Report on

Secure Telephony Enabled Middle-box (STEM)

Maggie Nguyen

04/14/2003

Dr. Mark Stamp - SJSU - CS 265 - Spring 2003

Table of Content

1. Introduction …………………………………………………………………………… 1

2. IP Telephony Overview ……………………………………………………………….. 1

2.1 Major Components of an IP Telephony System ………………………………………. 1
2.2 Protocol Origin of IP Telephony Protocols …………………………………………... 2
2.3 How SIP Works ………………………………………………………………………….. 2

3. STEM Architecture ……………………………………………………………………. 3

3.1 Architecture Components …………………………………………………………… 3
3.2 Call Scenarios ………………………………………………………………………….. 5

4. STEM Countermeasures on Network Vulnerabilities …………………………………….. 7

4.1 Denial of Service ……………………………………………………………………….. 7
4.2 Eavesdropping ………………………………………………………………………….. 8

5. References ……………………………………………………………………………….. 8

Figure List:

Figure 1: Major System Components of an IP Telephony Network [1] ………………………... 1
Figure 2: SIP Call Setup [3] …………………………………………………………………… 2
Figure 3: SIP Call Flow Diagram [2] ………………………………………………………….. 3
Figure 4: STEM Network Components [2] ……………………………………………………. 3
Figure 5: Firewall Architecture Block Diagram [2] ……………………………………………. 4
Figure 6: Incoming Net-to-Net Call Flow [2] …………………………………………………. 5
Figure 7: Net-to-Phone Call Flow [2] …………………………………………………………. 6

1. Introduction

STEM architecture is prototyped by Brennen Reynolds and Dipak Ghosal. Its article is published in the IEEE Communication Magazine in October of 2002.

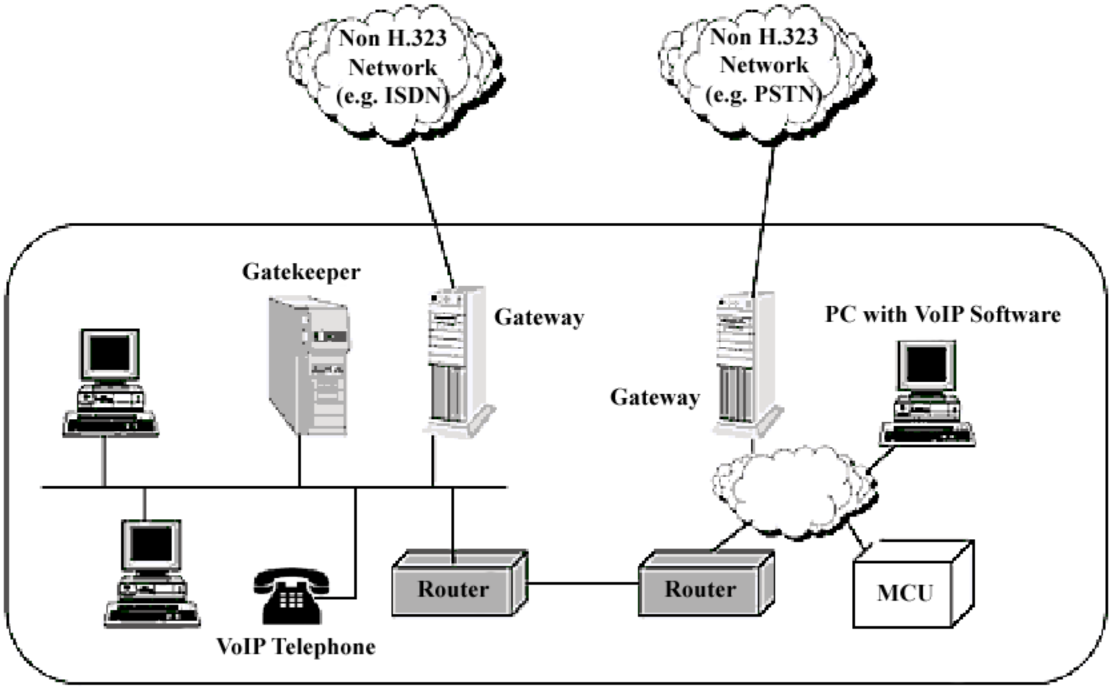
STEM is proposed as a solution to network vulnerabilities, targeting the transmitting of real-time data over enterprise networks. The architecture involves a basic SIP-deployed network, mostly used for IP telephony and other dynamic applications.

2. IP Telephony Overview

IP Telephony is the technology that enables the delivery of voice signals via the data network, rather than the public switched telephone network (PSTN). The basic steps involve the conversion of the analog voice signal to digital format and compression/translation of the signal into IP packets for transmission over the Internet. The process is reversed at the receiving end.

2.1 Major Components of an IP Telephony System

Figure 1: Major System Components of an IP Telephony Network [1]



- ***Gateways:*** devices that helps with the communication and translation between the end points in different networks.
- ***Gatekeepers:*** devices to keep track of registered endpoints which are the LAN clients.
- ***IP Telephones and PC-based Software Phones:*** terminals that are enhanced with functionalities and services for IP Telephony.
- ***MCUs****:* is an optional component introduced in the H.323 standard. The MCU is required in a centralized multipoint conference where each terminal establishes a point-to-point connection with the MCU.

2.2 Protocol Origin of IP Telephony Protocols

There are two different architectures that enable the implementation of IP telephony technology. STEM architecture is currently using the network required for SIP deployment.

Internet Engineering Task Force (IETF)	*International Telecommunications Union (ITU)*
Signaling: Session Initiation Protocol (SIP) Transport: Real Time Protocol (RTP) Media Description: Session Description Protocol (SDP)	Signaling: H.323 Codecs: G.711 (PCM), G.729, … ISDN: Q.931

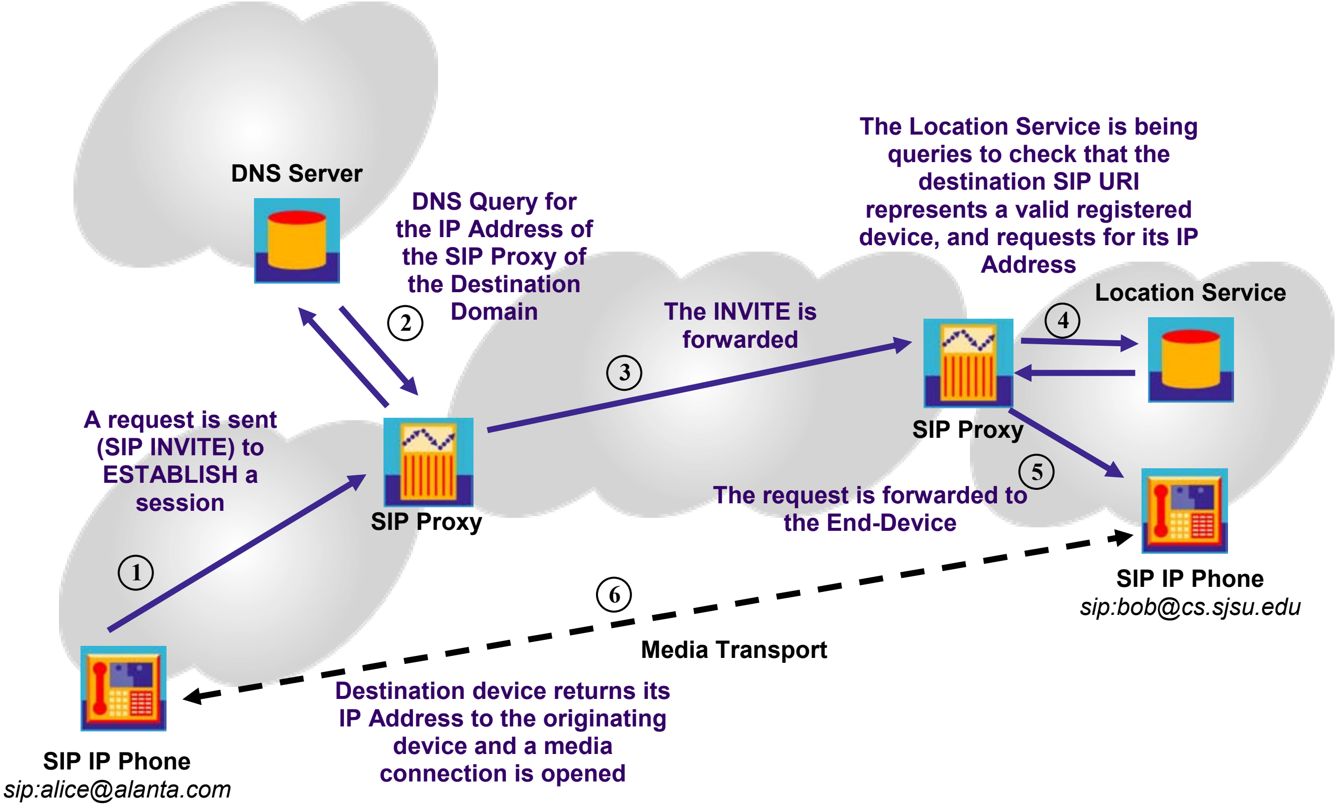
2.3 How SIP Works

A typical example of a SIP message exchange is between two users, Alice and Bob. Alice uses her SIP phone to call Bob on his SIP phone over the Internet. Also, there are two SIP proxy servers that act on behalf of Alice and Bob to facilitate the session establishment.

Alice "calls" Bob using his SIP identity, a type of Uniform Resource Identifier (URI) called a SIP URI. It has a similar form to an email address, typically containing a username and a host name.

Examples: *sip:alice@atlanta.com* and *sip:bob@cs.sjsu.edu*

Figure 2: SIP Call Setup [3]



DNS Query for the IP Address of the SIP Proxy of the Destination Domain

The INVITE is forwarded

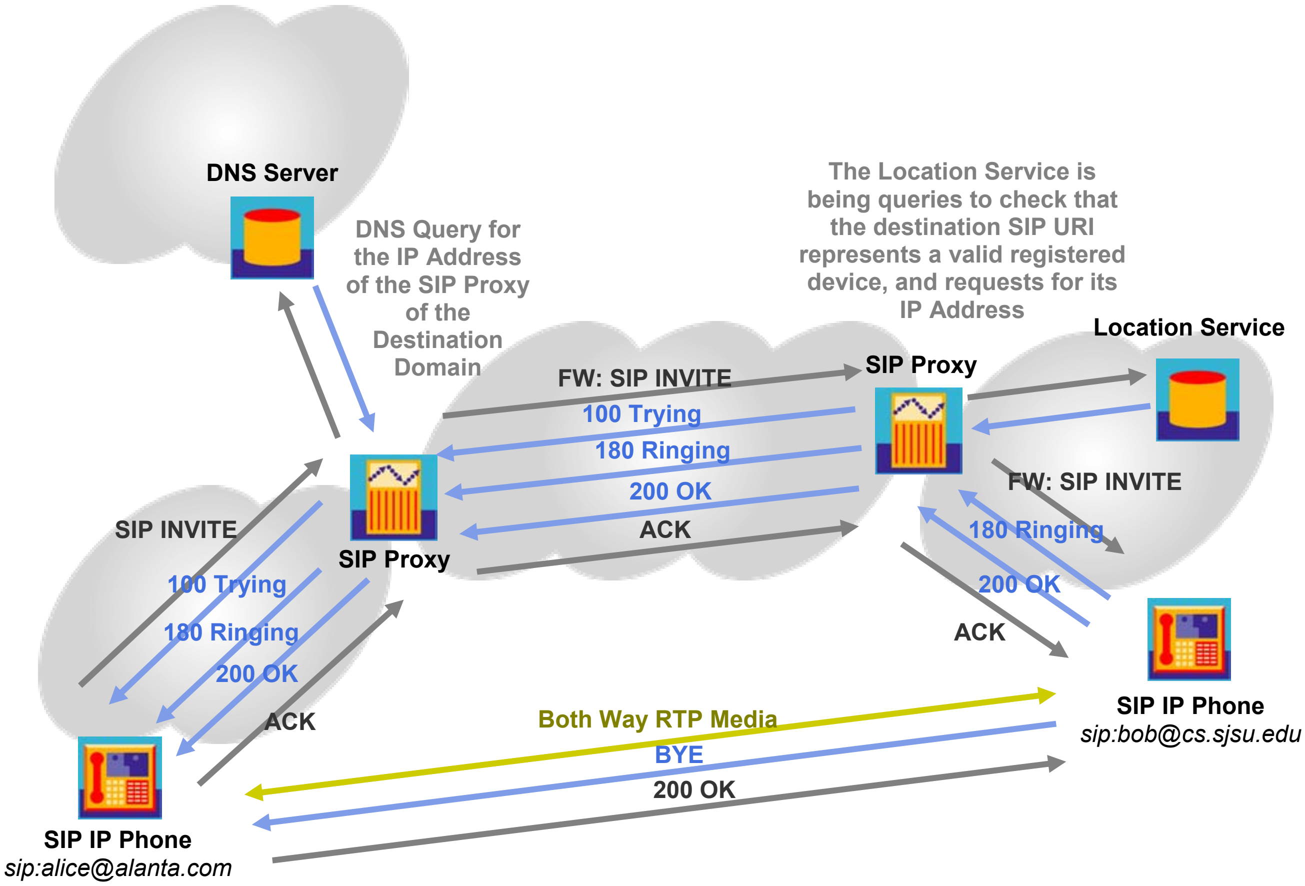
The Location Service is being queries to check that the destination SIP URI represents a valid registered device, and requests for its IP Address

A request is sent (SIP INVITE) to ESTABLISH a session

The request is forwarded to the End-Device

Destination device returns its IP Address to the originating device and a media connection is opened

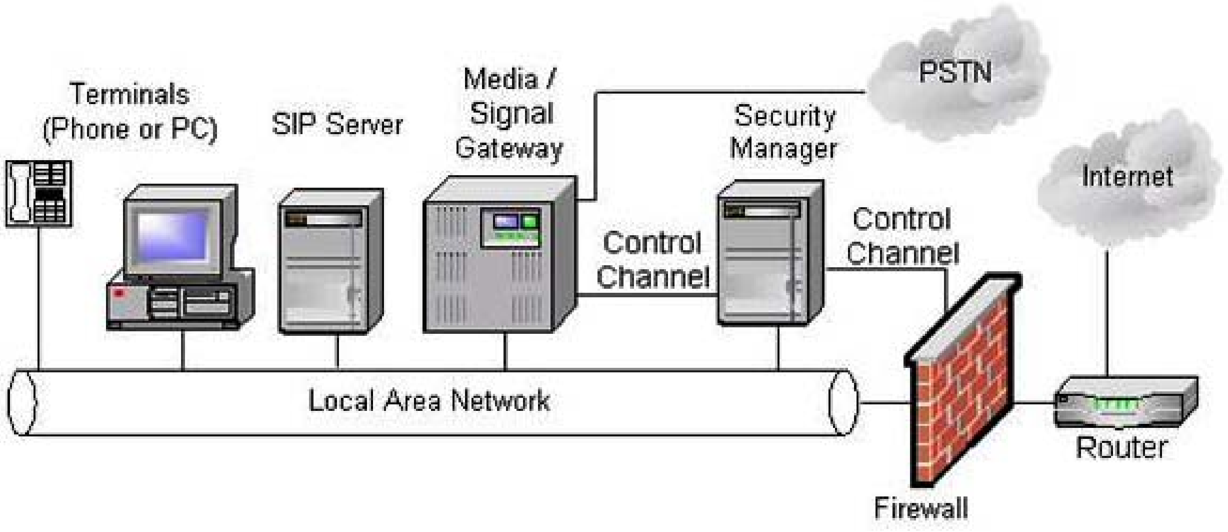
Figure 3: SIP Call Sequence [2]



3. STEM Architecture

3.1 Architecture Components [4]

Figure 4: STEM Network Components [2]



Security Manager (SM):

- A database mapping between user addresses (SIP URIs) to machine addresses (IP addresses) *(This can be implemented by the SIP Location Server)*
- A call reference database with an entry for each employee. A profile could contain information regarding to incoming call preferences and a list of spam addresses to be blocked. *(This can be implemented in the SIP Server or SIP Location Server)*
- Various threshold levels to be triggered when the network is under attacked
- Authentication mechanism/database to allow only authorized users to use IP Telephony services. The SM acts as a proxy between the user terminal and the authentication database. Successful authentication will prove to the SM that the user can be trusted.

Upon a query to a user profile in response to an incoming call, the SM will respond differently to the firewall based on the profile setup.

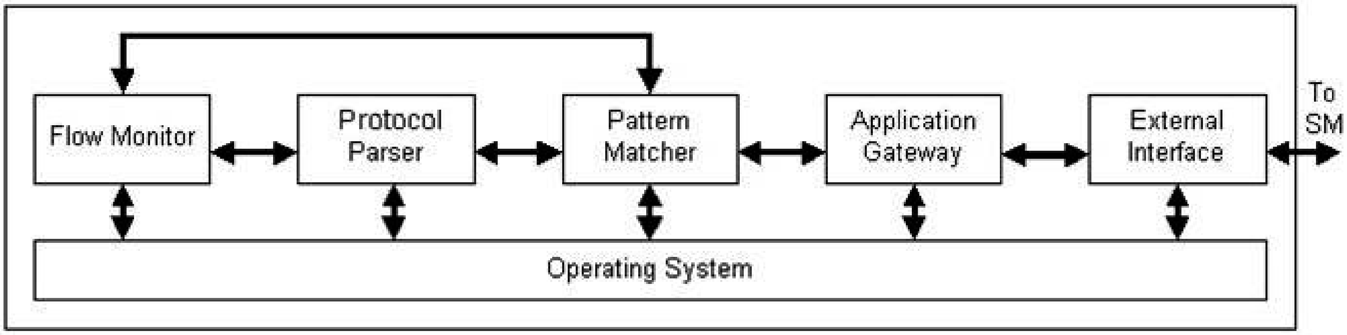
Example: - Automatically accept the call
- Forward the call to another user or service
- Automatically drop the call

This is a dynamic feature of the STEM architecture in dealing with the dynamic nature of real-time applications.

Firewall:

The overall function of the firewall still remains to allow only certain traffic to pass through the private enterprise network. However, conventional firewall traffic filtering only operates at the network and/or transport layers, and thus it is unaware of the application layer. Therefore, the STEM architecture is proposed with a flexible and enhanced firewall that is aware of the applications running on top of the network and/or transport layers.

Figure 5: Firewall Architecture Block Diagram [2]



The components are implemented as modules and can be loaded independently depending on how administrators want to setup the firewalls.

- **Pattern Matcher:** allows a configuration of static rule sets using machine addresses, transport protocols, and port numbers.

- **Protocol Parser:** includes multiple parsers. Each parser is designed to understand the operation of a single complex protocol.
  Example of the SIP Protocol Parser:
  - a call monitor component to ensure that each call follows the protocol-specified state transitions

- Creating pinholes based on the dynamic port requests in the call setup.
- Dealing with two calls selecting the same port number: monitoring each port and internal IP address of a data stream.
- Closing a port after the associated stream(s) is terminated.
- Extracting the CODEC advertised by a terminal during a call setup and passing to the Flow Monitor to detect malicious streams.

- **Flow Monitor:** handles malicious data streams. It monitors the data rate of the call streams to see if they exceed some thresholds, set by the bandwidth advertised at the call set up and the bandwidth the firewall can respond. To respond to a malicious stream, either its packets will be dropped or other protection algorithm will take place.

- **Application Gateway:** talks to other applications.

- **External Interface:** allows the firewall to talk to other devices.

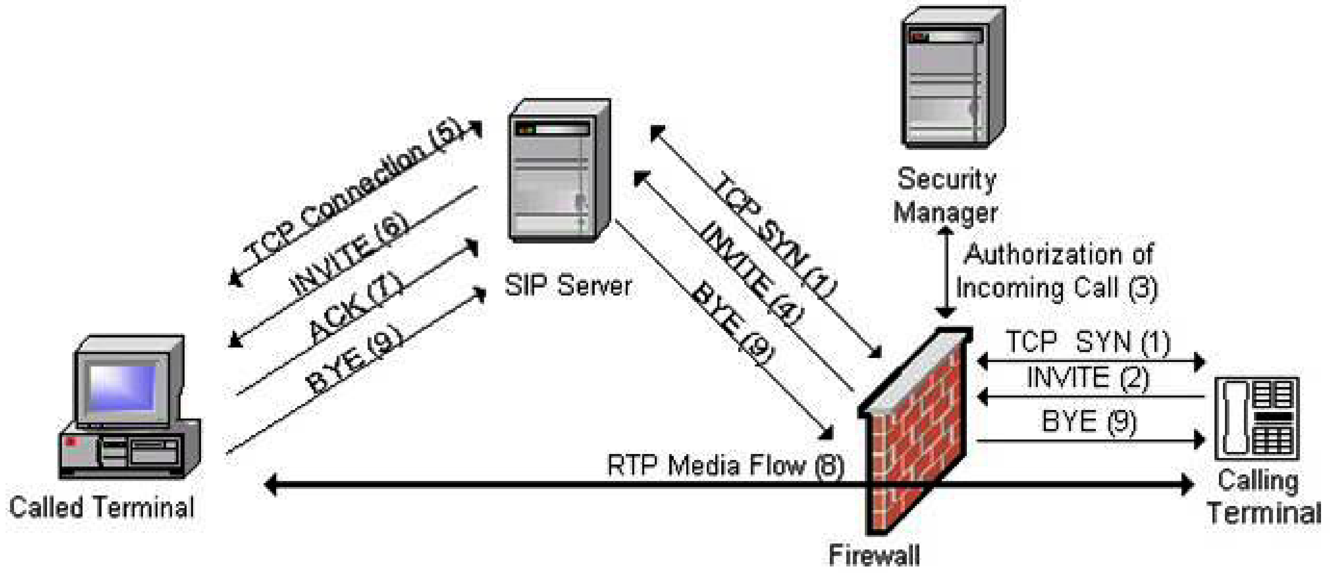
Media/Signaling Gateway (M/S Gateway):
The media/signaling gateway has the same functionalities of a normal IP Telephony gateway. It is responsible to translate calls between a circuit-switched network and a packet-switched network. In STEM architecture, the gateway also needs to communicate with the SM. All out-going calls need to be authenticated with the SM before the gateway allows all calls to be placed.

User Terminals:
There are two types of terminals: PC-computer with IP Telephony software or a telephone that is capable of IP Telephony functions. Both types of terminals must be able to communicate with the SM and understand SIP (or H.323).

3.2 Call Scenarios [4]

Net-to-Net Scenario:

Figure 6: Incoming Net-to-Net Call Flow [2]



For Incoming-Calls:

- The calling terminal sends a TCP SYN packet to port 5060 (SIP port) of the destination terminal.
- SIP Protocol Parser in the firewall identifies the port and forwards the packet to the SIP proxy.
- SIP proxy completes the three way handshake with the calling party.
- The calling terminal sends a SIP INVITE over TCP.
- SIP Protocol Parser identifies the request and contacts the SM for relevant information.
- SM responds whether or not to allow the call based on the user profile preference. If yes, the IP address of the called terminal is sent back.
- The INVITE request is forwarded to the SIP proxy.
- SIP proxy forwards the INVITE message to the called terminal after establishing a TCP connection.

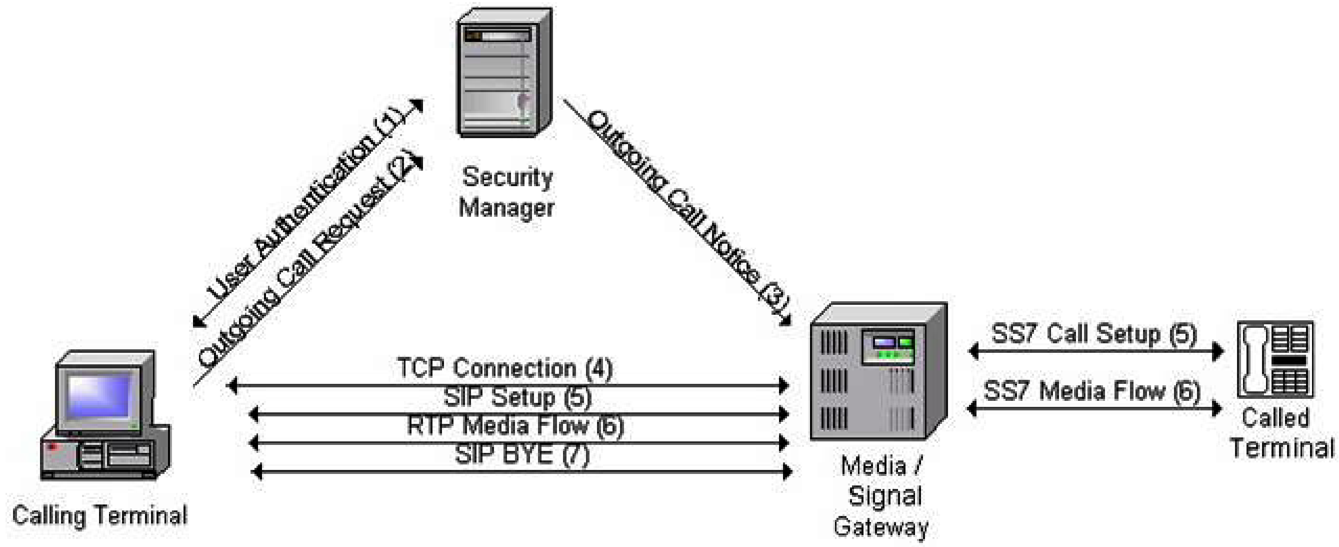
- For the rest of the call setup, the SM is not involved, and the Protocol Parser assumes a passive role, extracting the information and passing it to other components within the firewall. All control messages are relayed through the SIP proxy.
- Real-time transport stream (RTP) is created directly between the calling and called terminals.
- Termination is detected in either two ways: Protocol Parser detects a BYE message or the Flow Control does not observe any traffic for the corresponding stream after an interval.

For Outgoing-Calls:

- User must inform the SM of the machine address they are calling.
- The SM instructs the firewall to allow the outgoing TCP SYN packet.
- After TCP connection is setup, the Protocol Parser and the firewall will operate in the same manner as for the incoming-calls.

Net-to-Phone Scenario:

Figure 7: Net-to-Phone Call Flow [2]



The net-to-phone call flow is similar to the net-to-net call but the call is routed through the M/S gateway and out over the PSTN instead of going through the firewall.

- Calling terminal must be authenticated with the SM before making a call.
- Calling terminal then informs the SM of its intention to make an outgoing call to the PSTN.
- SM instructs the M/S Gateway to accept the call from the calling user terminal.

- TCP connection is established between the calling terminal and the M/S Gateway.
- Calling terminal sends a SIP INVITE message to the M/S Gateway.
- M/S Gateway converts the INVITE message into appropriate SS7 (Signaling System 7) messages.
- A voice port is allocated for the call, and the SS7 messages are sent to the called terminal.
- A connection is setup between the gateway and the called terminal over PSTN.
- Upon termination, the gateway de-allocates the voice port and all connections.

4. STEM Countermeasures on Network Vulnerabilities

4.1 Denial of Service

Net-to-Net:

Attack: Flooding of TCP-SYN packets to a terminal. (SIP Proxy is likely a potential target).
Result: Unable to accept any new connections.
Countermeasure*:* Flow Monitor of the firewall keeps track of incoming SYN packets for each source IP address. If the number of SYN packets for a particular source exceeds the threshold number, Flow Manager instructs Pattern Matcher to drop all SYN packets from the source for a period of time.

Attack: Flooding of SIP INVITE requests.
Result*:* Overwhelmed with incoming call requests.
Countermeasure: A counter monitors the number of INVITE messages sent per stream over a given interval of time. If the threshold level is exceeded, the Protocol Parser instructs the Pattern Matcher to drop subsequent control and audio packets associated with that stream.

Attack: Malicious RTP stream with large and same sequence number.
Result: Target is unaware because same sequence packets are dropped. However, network links become saturated.
Countermeasure: The CODEC and bandwidth requirements for each call are announced during setup and extracted by the Protocol Parser. This information is given to the Flow Control, which monitors the data rate for each stream. If the data rate is exceeded some thresholds, data stream can be terminated or set to a lower data rate.

Net-to-Phone and Phone-to-Net:

Attack on the PSTN side: *(on the internal network side, users are authenticated)*
Attack on the limited number of voice port in the M/S Gateway.
Result: Tie up all voice ports and saturate the links.
Countermeasure: M/S Gateway to send out Transfer Controlled message (TFC) when all voice ports are occupied to reduce the call setup requests sent to the M/S gateway.

** STEM architecture does not provide countermeasures to an internal LAN DoS attack that a user within an enterprise launches a DoS attack to another internal user terminal.*

4.2 Eavesdropping

Within the STEM architecture, there are two information flows that can be eavesdropped: the control flow and the data flow.

The control flow includes communications between
- Terminals and SM
- SM and firewall
- SM and M/S Gateways

The information within these flows may contain user authentication and device configuration messages.

Countermeasures on control flows:
- STEM architecture only uses protocols that ensure the protection of data by encrypting messages.
- Timestamp is included in the encrypted message to prevent replay attack.

The STEM architecture does not directly protect the system from the data flow eavesdropping. Each application protocol (SIP, H.323) should implement a form of payload encryption. Both SIP and H.323 have provisions defined in the specifications to provide this feature.

** STEM architecture also does not provide countermeasures for a session hijacking attack that an unauthorized third person impersonates a user of one end of the session.*

5. References

[1] International Engineering Consortium. H.323.
http://www.iec.org/online/tutorials/h323/

[2] Reynolds, B. Challenges Challenges and Rewards in Enterprise Deployments of IP Telephony Presentation. http://networks.cs.ucdavis.edu/~ghosal/Research/Talks/IP-Tel-Netlab%20talK%20-%20rev%202.ppt

[3] Reynolds, B. Deploying IP Telephony in an Enterprise and the Vulnerabilities that Come With It Presentation. http://seclab.cs.ucdavis.edu/secsem2/ReynoldsSeminar.ppt

[4] Reynolds, B. and D. Ghosal. STEM: Secure Telephony Enabled Middlebox. *IEEE Communications Magazine Special Issue on Security in Telecommunication Networks*. October 2002. http://www.off-pisteconsulting.com/research/pubs/ieee_comm.pdf