# Securing VoIP and PSTN from Integrated Signaling Network Vulnerabilities

Hemant Sengar† Ram Dantu‡ Duminda Wijesekera†

†Center for Secure Information Systems
George Mason University
Fairfax, VA 22030
{hsengar,dwijesek}@gmu.edu

‡Network Security Laboratory
University of North Texas
Denton, TX 76201
rdantu@unt.edu

***Abstract*— The liberalization of public switched telephone network (PSTN) and growing acceptance of SIGTRAN protocol suite have introduced new and yet to be trusted signaling entities. Thus security threats emerging from one network not only affects itself but other network also. We show how this integrated signaling environment can become a security threat to emerging VoIP and PSTN networks. We propose a security solution as a fix. Our proposal goes beyond "Gateway Screening" and "SS7 Gatekeeper" proposed by Telcordia and Verizon respectively to defend vulnerable SS7 network.**

## I. Introduction

A study done by the National Research Council's Committee on Information Systems Trustworthiness in 1999 states that *vulnerabilities in the [PSTN] can affect the Internet, and vulnerabilities in the Internet technology can affect the telephone network*. IP telephony is emerging as a viable alternative to traditional wired and wireless telephone systems, commonly referred to as *public switched telephone network* (PSTN). They have different networking architectures, VoIP uses IP, a packet switched network and PSTN uses circuit switched network where a signaling network known as *signaling system number 7* (SS7) sets up connections for voice trunks. SS7 being designed in an era where few large companies controlled the entire network, and therefore were the only entities entitled to inject messages into it. But the telecommunication deregulation act of 1996 [5] in the USA and liberalization of economies in other countries have changed this situation. Because the close knit community of old SS7 users had complete trust in each other, SS7 was engineered for performance and failure tolerance in mind, but not the security. New players in the market and with the convergence of IP and other networks which provide numerous entry points at the interface brings along with many vulnerabilities. These vulnerabilities are not only confined to SS7 network or IP network in isolation but extends to SS7 nodes and SIGTRAN based IP signaling points (IPSPs) as well. Our work first tries to identify security threats and presents secured signaling architecture to the vulnerable integrated signaling network.

## II. Background

Signaling System 7 (SS7) is an out-of-band signaling standard for the telephone network developed by the *international telecommunication union* (ITU-T), and defines the protocols stack of its signaling network. It meets the requirements of call control signaling for telecommunication services such as telephone, ISDN and circuit switched data transmission services. Besides, it can also be used for other services such as intelligent network, cellular mobile telephony and network management. Individual users and organizations access the PSTN network using Dial-Ups, PBXs and ISDN connections. The interior of the network consists of three main *network elements*. These are *service switching points (SSPs)*, *signaling transfer points (STPs)* and *service control points (SCPs)*. Network elements or signaling points (SPs) in PSTN are identified by address called *point codes*. Point codes are carried in routing labels (RL) contained in each messages exchanged between the *network elements*. Routing labels have the originating point code (OPC) and destination point code (DPC) of a message. *Network element* uses its routing table to select appropriate signaling route for the messages. These *network elements* are arranged throughout the SS7 network in such a way that the network provides the maximum performance, reliability and flexibility. The SS7 protocol stack consists of four functional levels. Levels 1 to 3 together form the *Message Transfer Part* (MTP) and are used for reliable point-to-point transfers. Level 3 also provide network management functions. Level 4 represents users of MTP3. Examples of the user parts include telephone user part (TUP), the ISDN user part (ISUP), the data user part (DUP) and the signaling connection control part (SCCP). MTP is implemented at each signaling point but user parts are implemented only depending upon the services supported at the signaling point. STPs provide routing functions and therefore user parts are absent. Detailed description of the SS7 protocol stack can be found in [1], [2].

With the emergence of Voice over IP (VoIP), there is a transition underway from SS7 based circuit switched networks to IP based data network. In this transitional period both IP and traditional telephony network will interoperate and co-exist. At the interface, *Gateway* network elements provide interoperability by accepting signals and media delivered through a protocol operation on one side of the network and converts into appropriate protocol operational on the other side. For signaling transportation, IETF developed a SIGTRAN protocol

1-4244-0144-5/06/$20.00 ©2006 IEEE

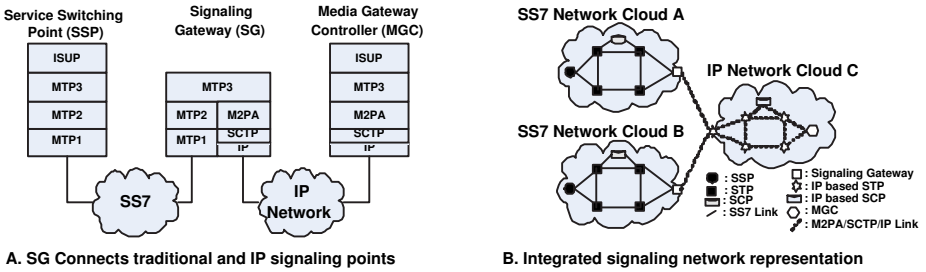



Fig. 1. M2PA in Signaling Transport Architecture

suite consisting of three components, standard IP transport, common signaling transport and adaptation module. A new proposed common signaling transport protocol (Stream Control Transmission Protocol (SCTP) [18]) supports a common set of reliable transport functions for signaling transport and an adaptation sublayer that supports specific primitives required by particular application protocol of SS7 or ISDN. There are a number of adaptation modules operating on top of SCTP, providing an interface to the upper layer protocols and applications. These modules provide lower layer services of SS7 and ISDN in a way that upper-layer protocols and applications do not realize that underlying transportation is IP based instead of traditional MTP of SS7 protocol suite. Out of these adaptation modules, in this paper we study *MTP2 Peer to Peer Adaptation Layer* (M2PA) because it maintains the SS7 network topology over IP network. M2PA supports the transportation of MTP3 messages over SCTP/IP, and allows full MTP3 messages handling and network management capabilities between two IPSPs in contrast to other adaptation modules that do not provide full network management capability. Therefore M2PA based nodes acts just as traditional SS7 nodes retaining MTP3/MTP2 (MTP2-User) interface and use IP Network instead of SS7 links. Figure 1 (A) shows how M2PA adaptation layer is used in signaling. M2PA based signaling nodes have MTP3 layer and hence can be represented by a point code. Signaling node devoid of MTP3-User parts act as an IP based STP and with the presence of user parts such as SCCP/TCAP or ISUP it may act as SCP or SSP etc.

## III. Signaling Nodes are Exposed to Attacks

Due to world-wide telecommunication de-regulation, the PSTN is open to all for a nominal fee. Therefore any body with a different level of experience and ethics can become a competitive local exchange carriers (CLECs) and hence have the ability to generate SS7 messages and put into the SS7 core or IP based signaling nodes. Signaling nodes are vulnerable to fabricated signaling messages, if they are unable to interpret or parse the spoofed messages properly. Another set of threats are arising in the environment where part of call involves PSTN interworking with *session initiation protocol* (SIP). Media gateway controllers (MGCs) are used to bridge SIP and ISUP networks so that calls originating in the PSTN can reach IP telephone endpoints and vice versa. In another case when a call is originating at one PSTN and terminating at another PSTN may also use two MGCs and SIP network in between [21]. In all these cases this interworking is possible by translation of ISUP messages into SIP messages and the mapping of ISUP parameters into SIP headers. Lack of ISUP security may pose some risks if embedded ISUP is blindly interpreted. Directly mapping of SIP headers to ISUP parameters may lead to SIP users accessing invalid or restricted numbers or selecting certain carrier identification code that is restricted by the PSTN policy. Unlike a traditional PSTN phone, SIP user agent may launch multiple simultaneous requests to occupy gateway ports as part of denial-of-service attack. Camarillo et al. [3] have discussed many such vulnerabilities arising during ISUP to SIP mapping. Signaling network management (SNM) messages are used to keep the network running and functioning properly under abnormal conditions such as congestion, link failures etc. These messages are critical to the health of the signaling network. The lack of integrity and authentication mechanism in the SS7 network can be exploited to launch many attacks by using SNM messages. Though IPSec can provide authentication and integrity security services but these services ends at the signaling gateway. Hijacked or misbehaving SS7 signaling nodes can send malicious SNM messages towards other signaling nodes (i.e. STP) or towards MGC or another IPSP. With some coordination between malicious nodes, it is possible to :

- Make various signaling links unavailable.
- If no alternative signaling link exists for signaling traffic towards one or more destinations, the concerned destination(s) are declared inaccessible.
- Make some routes unavailable.
- Diverting traffic to some particular route as expected by the hijackers.
- Diverting traffic to alternative available signaling links leads to more resources utilization.
- May require signaling link or signaling link set activation procedure to be started, consuming more resources.

An intruder outside of the trust domain or enterprise may monitor the traffic flow. Traffic flow analysis provides information such as nature of traffic, load and network topology besides subscribers behavior and its identity. This information later on can be used to mount attack on the specific user or the network itself. SS7 signaling points of SS7 network are

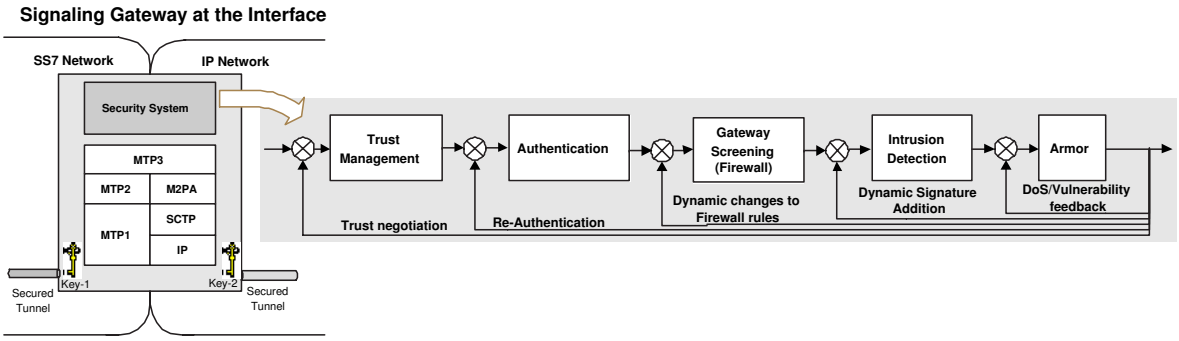



Fig. 2. Secured Signaling Gateway Architecture

uniquely identified by their *point codes* and in IP network IPSPs are identified by their IP addresses. Because MTP3 layer is adapted to SCTP using M2PA in IP network and MTP requires that each node with a MTP3 layer is identified by a SS7 point code. Therefore, M2PA based IPSPs have two identifiers, one is its IP addresses and the other one is its SS7 point code. Now a security threat arises if we don't properly bind the IP addresses of a node with its corresponding point code. IPSPs may have IPSec as a security measure between them, and it authenticates two peers based on its IP addresses but not on its point code. So, still it is possible that an authenticated IPSP may spoof its outgoing message's routing label.

## IV. Security Goals

The previous section describes some threats that arise either due to incorrect messages, abnormal behavior of protocol state machine or the lack of authentication and integrity checks. We therefore focus on these threats and define our main security goals in this analysis. Integrity without authentication is insufficient to avoid the security breaches in our examples. Thus the purpose of authentication in this paper is to maintain integrity and authorized messages flow across signaling nodes.

> **1. Authentication Goal :** A message *m*, protected by an authentication goal, ensures that if a node in *subnetwork A* is declared to be the originator of the message *m* and received by another node in *subnetwork C*, then *m* actually originated by the claimant and the payload received at node in *subnetwork C* is the same as sent by the originator.

Our secondary and equally important security goal is to detect and prevent spurious and fabricated signaling messages. Message's well-formedness requires that it's structure is syntactically correct and content is right. Syntactically correct means that the message is encoded according to ITU-T/ANSI/IETF-M2PA specification. Message's *content* is about *message type*, *message parameters* and *parameter values* allowed in these messages. The distinction between the former and the latter is that here message may be syntactically correct but still it can be treated as an invalid message if it contains any parameter and parameter-values that are not allowed as per service level agreements between two *sub networks*. For example, *User-user Information* is a variable length optional `IAM` parameter used in countries that offer user-to-user signaling of ISDN users. The parameter contents are not specified by ITU-T, and are coded as agreed by individual user pairs [2]. Generally carrier service providers in USA, mutually agree to prohibit use of this parameter, so any `IAM` message containing this parameter is syntactically well formed but still considered incorrect.

> **2. Message's Correctness Goal :** A message $m$ received from an authorized node, is said to be syntactically correct if array of header fields and the array of parameters for that message type is as per specification. Message $m$ is content-wise correct if the content of both the arrays are allowed ones.

Finally, our third security goal is to identify and prevent violation of protocol state machine. Authenticated and authorized nodes, whether it is SS7 node or IPSP, may behave improperly by injecting unauthorized messages into the network with the aim of breaking the agreed upon protocol. A peer node receiving an inaccurate message from an authenticated and authorized node may detect its inaccurateness by maintaining protocol state transitions and call state information of the received messages.

> **3. Behavior Compliance of Protocol State Machine Goal:** A well-formed message $m$ received from an authorized node is contextually correct, if it brings right protocol state transition.

## V. Secure Signaling Architecture

While developing the secure signaling architecture, we have considered only the case of Figure 1(B) trust set relationship. Cloud A, B and C are three different trust sets, joining each other through the interface by signaling gateway (represented by □). The signaling nodes internal to the clouds are connected through secure tunnels which provide message authentication and integrity security services. At the interface, joining nodes of two different trust sets are connected through a secured tunnel, thus providing security services throughout the signaling network irrespective of being SS7 or IP network. Figure 2

shows signaling gateway equipped with a comprehensive security system implementation which consists of components such as firewall, intrusion detection system (IDS), trust and authentication mechanism etc. Though for simplicity, we have shown SS7 signaling link and IP link as *Secured Tunnel* but both are achieved using separate processes and using different session keys. IDS maintains call state information and observes protocol state behavior. In the next few sections we describe the design details of the proposed secured gateway architecture.

### A. Security Implementation across Protocol Layer

When we think of security implementation across protocol layers then we have to take consideration of the protocols operating in two different networks namely SS7 and data network. In data network, IP is the most predominant network layer protocol thats why in all the IETF's SIGTRAN related RFCs, we find IPSec as a recommended solution to provide security services. In the SS7 network, MTP3 is the network layer, but is devoid of any network level security services. To fill the gaps, MTPSec [16] is proposed for the SS7 side which is akin to the IPSec to provide same security services irrespective of differences in the protocols/networks. In this paper we show how to use MTPSec in SS7 network and IPSec in IP network for achieving authentication and integrity security services throughout the integrated signaling network.

*1) MTPSec : Secure MTP3 tunnels in SS7 network:* Figure 3 a.) shows how the MTP3 layer is divided into two main group of functions. First group, *Signaling Network Management* (SNM) minimizes disruptions in the signaling network and the other group, *Signaling Message Handling* (SMH) ensures that a message originated by a user-part is delivered to the same user-part at the destination node. MTP3's SMH is further subdivided into three subgroup of functions : message discrimination, message distribution and message routing. One more subgroup of functions, namely, *message transfer part security* (MTPSec) is added in SMH to provide message authentication and integrity security services. Figure 3 a.) shows the placement of this group with others in SMH part of MTP3 layer.

Proposed MTPSec component can provide link-by-link security in the SS7 network provided all the SPs in the network have MTPSec component in place. Alternatively it can be deployed at the edges of two different trust sets. Flow of messages using the services of MTPSec component in one SP to another SP is called *tunnel*. Proposed secure MTP3 tunnels between SPs and to SG (MTP3 at SS7 network side) are created using a *key exchange (KE)* and *authentication header (AH)* protocol as in IPSec. KE protocol identifies and negotiates key parameters between two MTP3 ends to set up a pair of tunnels between them. The AH protocol provides the framework for authenticating and checking the integrity of exchanged messages. The proposed placement of this part (i.e. AH) is at between the routing label and the user message (UM) part as shown in Figure 3 b.).

Here we briefly describe the operational details of MTP3 in the presence of MTPSec component. Further details about the MTPSec can be obtained from Sengar et al. [16]. MTPSec maintains security association (SA) data for each active signaling data link. SA contains all the negotiated information such as the hashing algorithm and shared key etc., between two ends. Each transmission channel (upstream and downstream) in a signaling link has its own SA. In the following paragraphs we show how MTPSec handles MTP3 packets.

**Messages coming from MTP3 or Above (User-parts)**

1) As in the case of MTP3 without security, first the *message routing* function determines the signaling link that is to be used. This function is responsible for load balancing the active set of MTP2 links. The resulting link and the payload is sent to the *MTP Security* module (see Figure 3 a.).
2) MTPSec looks up the SA for corresponding link and retrieves the hashing algorithm and keys. It uses the *message type* and SI value to determine the parameters to be hashed. It creates a hash of the parameter values in the AH's *authentication data field* and writes the packet to the *output buffer* (OB) of MTP2 in the selected MTP2 link.

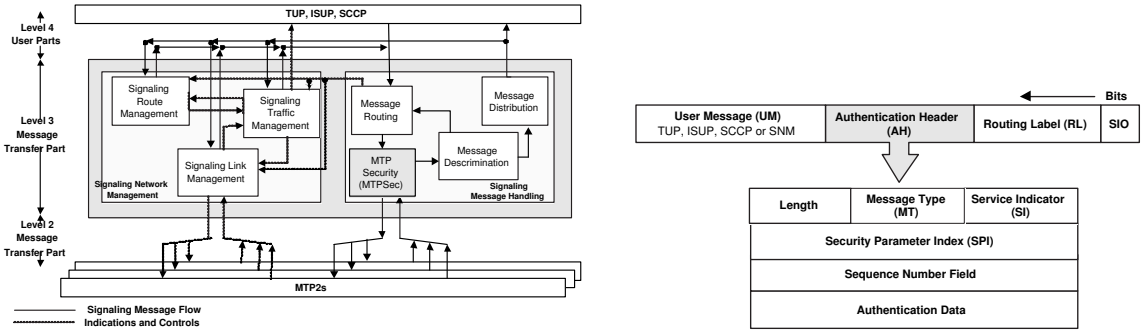
**Messages Coming Up from MTP2**

1) MTPSec takes packets from the *input buffer* in the same order as they are put there by MTP2 links. First, MTPSec computes the hash of chosen message fields as indicated by the service indicator (SI) and message type (MT) fields of the authentication header (AH).
2) If *authentication data* included in the AH part matches the hash then the remaining data is passed to *message discrimination*. Otherwise, it can be dropped or logged for further analysis depending upon the implementation choice.
3) The rest of the processing is the same as MTP3 without security.

*2) IPSec : Secured Network Layer in IP Network:* The decomposed gateway architecture is secured by IPSec. IETF's internal draft "Security Consideration for SIGTRAN Protocols" [9] addresses the security issues in SIGTRAN protocol suite. All the IP nodes supporting SIGTRAN are required to support IPSec and the support for TLS is optional. All SIGTRAN nodes using IPSec must implement IPSec ESP in transport mode with non-null encryption and authentication algorithms to provide per packet authentication, integrity enforcement, confidentiality, and must implement replay protection mechanisms of IPSec [9]. For peer authentication, negotiation of security association and key management, all SIGTRAN nodes must support IKE [4]. Peer authentication must be supported by using pre-shared keys and may also support certificate based authentication using digital signatures.

### B. Binding of IP addresses to a Signaling Point Code

As stated in section III, there is a need to bind IP addresses to the corresponding signaling point code of the node. At




a.) Enhanced MTP3 Layer b.) Authentication Header Format

Fig. 3. Proposed Enhancements to SS7 Network Architecture

present, both internet key exchange (IKE) and stream control transmission protocol (SCTP) lack a way of binding them. We now propose a mechanism to do so.

*1) IKE fix:* IETF RFC 2409 [4] describes the key exchange mechanism, its *Main Mode* exchange uses six messages in three round trips to establish IKE SA. These three trips are divided into three steps. In the first step peers do SA negotiation and in the second they exchange Diffie-Hellman values and nonces and when that is finished, authenticate each other. We have enhanced the last lap, peer nodes will not only identify each other by their IP addresses but also with their point codes. We have shown only the last lap of message exchange, all other details and notations used are same as described in IETF RFC 2409.

**Message 5 from Initiator(I) to Receiver(R):** I sends its own point code $PC_I$, IP address $IP_I$, signed $Nonce_R$ and its own certificate $Cert_I$, encrypted with $SKEYID_E$.

**Message 6 from R to I:** R sends $PC_R$ point code of receiver, IP address $IP_R$, signed $Nonce_I$ and its own certificate $Cert_R$, encrypted with $SKEYID_E$.

*2) SCTP Association setup fix :* Setup of an association between SCTP based IPSPs involves the exchange of at least four SCTP packets between them. Whenever IPSP-A is willing to create an association with IPSP-B, A will send out an INIT chunk, the first SCTP packet in association setup procedure. Point B responds with INIT-ACK. Inside the INIT-ACK is a state cookie that is echoed back to B in the COOKIE-ECHO. Upon receiving the COOKIE-ECHO, endpoint B returns an acknowledgment, the COOKIE-ACK, and the association is set up. We propose to create a new parameter to be included with INIT and INIT-ACK as an optional parameter. The parameter value contains point code of the signaling node. The upper two bits of the *Parameter type* implicitly instructs a receiver, how to deal with unrecognizable parameter type. We have used 00xxxxxx-xxxxxxxx bit pattern for the parameter type. Any node which does not recognize this parameter has to stop processing the entire SCTP chunk and discards it silently. It serves dual purpose, one for identifying point code carrying parameter and secondly it makes sure that IPSP-A is handshaking with another IPSP, not with an ordinary SCTP based host which does not have any SIGTRAN adaptation layer.

These proposed enhancements to IKE and SCTP association setup properly binds both the identifiers (IP addresses with point code) with minimal modifications to already established protocol exchanges.

### C. Trust Management

In the previous section V-A, we saw how two signaling nodes can authenticate each other and derive session keys to setup secure tunnels. Now at the interface, between two networks, we need to define service level agreements (SLAs) and access control(AC) policy before allowing incoming traffic to our own network. SLA not only helps to identify what is possible to deliver but also deliver what is promised. There are many parameters in MSUs which are not allowed to be populated by either party. For example, *User-user Information* is a variable length optional `IAM` parameter used in countries that offer user-to-user signaling of ISDN users. The parameter contents are not specified by ITU-T, and are coded as agreed by individual user pairs [2]. Generally carrier service providers mutually agree to prohibit use of this parameter, so any `IAM` message containing this parameter is syntactically well formed but still considered incorrect. Similarly AC policy may save own network from many threats which are arising if we allow outsider node to start network management procedures to operate. AC list is maintained at the SG, to check which outsider nodes (by checking OPC) are allowed to perform which network management procedures. The information maintained by this component is used by Firewall to perform message-content checking.

### D. Enhanced Firewall Solution

Any message coming towards its own network should be admitted only when it fulfills the criterion of well-formedness. Well-formed messages are syntactically correct and the content of the payload and header part of the message is as specified. Screening rules at the SS7 side are more or less fixed whereas at IP side it depends upon the adaptation module used between IPSPs. Out of many adaptation modules

available, we specifically take M2PA as an example.

**Syntax Screening :** ensures that message is encoded according to the standard. For example in the case of M2PA messages, the version field in header should be 1, Spare field should be all zeros, Message Class is 11, Message type is either 1 or 2 for User data or Link Status respectively, Message length field really equals the message length. Same way the parameters contained in the message and its value should follow the standard and its length field equals the combined length of tag, length and value field of the parameter. For a particular message class and type, it should have some defined and permitted parameters only whether it is a mandatory or optional.

**Content Screening :** further screens those messages which were selected or passed by the syntax screening. It acts as per service level agreements (SLAs) made between the carrier service providers. It is also possible that some providers may have their own access controls operating on the ingress traffic to their network further restricting the allowed messages. Though these messages are syntactically correct but according to service provider's point of view they are incorrect and may pose some threats. For example in *DPC* field of RL contained in SIF is 32 bit unsigned integer, so any value may be syntactically allowed but it may be content wise inappropriate if the receiving node does not serve this destination point code and it should not have come to this node.

### *E. Intrusion Detection System at SG*

We maintain call state information for each voice trunk through the exchanged messages and its effect on the protocol state machine. Call state information not only helps in establishing the relationship between the exchanged messages but also records voice trunk usage and its involved parties for later statistical analysis. The anomalous behavior at a node can be observed by state transition analysis of protocol. If we define all the protocol states and its involved events and constraints then any deviation from this normal behavior (i.e. state) will represent abnormal behavior.

### *F. Protocol Armor*

As soon as the new vulnerability is discovered, this component allows a quick fix to more common problems such as DoS and protocol vulnerability before a relevant signature can be found and implemented at the appropriate security component. To avoid traffic flow analysis it can mask IP addresses and port numbers of the outgoing packets or by introducing bogus traffic.

## VI. Related Work

The Telcordia specification [6] provides some screening capability, deployed today at the SS7 gateway *Signaling Transfer Points* (STPs). Major STP vendors have incorporated *Gateway Screening* into their products. Generally *Gateway Screening* screens MTP message headers and if the message type is *Network Management Message* then it checks message content like *Message Type* and *Affected Destination*. Realizing the need for enhanced security measures, Telcordia later on screens ISUP and SCCP messages for specific *message types* and some *message priority* fields. Verizon's *SS7 Security Gatekeeper* [22] goes well beyond Telcordia's *Gateway Screening* by incorporating syntax, content screening and checking their proper sequencing.

Sailer [14] in 1998 proposed an enhancement of existing network services interfaces by standardized security service interfaces to enable the provision of open security services. A new application level protocol referred to as the *Security Services Application Part (SecAP)* was envisioned to fulfill the need of additional signaling protocols between core network functions and specialized security services functions. Lorenz et al.[8] and Moore et al.[11] analyzed the vulnerabilities in SS7 network and presented an attack taxonomy. Similarly Oneglia et al.[12] presented SS7 network vulnerabilities with respect to access control. As part of the solution they developed test cases to verify signaling traffic traffic coming towards one's network. Sengar et al. [16] proposed MTPSec component at MTP3 layer to provide link-by-link security in SS7 network. Within IP network, IETF's SIGTRAN working group has proposed IP Security (IPSec) and Transport Layer Security (TLS) for the security of signaling messages [9], [13], [7], [17]. In addition, many recent commercial products are coming out in the market to secure SS7.

InteleGuard firewall solution by Sevis Systems, capture signaling messages directly from SS7 links and analyze them based on policies activated by the service provider [10]. InteleGuard Signaling Firewall, enables security and operations policy definitions for active monitoring and controlling SS7 network traffic. Every incoming and outgoing message is controlled via a rule-based operations policy. It allows to filter, modify, monitor and/or alert on any SS7 message in real time. Its ability to go beyond traditional gateway screening found on many STPs lies in its inspection capability that can make filtering decisions based on the content of the message parameters [19]. Tekelec's EAGLE STP gateway screening (GWS) provides access control and screening of inbound and outbound messages. GWS provides two levels of screening at the message transfer part (MTP) and signaling connection control (SCCP) level [20]. SecureLogix's Telewall is a firewall for private branch exchanges (PBXs) that detects, logs and controls all inbound and outbound telecom network activity based on user defined security policy. It protects data networks, phone systems and other critical infrastructure from back door modem access and other external attacks through the PSTN [15]. All of the security products developed known to us are firewalls for the SS7 network. They come with known limitations of firewall solutions.

## VII. Conclusion

IP telephony provides a viable alternative to traditional wired line and wireless telephone systems. Still, to connect traditional telephone subscribers with IP phones, signaling

messages need to traverse SS7 and IP network. This interoperability is possible due to SIGTRAN adaptation modules, which transport SS7 signaling messages over IP network. Besides the VoIP services, SIGTRAN based signaling nodes are used for location based services, SS7 and SMS offload. Such a critical signaling infrastruture is vulnerable to many security threats arising due to message structure, message content, misbehaving signaling nodes and traffic analysis etc. To avoid security threats to integrated signaling network, we propose a comprehensive layered security solution. When implemented at a signaling gateway, it avoids security threats to cross over to another signaling network and puts a check to misbehaving signaling nodes.

## REFERENCES


[1] P. Bhatnagar. *Engineerig Networks For Synchronization, CCS7, and ISDN*. IEEE Press, first edition, 1997.

[2] J. Bosse. *Signaling in Telecommunication Networks*. John Wiley Sons Inc, first edition, 1998.

[3] G. Camarillo, A. Roach, J. Peterson, and L. Ong. RFC 3398 : Integrated Services Digital Network (ISDN) User Part (ISUP) to Session Initiation Protocol (SIP) Mapping. RFC 3398, IETF Network Working Group, December 2002.

[4] H. D and C. D. RFC 2409 : The Internet Key Exchange (IKE). Rfc 2409, IETF Network Working Group, 1998.

[5] FCC. Telecommunications Act of 1996. Report 110 Stat. 56, Pub. LA. No. 104-104, 1996.

[6] GR-82-CORE. Signaling Transfer Point (STP) Generic Requirements. Technical report, Telcordia, Morristown, New Jersey, 2001.

[7] C. Groves, M. Pantaleo, T. Anderson, and T. Taylor. RFC 3525 : Gateway Control Protocol Version 1 . RFC 3525, IETF Network Working Group, June 2003.

[8] G. Lorenz, T. Moore, G. Manes, J. Hale, and S. Shenoi. Securing SS7 Telecommunications Networks. In *Proceedings of the 2001 IEEE Workshop on Information Assurance and Security*, West Point, NY, June 2001.

[9] J. Loughney, M. Tuexen, and J. Pastor-Balbas. Security Considerations for SIGTRAN Protocols - work in progress. *IETF Network Working Group*, June 2003.

[10] T. McElligott. Sevis puts SS7 on guard. Report, Telephony Online, Primedia Pub., 2001.

[11] T. Moore, T. Kosloff, J. Keller, M. G., and S. Shenoi. Signaling System (SS7) Network Security. In *45th Midwest Symposium on Circuits and Systems*, volume 3, pages 496–499, August 2002.

[12] F. Oneglia and T. Baritaud. CCS 7 Networks Dependability Studies: Phase 2 Deliverable 2. Technical Report Annex A - Protocol analysis in Access Control, June 1998.

[13] L. Ong, I. Rytina, M. Garcia, H. Schwarzbauer, L. Coene, H. Lin, I. Juhasz, M. Holdrege, and C. Sharp. RFC 2719 : Framework Architecture for Signaling Transport. RFC 2719, IETF Network Working Group, October 1999.

[14] R. Sailer. Signaling and service interfaces for separating security sensitive telecommunication functions considering multilateral security. In *6th Open Workshop on High Speed Networks*, Stuttgart, October 1997.

[15] SECURELOGIX. TeleWALL Firewall. White paper, http://www.securelogix.com/telewall/, 2001.

[16] H. Sengar, D. Wijesekera, and S. Jajodia. MTPSec: Customizable Secure MTP3 Tunnels in the SS7 Network. In *19th International Parallel and Distributed Processing Symposium, Workshop-17, IPDPS*, 2005.

[17] G. Sidebottom, K. Morneault, and J. Pastor-Balbas. RFC 3332 : Signaling System 7 (SS7) Message Transfer Part 3 (MTP3) - User Adaptation Layer (M3UA). RFC 3332, IETF Network Working Group, September 2002.

[18] R. Stewart, Q. Xie, K. Morneault, C. Sharp, H. Schwarzbauer, T. Taylor, I. Rytina, M. Kalla, L. Zhang, and V. Paxson. RFC 2960 : Stream Control Transmission Protocol. Technical report, IETF Network Working Group, October 2000.

[19] S. Systems. Inteleguard signaling firewall. White paper, http://www.sevis.com/inteleguard.htm, 2001.

[20] TEKELEC. Tekelec EAGLE STP. White paper, http://www.tekelec.com/productportfolio/eagle5sas/, 2001.

[21] A. Vemuri and J. Peterson. RFC 3372 : Session Initiation Protocol for Telephones (SIP-T) Context and Architectures. RFC 3372, IETF Network Working Group, September 2002.

[22] Verizon. SS7 Security Gatekeeper. Technical Report Request for Information - Verizon Communications, May 2002.