Scientific Papers (www.scientificpapers.org)
Journal of Knowledge Management, Economics and Information Technology

Vol. II, Issue 2
April 2012

Security in VoIP

Author: **Floriana GEREA,** Economic Informatics Department, Academy of Economic Studies, Bucharest, Romania, floriana.gerea@gmail.com

VoIP relies on packet switching, similar to the way that e-mails are sent over the Internet. The technology breaks down a voice call into bite-size information packets. Instead of keeping the switch open all the time, the information is sent and received as needed, allowing excess line capacity to be used to carry other data. When the voice data arrives at its destination, it's reassembled into a voice call. As voice over IP services grow in popularity, the potential for viruses, worms and other security threats aimed at the technology also will grow. The current paper's purpose is presenting several security solutions and applying them to integrated systems at an economical and social level.

Keywords: *VoIP, DoS, SIP, ARP*

Introduction

This chapter focuses on studying existing security problems that can affect communication systems and also on presenting solutions that can improve VOIP communication technologies by extending this article's conclusions. I will be taking into consideration management strategies and the necessary resources for a better costumer orientation and risk management, all with the purpose of implementing SLA.

In VoIP technology, the employees can easily access, falsify and divulge the data. Sometime such behaviour is a disaster for a big and famous company. Some service providers develop some technical method aimed to avoid the security threats from the interior. For instance, some providers limit the authority to access and manage the hardware, monitor the procedures, and minimize the number of staff who has privilege to access the vital parts of the infrastructure. However, at the provider backend, the administrator can also access the customer's VM-machine. The users have no control nor any knowledge of what could happen to their data. This, however, is becoming increasingly challenging because as security developments are made, there always seems to be someone to figure out a way to disable the security and take advantage of user information. I propose to fix the security problem on the present, but I also prepare for the future.

The levels that can attac a VoIP infrastructure Denial-of-Service or VoIP Service Disruption

Denial-of-service (DoS) attacks can affect any IP-based network service. The impact of a DoS attack can range from mild service degradation to complete loss of service. There are several classes of DoS attacks. One type of attack in which packets can simply be flooded into or at the target network from multiple external sources is called a distributed denial-of-service (DDoS) attack. [3] DoS attacks are difficult to defend against, and because VoIP is just another IP network service, it is just as susceptible to DoS attack as any other IP network services. Additionally, DoS attacks are particularly effective against services such as VoIP and other real-time services, because these services are most sensitive to adverse network status. Viruses and worms are included in this category as they often cause DoS or DDoS due to the increased network traffic that they generate as part of their efforts to replicate and propagate. [9]

ARP Spoofing

ARP is a fundamental Ethernet protocol. Perhaps for this reason, manipulation of ARP packets is a potent and frequent attack mechanism on VoIP networks. Most network administrators assume that deploying a fully switched network to the desktop prevents the ability of network users to sniff network traffic and potentially capture sensitive information traversing the network. Unfortunately, several techniques and tools exist that allow any user to sniff traffic on a switched network because ARP has no provision for authenticating queries or query replies [4].

Additionally, because ARP is a stateless protocol, most operating systems (Solaris is an exception) update their cache when receiving ARP reply, regardless of whether they have sent out an actual request.

H.323-Specific Attacks

The only existing vulnerabilities that we are aware of at this time take advantage of ASN.1 parsing defects in the first phase of H.225 data exchange. More vulnerability can be expected for several reasons: the large number of differing vendor implementations, the complex nature of this collection of protocols, problems with the various implementations of ASN.1/PER encoding/decoding, and the fact that these protocols —alone and in concert — have not endured the same level of scrutiny that other, more common protocols have been subjected to. For example, we have unpublished data that shows that flooding a gateway or media server with GRQ request packets (RAS registration request packets) results in a DoS against certain vendor gateway implementations—basically the phones deregister [9].

SIP-Specific Attacks

Multiple vendors have confirmed vulnerabilities in their respective SIP (Session Initiation Protocol) implementations. The vulnerabilities have been identified in the INVITE message used by two SIP endpoints during the initial call setup. The impact of successful exploitation of the vulnerabilities has not been disclosed but potentially could result in a compromise of a vulnerable device. In addition, many recent examples of SIP Denial of Service attacks have been reported.

Recent issues that affect Cisco SIP Proxy Server (SPS) demonstrate the problems SIP implementers may experience due to the highly modular architecture or this protocol. The SSL implementation in SPS (used to secure SIP sessions) is vulnerable to an ASN.1 BER decoding error similar to the one described for H.323 and other protocols. This example illustrates a general concern with SIP: As the SIP protocol links existing protocols and services together, all the classic vulnerabilities in services such as SSL, HTTP, and SMTP may resurface in the VOIP environment.

Policies and Processes Encryption

All VoIP systems should use a form of Media (RTP channel) Encryption in order to avoid the sniffing of VoIP data. All communications between network elements should be encrypted. Complete end-to-end IP voice encryption is recommended to mitigate the threat of eavesdropping attempts. Additionally, all administrative access to critical server and network components must use encrypted protocols such as SSL and/or SSH. All access to remote administrative functions should be restricted to connections to the switch itself or to a designated management PC.

Physical Security

Physical security is an essential part of any security plan. Physical security refers to the protection of building sites and equipment (and all other information and software contained therein) from theft, intrusion, vandalism, natural disaster, man-made catastrophes, and accidental damage (e.g., from electrical surges, extreme temperatures, and spilled coffee). It requires suitable emergency preparedness, reliable power supplies, adequate climate control, and appropriate protection from intruders.

Safeguards can be broken down into two categories: human and environmental.

Human safeguard recommendations are:

- Console access should be restricted or eliminated.
- Logon, boot loader, and other passwords must be a minimum of eight characters including at least one each of alpha, numeric, and ctl characters.
- VoIP components must be located in a secure location that is locked and restricted to authorized personnel only.
- Access to these components, wiring, displays, and networks must be controlled by rules of least privilege.

- System configurations (i.e., hardware, wiring, displays, networks) must be documented. Installations and changes to those physical configurations must be governed by a formal change management process.
- A system of monitoring and auditing physical access to VoIP components, wiring, displays, and networks must be implemented (e.g., badges, cameras, access logs). From the point at which an employee enters the building, it is recommended that there be a digital record of their presence.
- The server room should be arranged in a way that people outside the room cannot see the keyboard (thus seeing users/admin passwords).
- Any unused modems must be disabled/removed.
- No password evidence (notes, sticky notes, etc.) is allowed around the system.
- The CPU case should be locked and the key must be accounted for and protected. A backup key should be made and kept securely offsite (e.g., in a safety deposit box).
- USB, CD-ROM, monitor port, and floppy disks drives should be removed, disabled, or glued shut.
- Adequate temperature and humidity controls must be implemented to avoid equipment damage.
- Adequate surge protectors and UPS must be implemented, maintained, and tested.
- Cleaning and maintenance people should be prohibited from the area surrounding
- Any electronics.
- Food, drink, or smoking is prohibited in the same areas.

IP-PBX equipment must be located in a locked room with limited access. This type of access must be provided as a user authentication system with either a key-card or biometric device. The use of a keypad alone to gain access is not permitted. All methods of gaining entry into the room must provide for a list of users that have accessed the room along with a date/time-stamp.

Security for the VoIP Infrastructure

One example of how to configure a secure an system cloud for VoIP is the creation of a network demilitarized zone (DMZ) on a single host.

In this example, three virtual machines are configured to create a virtual DMZ on Standard Switch 1: Virtual Machine 1, 2,3 and 4 run Web server and are connected to virtual adapters through standard switches. These virtual machines are multi homed. The Machine 5 and 6 runs an Asterisk server. The conduit between these elements is Standard Switch 2, which connects the firewalls with the servers. This switch has no direct connection with any elements outside. From an operational viewpoint, external traffic from the Internet enters Virtual Machine 1 through Hardware Network Adapter 1 (routed by Standard Switch 1) and is verified by the firewall installed on this machine. If the firewall authorizes the traffic, it is routed to the standard switch in the DMZ, Standard Switch 2. Because the Web server and application server are also connected to this switch, they can serve external requests. Standard Switch 2 is also connected to Virtual Machine 4 and Virtual Machine 5. This virtual machine provides a firewall between the DMZ and the internal corporate network. This firewall filters packets from the Web server and application server. If a packet is verified, it is routed to Hardware Network Adapter 2 through Standard Switch 3. Hardware Network Adapter 2 is connected to the internal corporate network. This network could be used for virus propagation or targeted for other types of attacks. The security of the virtual machines in the DMZ is equivalent to separate physical machines connected to the same network.

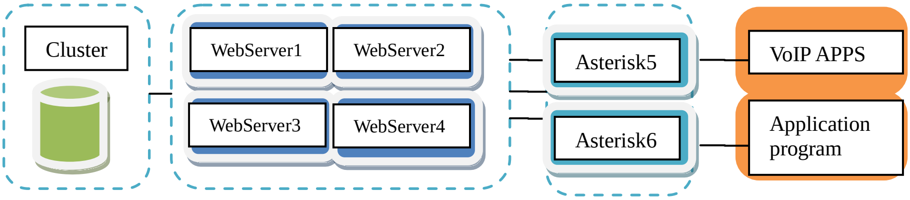

Figure 1: Architecture VoIP

VoIP is a highly critical data application and as such, is subject to all the policies detailed in other data security policy sections (this assumes that the VoIP Security Policy module is part of a larger set of security policy modules).

In the traditional VoIP technology because the information is on a single server several problems can appear regarding data availability and integrity, security and in order to resolve these, money is spend on hosting software, applications and people with the requisite expertise. On the other hand Cloud Computing is less expensive because of its financial benefits. Assuming that the hardware equipments can encounter several malfunctions, in a time when the services' quality is extremely important, the information needs to be available in real time. The traditional approach is to invest in a large number of equipments in order to avoid the loss of call and provide a correct functionality of the telephony service. However, these long term investments may be justified but at a closer analysis we can find that those equipments are not using all their resources. There has been statistically proven that most of the servers' hardware will never be fully used and as time passes they will be replaced due to moral and physical degrading. Cloud computing can solve all these aspects. Organizations can avoid large investments in equipments and software by using a much smaller number of resources for one solution. In this way investments can be made in fewer equipments with larger resources that are wiser employed, by creating a large number of virtual nods on one physical machine. By monitoring and controlling performance, organizations can easily decide which resources can be allocated on different services.

The reduction of operational costs

The major advantage of this facility is the low cost. The reducing of costs is due to utilization of the same environment both for voice transport and for data. If a company has a connexion to Internet (not totally explored), then this connexion can be utilized also for the voice transmission with no additional costs. Another cost reducing is represented by the fact that conversation between VoIP users is free. Generally, only the calls between VoIP and PSTN involve costs, while the calls between VoIP users don't involve any costs except for the connection to Internet. And because the connection to Internet already exists or is used in other purposes, VoIP telephony between its users is considered free. We also must mention the personnel costs that in the traditional method implies, because it requires a large number of people to mange resources, allocated in different geographical areas. Also, every new installation needs to be fully made, and this translates in large installation time for every new server. In cloud computing these aspects can be solved in a reduced amount of time, the installation of services taking very little. It is done by cloning other virtual nodes, so all the software and application installation is done only once and then all the new software is installed by cloning. In this way a large number of identical servers can be created within minutes, without the need to separately install each necessary application. Cloud computing reduces human error to a minimum, due to the fact that there is no need to process the same information every time. It is enough to have only one correct virtual machine, that has been tested, all the other being replicas of the first.

Improved functionality: another important advantage is that of a improved functionality as compared to classic telephony. Some of the functionalities offered by VoIP are difficult or even impossible to accomplish in the classic telephony. Among these, there is the possibility to use an IP telephone wherever there is a connexion to Internet. This creates the possibility that the "fix" telephone be taken in traveling, having the call number everywhere. The most important beneficiaries of this facility are the Call Center agencies that use VoIP telephony in foreign countries due to the reduced costs with cheaper work force.

The classical method required for each modification to restart all the installation procedures, which involved time spent and large costs. Cloud computing has the extraordinary benefit of easily moving information from one machine to another and between servers, without taking into account the geographical distance. It is possible for a virtual machine to have a node in Bucharest and to move that service within minutes on another server in Brasov, without damages or problems. Within minutes servers can be moved from one location to another, from one country to another, while keeping the service functional even while migrating. This option did not exist in the traditional method. Using this method implied that the service would not be functional for at least several days, and that the physical movement of the server from one location to another was needed as well as a list of modifications that are necessary for any physical movement. In order for a cloud application to be valid, it is essential to provide guarantees regarding the system's functionality. In the real telecommunication world, any bit loss means the interruption of the call, this leading in time to the loss of customers and losses for the business. Thus it is essential for all the information to be complete, available and secure. Because the users' demands for cloud services are varied, suppliers need to make sure that these can be flexible.

Conclusions

As a conclusion, the VoIP industry consolidates in this period its position in the market through its innovation and the high level of security and adaptability, threatening to eliminate the traditional solutions (that are expensive, unsecured and inflexible).

By innovation and a perfectible degree of security, VoIP industry is consolidating is market place, frightening to be able soon to take the place of conventional solutions (expensive, insecure and inflexible).

VoIP allows to create inexpensive systems, with little upfront costs and to be scaled to massive sizes, when needed. The advantages can be defined both by the providers, which are motivated by the future profits that can arise due to the lower costs that the classical technology, as well as the users who have the possibility of reducing or eliminating the telephony service costs.

References

[1] G. GRUMAN, E. KNORR, *What cloud computing really means. InfoWorld* (2009, May), [Online], Available: http://www.infoworld.com/d/cloudcomputing/what-cloud-computing reallymeans-031

[2] L. SIEGELE, *Let it rise: A survey of corporate IT,* The Economist, (Oct., 2008)

[3] P. WATSON, P. LORD, F. GIBSON, P. PERIORELLIS, and G. PITSILIS, *Cloud computing for e-science,* (2008), pp. 1–5

[4] A. GHENCEA, V. GAUCAN, D. PIRVU, *Distributed Systems and Web Technologies*, Journal of Knowledge Management, Economics and Information Technology, Vol. I, Issue 5, August 2011

[5] M.-E. BEGIN, *An egee comparative study: Grids and clouds – evolution or revolution*, EGEE III project Report, vol. 30 (2008)

[6] B. ROCHWERGER, D. BREITGAND, E. LEVY, A. GALIS, K. NAGIN, I. M. LLORENTE, R. MONTERO, Y. WOLFSTHAL, E. ELMROTH, J. CACERES, M.BENYEHUDA, W. EMMERICH, F. GALAN, *The Reservoir model and architecture for open federated cloud computing*, IBM Journal of Research and Development, Vol. 53, no. 4 (July, 2009), pp. 1–11

[8] *“Implementing QoS Solutions for H.323 Videoconferencing over IP”*, Cisco Systems Technical Whitepaper Document Id: 21662, 2007

[9]. P. CALYAM, M. HAFFNER, E. EKICI, C. G. LEE, *Measuring Interaction QoE in Internet Videoconferencing*, Proc. of IFIP/IEEE MMNS, 2007

[10]. S. WINKLER, *Digital Video Quality: Vision Models and Metrics*, John Wiley and Sons Publication, 2005