SIP user agents (UAs) may launch multiple simultaneous requests to occupy gateway ports as a prelude to a denial-of-service attack. Many such vulnerabilities arising during ISUP-to-SIP mapping have been discussed by Camarillo *et al.* [12]. Table 2 provides a comprehensive list of vulnerable parameters across various protocol layers of SS7 protocol stack and SIGTRAN adaptation modules.

Other Miscellaneous Threats

Threats Arising Due to Eavesdropping

An intruder outside of the trust domain of an enterprise network may monitor the flow of signaling traffic to gain information such as the nature of traffic, load, and network topology besides the behavior and identity of subscribers. For example, SIP messages between MGCs (Fig. 4) contains topological information in their header fields, such as Via and Record-Route. Similarly, the Protocol Data parameter of M3UA and the User Data field of M2PA messages contain the point codes of SS7 signaling nodes and subscriber specific data. Data recorded from such traffic can be used later on to mount attacks on a specific user or the network itself. As a result, there is a need to mask the routing information and the callee's and caller's identity, and disguise traffic flow.

Threats Arising Due to Authenticated, but Misbehaving Nodes

As stated above, SPs in an SS7 network are uniquely identified by their point codes, and IPSPs in IP networks are identified by their IP addresses. In M2PA-based IPSPs, the MTP3 layer is adapted to SCTP using the M2PA adaptation layer in IP networks. MTP requires that each signaling node with a MTP3 layer be identified with a point code. Thus, M2PA-based IPSPs have two identifiers, first their IP addresses (i.e., as a SCTP-based multihomed host) and second, their SS7 point code. In case of M3UA, SGs also have a point code address. Now, a security threat arises if IP addresses of a multihomed signaling node are not properly bound with its corresponding point code. Although IPSPs may run IPsec between them, and it authenticates two peers based on IP addresses, not on their point codes. Consequently, it is possible that an authenticated IPSP may lie about its true point code to gain undue advantages, such as

Protocol layers	Parameters of SS7 and SIGTRAN messages to be screened
SS7 layer: ISUP **SIGTRAN modules: M3UA, M2PA**	• Validity of circuit identification code, allowed optional parameters, presence of all mandatory parameters, permissible parameters and its value, and permissible *message type* • SIGTRAN message type and its allowed parameters (validity of tag-length-value) (in case of M2PA, *user data* field is screened) **Reasons:** Misprovisioned switches may fail to parse and/or interpret parameters properly **Security implementation:** SG firewall checks syntax and semantics of messages, trust management, and service level agreements — only allowed parameters and values are permissible
SS7 layer: TCAP **SIGTRAN modules: mainly SUA**	• Checking *component portion*, *component type*, *operation code*, *parameter code*, etc. • Permissible parameters and their values, presence of all mandatory parameters • SIGTRAN message types and their allowed parameters (validity of tag-length-value) **Reasons:** Switch may fail to parse and/or interpret parameters properly Messages may be used to control and regulate the switch, example: automatic code gap validity of *request* and *response* messages **Security implementation:** SG firewall checks syntax and semantics of messages, trust management, and service level agreements — only allowed parameters and values are permissible
SS7 layer: SCCP **SIGTRAN modules: mainly SUA**	• Calling and called party addresses, global title address, and *translation type* • Affected point code, subsystem numbers (SSNs), etc. • SIGTRAN message type and its allowed parameters (validity of tag-length-value) **Reasons:** Switch may fail to parse and/or interpret parameters properly; routing depends on proper addresses; SCCP management messages maintain subsystem of a node **Security implementation:** SG firewall checks syntax and semantics of messages, trust management, and service level agreement — only allowed parameters and values are permissible
SS7 layer: MTP3 **SIGTRAN modules: M3UA, M2PA**	• Permissible values in SIO, OPC, DPC fields of the signaling messages • Permissible *message type*, *H*0/*H*1 code of network management messages • SIGTRAN message type and its allowed parameters (validity of tag-length-value) (in case of M2PA, *user data* field is screened) **Reasons:** Switch may fail to parse and/or interpret parameters properly, spoofing OPC involves fraud, network management messages control switch functions, because dynamic updating of routing table is possible at STPs **Security implementation:** SG firewall checks syntax and semantics of messages, trust management, and service level agreement — only allowed parameters and values are permissible
SS7 layer: MTP2 **SIGTRAN modules: M2PA**	• *Message Length* field of M2PA message is consistent with the message's actual length • Similarly, *LI* field value of MTP2 and actual length of the message is consistent • Consistency of ssequence numbers, FSN and BSN **Reasons:** Inconsistent message construction **Security implementation:** SG firewall

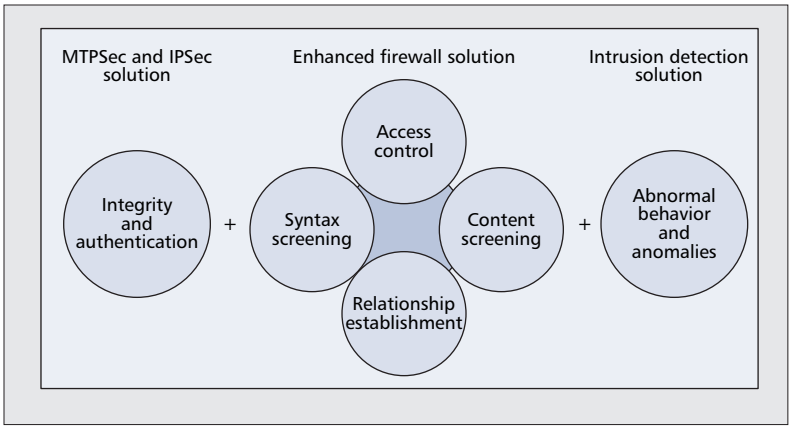
■ Table 2. Message content and structure screening at signaling gateways.

send signaling traffic posing as some other nodes, or start network management procedures posing as an authorized node to send these network management messages. For example, an M2PA node can send User Data messages with spoofed OPC to another peer node, though the link between both nodes is secured with IPsec.

Threats Arising Due to Violation of Protocol State Machines

Exploits related to violation of protocol state machines arise when a peer signaling node behave abnormally. For example, before an SCTP association (i.e., link) can be opened to carry signaling traffic, the link alignment procedure verifies its suitability as an SS7 signaling link. As part of the procedure, for a specified time, say $T4$ (≈ 8 s), *link-status proving* messages are exchanged between two ends of the SCTP association and monitored for the transmission errors at either end. This procedure of ensuring the suitability of the link is referred to as proving. If both ends of the link maintain their alignment for a period $T4$, they start sending *link-status ready* message to verify that both ends have completed *proving*. In the case when one side is aligned, then it starts a timer $T1$ (≈ 40 s) and continues sending a link-status ready message to the peer node while waiting for a link-status ready or *link-status processor outage* message from the other side. Now suppose at the expiration of $T4$ the remote M2PA node still continuously sends link-status proving messages without any *ready* message; then it exhibits an abnormal behavior.

Similarly, for a call-connection setup there is a predefined sequence of messages to be exchanged between two signaling end points. For example, to set up a call, the caller sends an initial address message (IAM) as a first message. In return, the callee sends address complete message (ACM) and answer message (ANM) to indicate that the called subscriber's phone is ringing and is picked up, respectively. At the end of the call, a release message (REL) and a release complete message (RLC) are sent in that order to release the connection and free the resources held at the switch. For a particular voice trunk, if an SP or an IPSP sees an REL message without first seeing an IAM message, then this exchange of messages are considered as a violation of the protocol state machine specification. Similarly, TCAP query and response messages should have a relationship between them, where a response message without any correlated request should be considered as an abnormal behavior.



■ Figure 6. *Security services provided by the proposed solution (at the SG).*

Current Status of Telecommunication Security Solutions

Telcordia's Gateway Screening Specification

The Telcordia specification [4] provides limited screening capability, implemented at gateway STPs, to weed out inappropriate and harmful ingress signals, referred to as *gateway screening*. Generally, gateway screening screens only message headers, except if the message type is *network management message*, that is, then it checks the message content fields such as *message type* and *affected destination* parameters. Realizing the need for enhanced security measures, Telcordia later incorporated screening ISUP and SCCP messages for specific message types and some *message priority* fields. Generally, gateway screening checks the OPC and DPC of the messages to determine whether it should be allowed to enter through the ingress point of the network. Because this capability does not check the content of the other higher layer protocols of SS7 (such as ISUP, TCAP, etc.), the responsibility falls upon the SSPs, SCPs, and IPSPs (i.e., the nodes which have higher layer protocols) to do so.

Other Academic and Industrial Work

On the academic side, in 1998, Sailer [13] proposed enhancing existing network service interfaces by standardizing security service interfaces at the application level to enable the provisioning of open security services. Lorenz *et al*. [14] and Moore *et al*. [15] analyzed the vulnerabilities in the SS7 network and presented an attack taxonomy. Sengar *et al*. [16] proposed MTPSec, a component at the MTP3 layer providing link-by-link security in the SS7 network.

On the industrial side, many recent commercial products are emerging to secure SS7. For example, the *InteleGuard firewall* [17] solution by Sevis Systems captures signaling messages directly from SS7 links, analyzes them based on policies activated by service providers: filter, modify, monitor and/or alert on specified SS7 signals. They go beyond traditional gateway screening by having content-based filtering. Verizon's SS7 Security Gatekeeper [18] provides a content and structure-based firewall. Tekelec's EAGLE STP gateway screening (GWS) [19] provides access control and screening of ingress and egress signals for MTP and SCCP.

IETF's Approach

IETF's SIGTRAN working group has proposed IPsec and transport-layer security (TLS) for the security of signaling messages traveling on SIGTRAN over SCTP links [20]. SS7 signaling links still remain untouched by International Telecommunication Union (ITU) and are devoid of any security solutions. The IPsec security mechanism existing between (SG, MGC) and (MGC, MG) defines two protocols, Authentication Header (AH) and Encapsulating Security Payload (ESP), which essentially provide security and confidentiality.

Proposed Security Solution

Securing intersignaling between PSTN and VoIP requires addressing protocols that operate on either side. On the VoIP, IP is the most dominant network layer protocol and IPsec is the most commonly recommended solution to provide security services in all of the SIGTRAN adaptation layers. In the SS7 network, MTP3 is the network layer protocol, which is devoid of any network level security services. To fill the gaps, Sengar *et al*. [16] proposed MTPSec — an IPsec solution for the MTP3 layer of the SS7 network, providing the same security services irrespective of the differences in the protocols and networks. Both sides of the interface thus provide authentication and integrity services to the signaling messages carried through.

Another security threat arises due to misbehaving or hijacked network entities. An incorrect signaling message (i.e., a message which does not satisfy a message's syntax, the content of the parameters, or its relationship with the previously exchanged messages) in the network, whether intentional or accidental, could cause denial-of-service attacks and may even bring down a networking element. To avoid integrated signaling network vulnerabilities, we propose a comprehensive layered security solution. Figure 6 shows three essential parts of our security solution. The *enhanced firewall* solution is implemented at the SG. *Syntax screening* allows only standard messages to pass through, *access control and content sscreening* enforces the access control rules and checks for permissible parameters and its values to pass through, thereby further restricting syntactically allowed messages. Those messages which have passed through both these screenings may still not be correct if they are out of sequence. *Relationship establishment* establishes a relationship between the exchanged messages and identifies the messages which are not part of the regular call establishment process.

Finally, the *intrusion detection* part of the proposed layered security implementation, monitors abnormal behavior at the protocol level. The protocol state machine is built from the specification, and is used to derive legitimate states and transitions. Our protocol state machine-based intrusion detection can be considered as a variant of the anomaly-detection mechanism, which classifies a deviation from legitimate state transitions as a suspicious attack [21, 22].

Conclusions

With the growing acceptance of the SIGTRAN protocol suite for transporting SS7 signals across IP networks, there is a need to secure both SS7 and IP networks. Still, most of the focus is on securing the public IP network, leaving SS7 network vulnerable and the signaling gateway virtually untouched. One reason for this disequilibrium may be the folklore that the *telephone network is secured enough and, consequently, there are no threats*. We argue the opposite, by showing some example exploits of fabricated messages or malicious (hijacked) signaling nodes. Even misconfigured SGs, STPs, SSPs, and MGCs can generate spurious messages and consequently affect other signaling nodes by shutting them down or by functioning erratically. To avoid such security problems, we propose MTPSec, IPsec, and *enhanced firewall* combined with

intrusion detection as a solution. MTPSec provides a much desired solution to the integrity and authenticity problem in the SS7 network.

References

[1] L. Ong *et al.*, RFC 2719: Framework Architecture for Signaling Transport, IETF Network Working Group, Oct. 1999.
[2] FCC, Telecommunications Act of 1996, Report 110 Stat. 56, Pub. LA. no. 104–104, 1996.
[3] J. G. van Bosse, *Signaling in Telecommunication Networks*, New York: Wiley, 1st edition, 1998.
[4] IPCC. Reference architecture, Technical report, International Packet Communications Consortium, June 2002, www.packetcomm.org
[5] C. Groves *et al.*, RFC 3525: Gateway Control Protocol Version 1, IETF Network Working Group, June 2003.
[6] K. Morneault *et al.*, RFC 3331: Signaling System 7 (SS7) Message Transfer Part 2 (MTP2): User Adaptation Layer. IETF Network Working Group, Sept. 2002.
[7] T. George *et al.*, RFC 4165: Signaling System 7 (SS7) Message Transfer Part 2 (MTP2)-User Peer-to-Peer Adaptation Layer (M2PA). IETF Network Working Group, Sept. 2005.
[8] G. Sidebottom, K. Morneault, and J. Pastor-Balbas. RFC 3332: Signaling System 7 (SS7) Message Transfer Part 3 (MTP3) — User Adaptation Layer (M3UA). IETF Network Working Group, Sept. 2002.
[9] J. Loughney *et al.*, RFC 3868: Signaling Connection Control Part User Adaptation Layer (SUA), IETF Network Working Group, Oct. 2004.
[10] GR-82-CORE, Signaling Transfer Point (STP) Generic Requirements, Technical report, Telcordia, Morristown, New Jersey, 2001.
[11] A. Vemuri and J. Peterson, RFC 3372: Session Initiation Protocol for Telephones (SIP-T) Context and Architectures, IETF Network Working Group, Sept. 2002.
[12] G. Camarillo *et al.*, RFC 3398: Integrated Services Digital Network (ISDN) User Part (ISUP) to Session Initiation Protocol (SIP) Mapping. IETF Network Working Group, Dec. 2002.
[13] R. Sailer, "Signaling and Service Interfaces for Separating Security Sensitive Telecommunication Functions Considering Multilateral Security," *6th Open Workshop on High Speed Networks*, Stuttgart, Oct. 1997.
[14] G. Lorenz *et al.*, "Securing SS7 Telecommunications Networks," *Proc. 2001 IEEE Wksp. Info. Assurance and Security*, West Point, NY, June 2001.
[15] T. Moore *et al.*, "Signaling System (SS7) Network Security," *45th Midwest Symp. Circuits and Systems*, vol. 3, Aug. 2002, pp. 496–99.
[16] H. Sengar, D.Wijesekera, and S. Jajodia, "MTPSec: Customizable Secure MTP3 Tunnels in the SS7 Network," *19th Int'l. Parallel and Distributed Processing Symp. Wksp. 17*, IPDPS, 2005.
[17] SEVIS Systems, "InteleGuard Signaling Firewall," White paper, 2001, http://www.sevis.com/inteleguard.htm
[18] Verizon, "SS7 Security Gatekeeper," Request for information, Verizon Communications, May 2002.
[19] TEKELEC, "Tekelec EAGLE STP," White paper, 2001, http://www.tekelec.com/productportfolio/eagle5sas/
[20] J. Loughney, M. Tuexen, and J. Pastor-Balbas, "RFC 3788: Security Considerations for Signaling Transport (SIGTRAN) Protocols, "IETF Network Working Group, June 2004.
[21] R. Sekar *et al.*, "Specification-Based Anomaly Detection: A New Approach for Detecting Network Intrusions," *ACM Comp. and Commun. Security Conf. (CCS)*, Washington DC, Nov. 2002.
[22] H. Sengar *et al.*, "VoIP Intrusion Detection Through Interacting Protocol State Machines," *IEEE Dependable Systems and Networks Conf. (DSN 2006)*, June 2006.

Biographies

HEMANT SENGAR (fhsengar@gmu.edu) is a Ph.D. student at George Mason University, Fairfax, VA, in the Department of Information and Software Engineering. He received an M.S. degree from the same university and a B.Tech. degree from Indian Institute of Technology, Kanpur. His current research interests are in the area of IP telephony and telecommunication networks security.

RAM DANTU (rdantu@unt.edu) has 20 years of experience in the networking industry, where he worked for Cisco, Nortel, Alcatel, and Fujitsu and was responsible for advanced technology products from concept to delivery. For the last five years, he has been researching in preventing DOS and spam attacks in VoIP networks. In recognition, he received five NSF awards during the past one year. He has co-chaired three workshops in VoIP security. He is currently an assistant professor in the Department of Computer Science and Engineering at the University of North Texas (UNT). His research focus is on detecting spam, network security, and next generation networks. Prior to UNT, he was Technology Director in Netrake where he was the architect of the redundancy mechanism for VOIP firewalls. His additional experience includes Technical Director in IpMobile(acquired by Cisco) where he was instrumental for the wireless/IP product concept, architecture, design and delivery. In addition to more than 50 research papers, he has authored several RFCs related to MPLS, SS7-over-IP, and Routing. Due to his innovative work, Cisco and Alcatel were granted a total of eight patents and another ten are pending.

DUMINDA WIJESEKERA (dwijesek@gmu.edu) is an associate professor in the Department of Information and Software Engineering at George Mason University, Fairfax, VA. During various times, his research interests have been in security, multimedia, networks, secure signaling (telecom, railway and SCADA), avionics, missile systems, web and theoretical computer science. He holds courtesy appointments at the Center for Secure Information Systems (CSIS) and the Center for Command, Control and Coordination (C4I) at George Mason University, and the Potomac Institute of Policy Studies in Arlington, VA. Prior to GMU he was at Honeywell Military Avionics, Army High Performance Research Center at the University of Minnesota, and the University of Wisconsin. His doctorates are in Computer Science and Logic from the University of Minnesota and Cornell University in 1997 and 1990, respectively.

SUSHIL JAJODIA (jajodiag@gmu.edu) is BDM International Professor of Information Technology and director of Center for Secure Information Systems at George Mason University, Fairfax, VA. He received a Ph.D. from the University of Oregon, Eugene, OR. His research interests include information security, temporal databases, and replicated databases. He has authored five books, edited 24 books and conference proceedings, and published more than 300 technical papers in the refereed journals and conference proceedings. The URL for his web page is http://csis.gmu.edu/faculty/jajodia.html