Buletinul Ştiinţific al Universităţii "Politehnica" din Timişoara

Seria ELECTRONICĂ şi TELECOMUNICAŢII
TRANSACTIONS on ELECTRONICS and COMMUNICATIONS

Tom 51(65), Fascicola 2, 2006

Widespread Deployment of Voice over IP and Security Considerations

Mihai Constantinescu[1], Doina Cernăianu[2], Dragoş Mischievici[3], Victor Croitoru[4]

Abstract – During the last years, Internet facilities like email, the world-wide-web (WWW), and e-commerce have generated a boost of Internet growth, making offering services possible in fundamentally new ways. One of these services is Voice over IP (VoIP), also named Internet Telephony (IP telephony). With most major telecommunications carriers preparing for VoIP mass deployment, the security of service cannot remain a second priority anymore. This paper analyzes the main aspects of VoIP wide deployment and highlights the benefits of using a new security concept, Session Border Controller (SBC), in solving VoIP security issues.
Keywords: VoIP, SIP, DoS, Firewall, SBC.

I. INTRODUCTION

The ubiquitous presence of Internet caused a powerful change in human life. People begin to use Internet facilities for almost all communications purposes (fig.1).

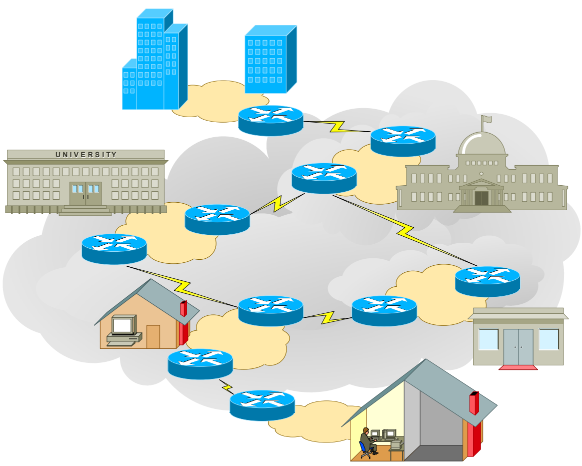

Fig. 1. Internet communications

One of these facilities is VoIP, or Internet telephony. Based on transport of voice traffic over IP networks, Internet telephony by its nature relies on technology that does not distinguish geographic borders. VoIP is not another facet of the traditional telephony service, but a new frontier in communications for individuals and businesses alike.

VoIP service has some major benefits. First, it allows costs saving by eliminating the toll charges for long-distance and even local calls. For enterprises with multiple branch offices, the use of VoIP eliminates all costs associated with calls between offices. Each phone extension is reached in the same way, despite the distance between extension and the main office. VoIP enables call transferring over a building, inside a town, or over continents. More than that, Internet telephony enables new applications such as conferencing, voice mail, unified communications (fig.2), and click to dial, all of these resulting in enhanced productivity.

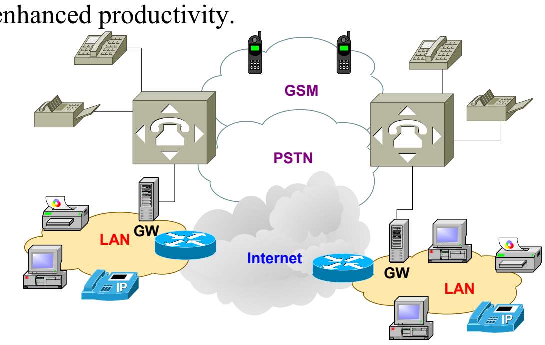

Fig. 2. Unified communications

VoIP reduces the costs and complexity of service implementation and management. Most of VoIP equipment allow remote configuration via a web-browser interface, eliminating the need for third party interventions.

However, the wide adoption of VoIP generates an increased risk of widespread security violations, and raises new security issues related to the privacy of communications, unified services, and transparency of service access over different networks and carriers. This paper presents the principles of VoIP communications, VoIP special characteristics related

[1] „Politehnica" University Bucharest, Electronics, Telecommunications and IT Faculty, Telecommunication Dept, 1-3, Iuliu Maniu Blvd, sector 6, Bucharesti, e-mail mac_2470@yahoo.com
[2] Teletrans SA Bucharest
[3] Teletrans SA Bucharest
[4] Politehnica" University Bucharest, Electronics, Telecommunications and IT Faculty, Telecommunication Dept, 1-3, Iuliu Maniu Blvd, sector 6, Bucharesti, e-mail croitoru@adcomm.pub.ro

to data networks, analyzes security problems occurred in VoIP use, and shows the role of Session Border Controller in solving them.

II. THE VOICE OVER IP PRINCIPLES AND SPECIAL CHARACTERISTICS

The transmission of voice signals through a network, either an IP network or an old public telephone network (PSTN-Public Switched Telephone Network/POTS-Plain Old Telephone System) involves the following:

- A coder/decoder (CODEC) equipment/operation that transforms analog voice signals into a digital stream;
- A signaling mechanism/protocol that coordinates the actions of network elements in order to complete a call between the endpoints (usual phones /IP phones);
- A call control (bearer-control) mechanism to transport the voice digital stream over the network;
- A database for addressing and billing purposes.

In the past, telephony was designed to cover a wide area and to provide basic voice communications services. In order to achieve this, telephony networks use a centralized architecture. There is a continuous wired connection (telephone circuit) from the telephone itself to the first telephone office (central office-CO). The old telephony network concentrates all intelligence in the core network switch in the CO. The telephone itself is a dump terminal. The call signaling and audio path use the same telephone circuit.

IP telephony delivers the same facilities, but in a totally different way. There are three approaches for voice services over Internet:

- Using signaling concepts from the telephone industry (ITU-T recommendation H.323); [1]
- Using control concepts from the telephone industry (Softswitches); [2]
- Using the Internet protocols (Session Initiation Protocol –SIP). [3]

The nature of interactive communications and the type of service is defined and determined by the signaling used for establishing the communication. Due to high flexibility and adaptability to a great diversity of IP networks, SIP is the most used VoIP protocol, and all discussion about VoIP will be directly related to it.

"Session Initiation Protocol (SIP) is an application-layer control (signaling) protocol for creating, modifying, and terminating sessions with one or more participants. These sessions include Internet telephone calls, multimedia distribution, and multimedia conferences [3]."

"SIP is not a vertically integrated communications system. SIP is rather a component that can be used with other IETF protocols to build complete multimedia architectures. Typically, these architectures will include protocols such as the Real-time Transport Protocol (RTP) [4] for transporting real-time data and providing QoS feedback, the Real-Time Streaming Protocol (RTSP) [5] for controlling delivery of streaming media, the Media Gateway Control Protocol (MEGACO) [6] for controlling gateways to the Public Switched Telephone Network (PSTN), and the Session Description Protocol (SDP) [7] for describing multimedia sessions."[3]

SIP has been designed as a multimedia protocol using a distributed architecture with universal resource location (URL) for text-based messages, trying to take advantage of the Internet model for creating VoIP netwoks and applications (fig.3).

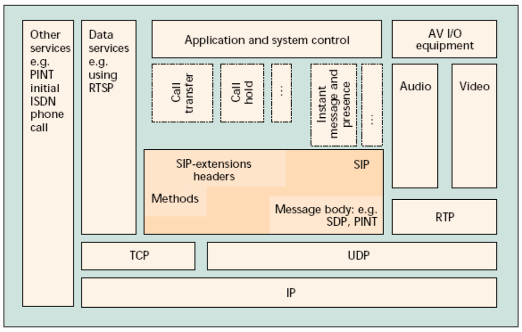

Fig. 3. SIP protocol stack

Because SIP is an IP-based protocol working in peer-to-peer architecture, unlike other VoIP protocols such as H.323, MGCP, or MEGACO, its intelligence resides at the network edge.

The SIP standard defines four entity types, as shown in fig.4:

- user agent (UA)
- proxy server (Proxy)
- registration server (Registrar)
- Redirect server (Redirect).

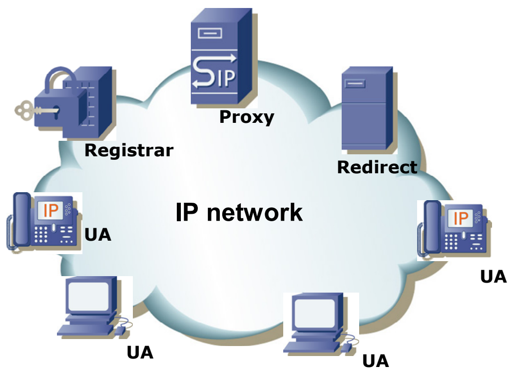

Fig. 4. SIP network elements

SIP signaling consists of an exchange of short messages that contain session descriptions, which allow participants to agree on a common set of media

parameters. The path between a pair of SIP clients is handled by SIP proxy/registrar servers. They keep information related to the current location of clients, authenticate and authorize users for services, and route requests to those clients.
Each SIP client has to register before to communicate, sending REGISTER requests to a SIP registrar server (fig.5).

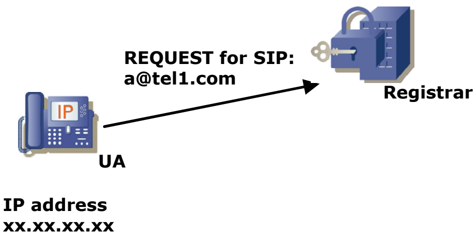

Fig. 5. SIP Registrar server

After a successfully registration, the SIP client can communicate with other SIP client using SIP proxy servers or SIP redirect servers.
The SIP proxy is a device in the signaling path that routes requests to their destinations (fig.6).

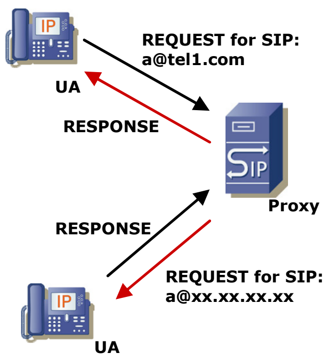

Fig. 6. SIP proxy server

Also named rerouting server, SIP redirect server responds to requests by redirecting them to another device (fig.7).

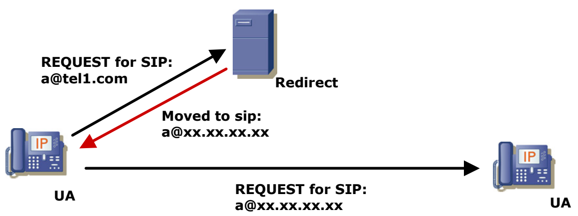

Fig.7. SIP Redirect server

SIP communication is made up of messages that are sent between devices using UDP, or TCP.
A SIP dialog means a persistent link between two devices that is used to associate transactions. A call contains multiple dialogs.
A SIP message contains a call identifier field (Call-ID) that is used to link the dialogs and transaction into an application-level concept of a call.

The default operation for SIP using UDP/TCP consists in responses generated by SIP proxy/registrar servers to requests generated by SIP phones (User Agent Client). The response message contains the source address from the request message in the SIP "via" header and in the "received" parameter, and the source port from the request message in the SIP "via" header.
The RTP is the most common media transport protocol used in SIP communications. Negotiation of RTP parameters is done using the SDP protocol. In the SDP part of the SIP message there are specified the address and port of each client to receive media.
SIP initiates a call through an INVITE message and an answer from the called party. Both the invitation and the answer contain a session description which indicates the terminal capacity. Proxy and rerouting servers are responsible for the parties' user names and IP addresses translation. (fig. 8).

```
INVITE sip:7170@iptel.org
SIP/2.0
Via: SIP/2.0/UDP
195.37.77.100:5040;rport
Max-Forwards: 10
From: "jiri"
<sip:jiri@iptel.org>;tag=76ff
7a07-c091-4192-84a0-
d56e91fe104f
To: <sip:jiri@bat.iptel.org>
Call-ID: d10815e0-bf17-4afa-
8412-
d9130a793d96@213.20.128.35
CSeq: 2 INVITE
Contact:
<sip:213.20.128.35:9315>
User-Agent: Windows RTC/1.0
Proxy-Authorization: Digest
username="jiri",
realm="iptel.org",
  algorithm="MD5",
uri="sip:jiri@bat.iptel.org",

........................................
```

Fig.8. SIP message example

As a protocol used in a distributed architecture, SIP allows companies to build scalable, resilient and redundant large scale newtorks. The protocol provides mechanisms to interconnect with other VoIP networks in order to add intelligence and new options to each of the terminals, SIP proxy servers and rerouting servers.

III. SECURITY PROBLEMS IN VoIP USE

Security issues in VoIP are different and in ways more complex than security for data applications. IP telephony involves multiple layers of the protocol stack, requiring interoperability among different new and legacy protocols, and interactions among multiple network elements. Denial-of-Service, eavesdropping, connection hijacking, and call fraud will take new forms in a voice-data unified network. New security risks arise from network interconnections, and also due to VoIP network vulnerability to virus and worm spreading through the data network elements. There is an individual solution for each threat, but a global one is much more desired.

Denial-of-Service (DoS)/Distributed DoS (DDoS)

"A DoS attack is a malicious attempt by a single person or a group of people to cause the victim, site, or node to deny service to its customers. When this attempt derives from a single host in the network, it constitutes a DoS attack. On the other hand, it is also possible that a lot of malicious hosts coordinate to flood the victim with an abundance of attack packets, so that the attack takes place simultaneously from multiple points. This type of attack is a Distributed Denial-of-Service."[8]
A DoS/DDoS attack can cause an enterprise a dramatic loss of revenue, due the loss of communication.

Eavesdropping (Call Interception)

Call interception is the possibility of unauthorized monitoring of RTP traffic. It can occur especially from within the network, and it exploits the vulnerability of SIP servers to registration hijacking, impersonation, and DoS/DDoS. The server can be tricked in acting as a codec converter between the two SIP clients, allowing voice traffic to be recorded or routed to other destination.

Signal Protocol Tampering

It occurs when a malicious user captures and changes the packets involved in the initiation of the call. Thus he can change different fields in VoIP packets, acting for the VoIP network as an authorized network user. In that way, the thief can make expensive VoIP calls.

Presence Theft

Presence theft consists in the impersonation of an authorized user sending or receiving data. It is linked with the Signal Protocol Tampering.

Toll Fraud

The ability of a hacker to use the resources of the VoIP network in order to make unauthorized VoIP calls.

Call Handling OS

The call management is done by machines running different operating systems (OS). If the OS is compromised, it opens a security gap to be used further.

Spam over Internet Telephony (SPIT)

Even though SPIT seems to be just an inconvenience, it is truly DoS and greatly reduces the bandwidth of the network.

Other security problems occur at VoIP service use over different networks, or carriers, involving call/user authentication protocol translation.

There are several solutions to these security issues, but most of them mean solving one issue in the detriment of the others.

Virtual LANs

The service providers look to protect the integrity of their networks, using firewalls and Network Address Translators (NAT), in order to implement Virtual LANs. By keeping VoIP and data in different VLANs, the network performance and security increase. Meanwhile, the peer-to-peer model of SIP encounters serious problems at NAT traversal. First, NAT does not allow any incoming calls from public to private hosts. Second, SIP messages encapsulate the source address and port at application level. The NAT changes the address and port of packets, but only in IP and TCP/UDP headers, so the messages will be discarded by the SIP client. Moreover, SIP uses different ports to communicate, therefore several SIP messages will be blocked by NAT due to port filtering. [9-19]

Encryption

Encryption is a good method of protection, but can be done only within the network. The users will be isolated from the outside. Even so, the existence of multiple encryption points can affect the performance of the VoIP network itself.

Direct Firewall Support

It implies the modification of firewall functionality, adding an Application Layer Gateway facility. That solution makes the security policy more complex to manage. It is also more restrictive to a scalable VoIP network. [9-19]

Reverse Proxies

It is based on segmenting the VoIP traffic using multiple servers that are acting as B2BUAs (Back-to-

Back User Agents). A B2BUA terminates the call signaling from one endpoint and initiates the same call to the other endpoint, but with other identity. In that way, the identity of the call is hidden to the rest of network elements. The use of reverse proxies solely for this purpose is irrelevant.

IV. SESSION BORDER CONTROLLER (SBC)

At first glance, SBC is a kind of firewall for VoIP traffic. In reality, due its complex activity, an SBS is much more than a simple multimedia firewall.

"In its simplest form, a Session Controller enables interactive communication across the borders or boundaries of disparate Internet Protocol (IP) networks. In doing this, Session Controllers connect islands of IP voice and/or video traffic without requiring all IP traffic to first be converted into TDM at a handoff point between networks. Session Controllers operate at Layer 5 of the network and work with - but don't replace – devices such as Softswitches, NAT devices and firewalls."[20]

An SBC cooperates with firewalls in order to enable authorized connectivity from the outside to inside, avoiding the "incoming signaling from public network" issue. An SBC performs some NAT functions, but does not interfere with it. The address and port changes affect only the current SIP connection, the rest of data traffic being under NAT control.
A SBC contains two logical entities [21]: SBC signaling server (SBC-SIG) and SBC media server (SBC_MEDIA).

SBC-SIG

SBC media server is dealing with SIP signaling between SIP clients behind the NAT and the SIP proxy server. It is configured as a transit point for SIP signaling messages and provides complete visibility and control of call establishment. The SBC signaling server also controls the interval for SIP register update, in order to avoid the "binding timer" issue.
The SBC-SIG processes the SIP user registration, modifies SIP header (contact and via header), in order to allows the correct processing of SIP clients and SIP server messages. It performs address and port modification to permit NAT traversal. This behavior qualifies it as a B2BUA.[21]
Communication with the SBC media server, for traffic management and synchronization, and resolution of SIP servers through DNS, is also done by SBC-SIG.

SBC-MEDIA

SBC media server operates under the control of the SBC signaling server. It acts as a transit point for RTP and RTCP traffic between SIP clients. It modifies SDP parameters to allow NAT traversal for media using NAT's pin-holes, but without interfering with NAT security policy. This is a typically RTP proxy behavior. [21]
Being under control of SBC signaling server, the SBC media server provides full visibility and control of the media traffic for each SIP connection. Additionally, it can act as a dynamic NAPT that hides details of the network elements and topology. [9-19]

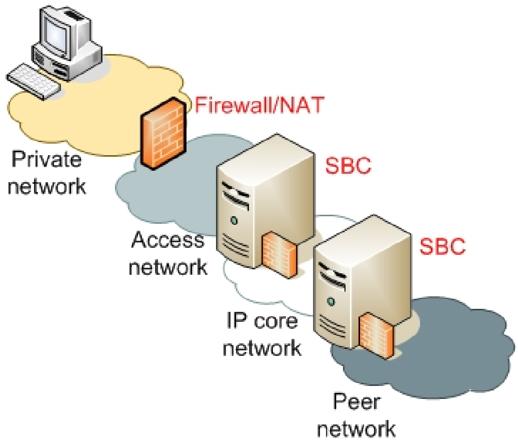

Fig. 9 SBC in a scalable VoIP architecture

V. SBC ROLE IN SOLVING VoIP SECURITY ISSUES

DoS /DDoS

SBC-SIG may identify badly-formed messages. It can knows the users identity. It will rejects the messages with wrong format and stop the signaling from the sourse IP identified as attacker. Additional, the firewall may be configured to filter the RTP traffic that don't have the SBC-SIG appouval (don't belong to a call).

Eavesdropping (Call Interception)

Call Admission Control (CAC) is the main function what differentiates SBC from ALG. Each SBC-SIG controls the call signalling though the network. Acting as a B2BUA, it hides the network internal topology from the exterior, protecting the identity of network users.

Signal Protocol Tampering

Each call signalling is monitored and all traffic from malicious sources is dropped.

Presence Theft

Presence theft is avoided by eliminating the Signal Protocol Tampering threat.

Toll Fraud

Each call is identified and SBC controls also VoIP network bandwidth use.

Call Handling OS

The data firewall protects the network from usual attacks, and the SBC gives more protection controlling the signalling and media traffic. Doing so, network elements are keeping safe.

Spam over Internet Telephony (SPIT)

CAC function of SBC has the ability to limit the traffic for each call, avoiding SPIT.

Virtual LANs

The NAT/firewall presence is no more a problem for VoIP traffic. The SBC-SIG acts as B2BUA, and opens pine-holes in firewall for the media traffic controlled by SBC-MEDIA. All fields in VoIP messages are changed by SBC-SIG.

Encryption

Encryption is no longer necessary, due the CAC function.

Direct Firewall Support

SBC work in cooperation with NAT/firewall, but does not affect the general security policy implemented on firewall. Doing so, the security remains simple and efficient. It allows also the scalability of VoIP networks.

Reverse Proxies

There is no need for additional media gateways acting as reverse proxies, due the B2BUA behavior of SBC-SIG.

VI. CONCLUSION

SBC is now the key element for VoIP security. By having full control and visibility of all media sessions, a SBC can easy implement a scalable VoIP network architecture over multiple boundaries, all existing equipment remaining unchanged. SBC can be used as an interface between an enterprise and the service provider network, on the border between two providers with a reciprocal agreement related to VoIP traffic, or within a provider offering VPN services to its customers, to bridge calls across the customers' VPN sites.

The future large deployment of SBC depends on a standardization that is still missing, and on the acceptance of SBC's manufacturers to refer to these standards.

REFERENCES

[1] ITU-T Recommendation H.323: *"Packet-Based Multimedia Communications Systems"*

[2] *Softswitch definition* http://en.wikipedia.org/wiki/Softswitch

[3] J. Rosenberg, et al., *"SIP: Session Initiation Protocol"*, RFC 3261, June 2002

[4] H. Schulzrinne, S. Casner, R. Frederick, V. Jacobson, *"RTP: A Transport Protocol for Real-Time Applications "*, RFC 1889

[5] H. Schulzrinne, A. Rao, R. Lanphier, *"Real Time Streaming Protocol (RTSP)"*, RFC 2326, April 1998

[6] IETF RFC 3015*: "Megaco Protocol Version 1.0"*

[7] Handley, M., Schultzrinne, H., IETF RFC 2327: *"SDP: Session Description Protocol"*, April 1998

[8] C. Patrikakis, et al, *"Distributed Denial of Service"*,in The Internet Protocol Journal, Volume 7, Number 4

[9] G. Huston, *"Anatomy: A Look Inside Network Address Translators"*, in The Internet Protocol Journal, Volume 7, Number 3

[10] M. Constantinescu, *"NAT/Firewall Traversal for SIP: issues and solutions"*, ISSCS 2005

[11] P. Srisuresh, M. Holdrege, *"IP Network Address Translator (NAT) Terminology and Considerations"*, RFC 2663, August 1999

[12] J. Rosenberg, D. Drew,H. Schulzrinne, *"Getting SIP through Firewalls and NATs"*, Internet Draft, draft-rosenberg-sip-firewalls-00.txt, February 2000

[13] J. Rosenberg, H. Schulzrinne, *"An Extension to the Session Initiation Protocol (SIP) for Symmetric Response Routing"*, RFC 3581, August 2003

[14] J. Rosenberg, A. Hawrylyshen, *"SIP Conventions for Connection Usage"*, Internet Draft , draft-ietf-jennings-sipping-outbound-00 (work in progress), July 2004

[15] D. Wing, *"Symmetric RTP and RTCP Considered Helpful"*, Internet Draft, draft-wing-mmusic-symmetric-rtprtcp-01 (work in progress).

[16] J. Rosenberg, J. Weinberger, C. Huitema, R. Mahy, *"STUN - Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs)"*, RFC 3489, March 2003.

[17] J. Rosenberg, R. Mahy, C. Huitema, *"Traversal Using Relay NAT (TURN)"*, Internet Draft, draft-rosenberg-midcom-turn-06, October 2004.

[18] J. Rosenberg, *"Interactive Connectivity Establishment (ICE): A Methodology for Network Address Translator (NAT) Traversal for Multimedia Sessions Establishment Protocols"*, Internet Draft, draft-ietf-mmusic-ice-03, October 2004.

[19] B. Carpenter, *"Middleboxes: Taxonomy and Issues"*, RFC 3234, February 2002.

[20] White Paper - *SignallingProxy™ - Accelerating the Deployment of SIP Services*, http://www.newport-networks.com/whitepapers/spwpes.html

[21] J. Hardwick, "Session Border Controllers, Enabling the VoIP Revolution" www.dataconnection.com