

## **Voice over IP: New telephony and security**

By André Fucs de Miranda, CISSP

### **Introduction**

Brazilian songwriter Chico Science used to say that “one step forward and you’re not at the same place anymore”. Unfortunately, this new place is not always the ideal world we longed to be. This is the reality that many companies are delving into the Voice over IP land are facing. Problems with security are many and, once again are driven by the usual expectation for panaceas; companies are making decisions today that will bring far too many headaches come the future.

The actual problem is identical to the one that occurred on the relation between financial institutions, internet banking, email and Trojan horses. Lured by the bright side of the new technologies, many companies find themselves damaged by not adopting efficient security devices and practices that would have protected them from the threats present in the new scenario. At the same time, IT security officers still ignore risk analysis far too often, and would rather adopt a strategy of obstructing the new technologies altogether. Therefore, devising solutions compatible with the company’s priorities will be a joint mission for both product managers and IT security officers.

Before going into further details about VoIP’s security aspects, it is interesting to look at some of the characteristics of the technology. VoIP is not only the traffic of voice over IP packets, but also includes the offer of communication services such as fax, voicemail, UMS and so on. It is also important to note that, although the VoIP market is still underdeveloped in Brazil, we shouldn’t ignore that voice transmission is just one of the first steps towards the IP Multimedia System.

We should also observe that although usually associated with the Internet, the use of this technology is not restricted to that universe, considering the worldwide increase in the number of IP telephony service providers that focus on the corporate market.

Another important characteristic of this tool is the fact that, being a result of convergence, VoIP technologies are frequently based on protocols of different origins. One example is the extensive use of the SS7 protocol and SIP on soft-switches. Besides the strong impact on the peopleware, this convergence also leads to the confrontation between different outlooks on security issues. The global telephony networks are culturally seen as restricted environments with minimal interface between the different service providers, while IP networks tend to enforce huge interaction of data.

Equally significant is the fact that on VoIP technologies, the segregation of voice and data is relatively weaker than in PSTN environments. Even though SIP, MGCP and NCS are concerned about the issue, companies are getting closer to the in-band signaling scenario present in SS5.

Still concerning the cultural distinctions between both environments, it is interesting to relate a recent experience with European professionals that occurred during a project in the Middle-East. These specialists, every one of them a veteran in telephony systems, but with little familiarity with IP technologies, nicknamed the professionals with an IP technology background *data cowboys*, due to the less-than-methodical way that the latter group worked. Historically, the telephonic system is ruled by local and international norms that specify even the environment operation methods, while the IP technology, originally conceived to resist a nuclear war, is far more flexible.

## **Security aspects**

In regards to security, a great effort is being made by developers and standard-makers to create mechanisms that guarantee the operational security of this new model. For instance, CableLabs lists the following risks in one of its standards:

- Service thievery;
- Violation of privacy;
- Signaling protocol manipulation and
- Service interruption.

The same specification offers an objective description of ways to seek protection from such menaces, particularly the service itself. The specification also describes a series of technological devices responsible for the protection of the communication channels against such menaces. Therefore, it is clear that the technology itself is not intrinsically insecure.

The security models applied to VoIP environments don't usually differ much from the ones used in secure Internet environments. One or more security devices are responsible for defining the communication limits between clients and the Call Management Servers. Generally, specialized firewalls known as Session Border Controllers – which work identically to application firewalls – are used, instead of generic ones. These SBCs are tasked with applying most of the security policies and access control, granting free access to legitimate clients and blocking the remainder of the traffic. The same model can be utilized in the communication between two companies.

Although efficient and functional, this model still has some chinks in the armor:

- Denial of Service attacks;
- Traffic analysis and
- Privilege delegation.

We will see below how well these issues are tackled by most VoIP environment security models. Most models try a generic approach, without considering the specific characteristics of the service.

### ***Denial of Service attacks***

Denial of service attacks generally happen in two different ways. The first is the exhaustion of the resources employed on the transport or processing of the service and the second is the direct compromising of the service provider. SYN Flood and WinNuke

attacks are, respectively, examples of the two types of threat. Currently, practically every security device is capable of minimizing the risks of exhaustion attacks, SBCs not being an exception. On the other hand, the level of protection against direct compromising attacks depends on the level of maturity of the equipment employed, including the SBC.

One of the major authorities on the subject has stated that several solutions, ranging from telephonic switches to media gateways, presented extremely low code maturity, being potential victims to direct attacks as simple as the infamous Ping of Death. Far from being mere baseless panic, it is indeed a real threat, as shown by two alerts issued by the CERT from Carnegie Mellon University. The consequence of the work of Finnish scholars, the CERT alerts list inconsistencies in several VoIP solutions, including a soft switch supporting up to 250 thousand phone lines. It is also a well known fact that some of the major SBC suppliers' management platforms were vulnerable to remote attacks.

Even though attacks and techniques geared against these platforms aren't widely spread on the internet at the moment, the problem still exists and it is necessary to take measures against it. It is a worrisome fact that some of the protection devices used today are of little use against these threats. With the exception of the SBCs, firewalls have little integration with VoIP protocols, and even those that do have some are more dedicated to remaining in control of the session than inspecting its content, in search of dangerous data. Considering the state of immaturity of these products the following question arises: How to protect the devices that should be protecting us?

Again employing the CableLabs standard, it is interesting to note how prominent the security issue is. Inside the MGCP protocol specification we find a topic named "Fighting the Restart Avalanche". The situation, characteristic of this protocol, tends to happen when several gateways are started simultaneously, and may provoke a jam the network, server instability and even a denial of service. Although similar to a SYN Flood, this vulnerability is noteworthy because it is described in the protocol specification and not in a document about security issues.

Nevertheless, even considering the gravity of the situation, the use of devices like SBCs is still of capital importance. All things considered, the ability of an SBC to deal directly with the signaling and voice transmission protocols adds a significant level of protection to these environments, but, for that to happen, it is fundamental that the SBCs are perceived as more than just NAT Transversal devices, which is one of their lesser tasks.

### ***Traffic Analysis***

Another important topic to consider is the high speed traffic analysis. There are many protocol analysis solutions available at the market today, but not one can guarantee the non-sampling data capture in high speed links. This means that important data may be ignored amongst the high flux of information. Obviously included in this concern are intrusion detection systems (IDS) that tend to have performance problems and packet loss when facing huge amounts of data. Considering that there are no solutions available at the moment to monitor security incidents in VoIP platforms, all these issues add up to a very dangerous scenario.

Nevertheless, there are ways to minimize the impact of such maladies, even if a definite solution still does not exist. One of the best practices is separating the traffic according to its characteristics. IP packets carrying telephonic conversation data are sent through one channel, while signaling information flows through another route. There are various manners to do that, such as the use of Policy-Based routing and Network-Based Application Recognition in Cisco platforms.

The idea behind traffic separation is quite simple. Most VoIP networks generate a large mass of packets, but if the amounts of packets containing voice and signaling are compared, the first is quite larger, while at the same time voice data is severely less complex than signaling information. This separation can be used, for instance, to provide greater granularity to an IDS, or some passive fraud prevention system.

The increasing concern surrounding traffic analysis arises from the importance of monitoring processes, a subject that, while not completely ignored, is usually recognized very timidly by companies, similarly to IDS.

The growth of wireless VoIP solutions like Voice over WiMax, or even the growth of voice-peering means that the attention given to monitoring must be doubled, for it is uncertain if the relation between high speed and monitoring will change. It is probable that, as it happens today, the data transmission technologies will evolve faster than the monitoring technologies.

### ***Privilege Delegation***

The ITU, an UN organization responsible for international telecommunication systems standardization, published in 2004 a document named “Telecommunications networks security requirements” or E.408.

Although it focus on telephony operators, this document can be interpreted with flexibility and be applied, for example, to VoIP environments of smaller scale, such a PABX. Like other previous ITU articles, the E.408 consists in a recommendation of practices to be adopted by telecom service providers. Among the several practices listed in E.408, one in particular is the need to specify the “actors or characters” in the operation of the system. According to the ITU, actors are the people or processes responsible for running a telecom network. Every time an actor acts on the network, it assumes the role of a character, such as the service’s subscriber, software or hardware provider, operator, and so on.

Also according to the document, we find the following among the security objectives in a telecom system:

- Only authorized actors should be able to access and utilize telecom networks;
- Legitimate actors should be able to access and operate the assets to which they are authorized;
- A telecom network must provide means to guarantee that the actors are prevented from having access to resources they have no right to access.

Such objectives clearly express the ITU's concern with a more efficient granular access control.

Faced with such a concern, it is natural that a convergent telecom system should present a high granularity of access rights and great capacity to register the operations being realized. Yet that is not always the case, for many VoIP solutions concentrate the majority of its efforts in the protection of the telephonic conversation, completely forsaking the system's operation.

It is important that, while respecting the limitations of each system, efforts are made towards a more efficient access control. It is of little use to totally segment a network with firewalls, cryptography and other devices if the security of the management application is simply ignored. There are some soft switches available today in which there is only one management login, an unthinkable scenario where all good practices of security are discarded. By forcing all operators to manage the system through one single login, it will be impossible to track the author of any system parameter changes.

Also of notice is the fact that in most VoIP solutions not only the call management system is critical to the environment's functions, but also DHCP servers, DNS, switches, routers and many other components. Security solutions must consider the system as a whole.

## **Conclusion and further considerations**

While IP telephony is still strong in the novelty factor, it is fundamental to see it as something more than telecommunications provider device. Well know problems like frauds in PABX systems, Voicemail and long distance communications continue to deserve attention. In this sense, the ITU's E.408 recommendation provides a very interesting approach to the subject and should be employed, along with the X.805 standard as a guide to the people responsible for the security processes in VoIP environments. It is interesting to note the way in which both documents deal with security for data and voice transmission solutions. Instead of specifying the devices and algorithms for data protection, the two documents are concerned with high level models based on classes and requirements that may serve as a basis to the security devices in a very flexible way.

Fact is that little by little VoIP is encroaching on both the home and corporate environments, and being an emergent technology, therefore going through several changes, it is extremely important that IT managers and professionals involved with it avoid focusing excessively on security devices.

Much is yet to happen in the VoIP market, and the degree of maturity of the technology involved still needs to grow, but the market clearly signals that IP media solutions will be a reality in the near future, raising the stakes in the competition between the telecom service providers. The way in which all of these systems will work in the future depends on decisions taken today.

About the Author:

André Fucs de Miranda is a Certified Information System Security Professional with more than ten years of experience in the international information security market, and has participated in some of the most important VoIP projects in the Middle East. His career includes companies such as Lucent Technologies, Unibanco and CFSEC Security Architects.