

Security in VoIP Systems

CONFIDENTIAL.

The information contained in this document is strictly confidential and property of Panda Software. This document cannot be reproduced or distributed by any means without the prior written consent of Panda Software International.

Fernando de la Cuadra
Enrique González Ochoa

©Panda Software International. January 2006

Index

Security in VoIP Systems	3
How can VoIP Systems be compromised?	4
Malware Attacks against VoIP	5
Other Effects	6
Security in VoIP used for Images	7
Conclusions	9

Security in VoIP Systems

Virus creators have always had an undeserved reputation for being intelligent people and skilful programmers with an in-depth knowledge of the mysteries hidden within computers. This reputation was doubtlessly justified in a world in which personal computers were considered strange and ultramodern, and where people with a basic knowledge of microcomputing were considered experts.

Since then, programmers who use malicious code have changed dramatically. Once thought of as being worthy of respect, they are now seen as common thieves, creating programs with the sole intention of stealing data or even for carrying out bank fraud.

More and more systems are being created to spy on and steal from computer users, and threats are being developed at the same rate as the new technologies they are attacking. As soon as e-mail became commonplace, worms had their moment of glory. Malware took advantage of the new popularity of P2P networks to reach more computers using file exchange systems. If advanced mobile telephones become popular, new threats will appear. The list could go on and on.

One technological advance which is being implemented in businesses at a very fast rate is VoIP (Voice over IP), a system which uses data networks to transmit voice conversations. This system saves the user a lot of money, as the Internet connection already in place is used to communicate telephonically without any additional cost. Some network modifications must be carried out and the telephones must be changed, but the process is not excessively expensive when compared with the telephone bills paid by medium and large-sized companies.

However, IP telephony is not free from risks, although fortunately these risks have not yet become reality. Users must not forget that the telephones and servers used for voice transmission are in fact computers which look like telephones. As a result, they have their own software, bugs and security issues.

There is another, more simple method of IP telephony which makes use of the computer's infrastructure. These systems use broadband connections to allow the users to talk via telephone. Using these connections along with speakers and microphones, you can communicate with somebody else who uses the same telephone system. It is similar to an instant messaging system but with telephones.

This is undoubtedly a novel, useful and economic system. However, just as malware adapted to new trends, is it fair to think that threats against IP telephony will also emerge?

In principle, because the technological framework underlying the IP telephone system is a programmable computer system it is perfectly susceptible to malware attacks. However, malware attacks on IP telephony are more complicated. Malware against VoIP could perhaps interrupt conversations, cutting them off or creating unwanted noise.

The attacks could also be more ingenious. For example, voices could be distorted or advertisements played in the middle of a conversation. In cases of really bad taste, strange sounds or insults could be added to the conversation.

Each of these problems could be classified as a first generation virus; in other words, viruses created by programmers who want to show how good they are at

programming through the use of hidden, self-propagating programs which manifest themselves in some visible way.

However, as we mentioned above, malicious programmers today are after something more: money. A virus attacking an IP telephone system would aim to gain direct economic benefits in some way. The first possibility, the playing of advertisements during conversations, would be the equivalent of Internet browser adware. This type of system, which in principle could give good results in advertising terms, would quickly become an unwanted feature. Protection systems should avoid unwanted intrusions during telephone calls.

In this case users would at least be aware that something strange is happening, but just imagine what would happen if the equivalent of an email worm were to attack a VoIP system. Without the user even realizing, a VoIP worm could make calls in the user's name offering products to all contacts saved in the system's telephone directory. The name of the person calling could even be hidden, so the identity of the computer infected with this talkative worm could remain a mystery.

This problem may seem quite small when compared to what could happen if calls were interfered with. A user's IP telephone system may be compromised and opened up to unwanted call diversions. If the user makes a call to a bank, for example, a Trojan could redirect the call to somewhere else where the user is asked for personal information such as PIN numbers, passwords etc... We have always been told that the best way to fight phishing is to call the bank to check that a message is authentic, but if this happens when we make what we think is a call to our real bank then we will fall victim to a quick and effective scam.

In this case, it is not just our computers that are at risk. Company routers could be affected by a call diversion code, so an anti-malware solution used on a personal computer would be of no use whatsoever.

Finally, as an equivalent to spyware, it is not unreasonable to consider the possibility of a computer code with voice recognition functions. In this way the user would be unaware that anything is wrong until he or she pronounces the words "my user name is" or "my PIN number is". At that moment the code would begin to record the conversation and subsequently forward the information to a thief who would then be in possession of supposedly secret data.

How can VoIP Systems be compromised?

The main problem faced by malicious programmers is how to insert their programs into a VoIP system. A PC offers a large number of possibilities because it is a multipurpose system in which several applications run simultaneously – for example an Internet browser, an email program etc... - in short, all tools which are used to consult information via the Internet.

It is easy to insert a malicious code in these systems without any problem, as long as the user does not have a suitable protection program in place. According to the last survey on company protection, Panda Software found that less than 30% of the companies surveyed had adequate protective measures in place.

However, even if the systems are protected, the actual implementation of the VoIP systems could result in their vulnerability to malicious programming. In the year 2003 it was announced that there was a problem with the H.323 protocol, which is used for IP telephone systems. The problem meant that, depending on the VoIP

solution manufacturer, the service may fail and there may even be buffer overflows, resulting in arbitrary code execution.

The H.323 protocol is the oldest protocol used. Many others have been developed since, including SIP, IAX/IAX2 and Skype. All these other protocols are also vulnerable to attacks which affect to a greater or lesser degree the quality of communication and compromise the security of the system at different levels.

Malware Attacks against VoIP

How can current malicious codes exploit Voice over IP communication? This is really a very interesting question. It is also interesting to examine the opportunities that are offered to malicious programmers by VoIP.

- **Trojans.** Trojans are programs which are installed in computers without the user's knowledge, and which can carry out many different actions, such as opening backdoors, stealing confidential data etc... A Trojan designed to carry out its functions in a VoIP system would be a small addition to current Trojans, so it is merely a matter of time before one is developed. "Trojan calls" would be more dangerous. For example, a person aware of a system vulnerability could make a "Trojan call" and carry out some malicious action during that call, taking advantage of a security hole in the VoIP system.

- **Worms.** Worms are self-propagating programs which do not necessarily infect system files. Although worms could try to propagate themselves via VoIP channels, this system would not make much sense.

However, it is possible to imagine the creation of a sound file (WAV, MP3 etc...) which, taking advantage of some vulnerability, could make the telephone system send the file to other systems. Here the file would reproduce itself again and be forwarded to even more systems.

- **Spyware.** This term is used to refer to programs which collect data regarding the Internet surfing habits, preferences and tastes of the user. The information collected is sent to the program writers or to a third party.

It is also possible to imagine a new form of spyware with voice recognition functions used to analyze conversations. Spyware could also take direct advantage of VoIP by trying to make calls to check if other users only use their systems at set times. In this way the program can tell if the PC is simply switched on, or is on line, but is unattended depending on whether or not the user answers the call. This would involve a small change in the way in which spyware works. While current spyware targets the infected user and collects his/her data, in this case other users are targeted as the infected user intrudes in their systems to collect information.

- **Adware.** These programs display advertisements using any possible means: using pop-ups, banners or by changing the browser homepage configured by the user etc...

Classic adware could use VoIP to interrupt calls by inserting advertisements. This system has already been used in traditional telephone systems (where users subscribe to a free telephone service) with limited success, but this method could be more successful in a VoIP system as the user would have no say in the matter.

- **Malicious Tools.** These are applications specifically designed to damage computer systems. They can have various functions: remote computer control, creation of malicious codes etc...

A tool like this could make calls to a premium-rate telephone number, generating a profit for the owners of the number. More serious circumstances could arise if a telephone helpline number is modified so that the user's call is redirected to a hacker. In this way it would be easier for hackers to obtain bank account details than it is with normal phishing.

- **Potentially Dangerous Applications.** These are legitimate programs which, in some cases, can be used in a malicious way in order to damage computer systems.

They can take the form of, for example, a malicious application under the guise of a telephone directory management tool, which is used to send the contact details in the directory to a potential attacker.

- **Spam.** Spam is unwanted electronic mail, normally containing advertisements, which is sent in bulk.

VoIP would make sending spam by telephone both cheaper and easier. In fact, the system has already been nicknamed SPIT, or "spam on IT phone".

- **Tracking Cookie.** Tracking cookies are often used by spyware programs in order to steal information. The equivalent in this case would be the theft of the call register.

- **Keyloggers.** These are programs that record which keys are pressed on the keyboard. In a VoIP system keyloggers could record which keys are pressed to make a telephone call, thus stealing information in order to carry out "spit".

Other equivalents which could be used in IP telephone systems are "micloggers" and "voiceloggers". These programs could record any PC microphone activity. Although IP telephone systems always use encryption tools to avoid man-in-the-middle attacks, if the system records a conversation before it is encrypted (or once it is decrypted), the conversation can be easily recorded.

- **RoVoIPs.** Bots, which take their name from the word "robot", are automated Trojans which carry out actions according to external orders. They are often used to send spam or to act as a bridge so that a hacker can carry out attacks on third party systems, etc... A classic bot could use VoIP systems to send "spit" to more computers, both with the information obtained from the affected system or by using information sent to it from the RoVoIP creator's own system. A RoVoIP-infected system could be made to obey orders given to it to tap the telephone line. This tapping could be known as "Gossips", which stands for "Generic order sender to IP systems".

Other Effects

As well as all these direct threats, one must consider the effects which classic threats could have on voice over IP technology. Just as worms progressed from targeting email to targeting Internet browsers, they could also begin to target VoIP.

- **Identity Theft.** A malicious application could steal a VoIP system user ID, deactivate the user's connection to avoid duplicity and use the stolen ID in its own VoIP network. In this way, the theft victim would be paying for the account when in fact the thief would be the one using it.

This use of communication lines is an update of "phreaking" techniques, which use telephone lines to make connections or have conversations unbeknownst to their legitimate owners.

- **Spyware.** Classic spyware collects information about a user's habits, and could take advantage of the new opportunities offered to it by VoIP. By collecting information about calls made, spyware could track a user's calling habits.

Spyware could also collect telephone numbers from the infected user, just as worms collect email addresses, and use them to make calls to other users.

- **DoS attacks against users.** These attacks could be carried out using a system that searches for contacts in the database or address book and sends mail to ALL those contacts. This process could even be carried out X consecutive times or indefinitely.

- **DoS attacks against VoIP providers.** Depending on the digitization and sound sampling systems used by a provider, a high frequency or low intensity noise could be played during the conversation. The user's ear or brain would not hear such a noise, but the sound sampling system would. In this way, sound samples must be obtained more quickly, and the samples themselves must be larger. As a result, customers use more bandwidth. This could ultimately result in a denial-of-service for the provider.

Security in VoIP used for Images

When we talk about VoIP our minds immediately think about what the letters themselves stand for: voice. However, we often forget that this system offers far more than just voice technology. It also uses an image transmission system which we could call LIoIP (Live Image over IP).

This type of system could lead to the creation of new types of malware based on the malicious applications used today.

- **Trojans:** A Trojan sent to a LIoIP system could take control of a video transmission system and carry out a wide variety of actions: activating and deactivating the camera at will, modifying the size of an image, changing the image contrast or resolution etc... These actions could be carried out statically by changing the image system configuration in a single move, or dynamically, allowing the attacker to access the system and alter the configuration as and when he pleases.

In addition, Trojan images could be used to send hidden messages created using steganography techniques. These messages could contain simple messages, texts to display in popup windows or codes used to load additional scripts.

- **Worms:** Worms are known for their ability to self-propagate. Worms could find their way into a LIoIP system via a malicious code taking advantage of, for example, a vulnerability in the graphic or video file management system. Via this method, the worm could execute code which would collect the addresses of other system users and send them a copy of the same image or video file.

In addition, a malicious code could be created that, instead of collecting user addresses, ran a random search of systems (using, for example, IP addresses) and identified those using a LIoIP system compatible with the infected system. The worm could then send and execute a copy of the same image or video file to these systems.

- **Spyware:** Spyware is used to collect information regarding a user's habits and tastes. In the same way, a similar code could be used to collect information regarding the user's preferences in terms of colors, shapes and brightness by tracking the images sent. These preferences could then be sent to an attacker. This information could be used to send targeted advertising (spam).

- **Adware:** For this type of malware, LIoIP systems would be heaven. Adware could carry out various different actions such as adding messages to conversations using subtitles, inserting small windows in the top and bottom corners and, in the most extreme cases, interrupting conversations by displaying a full-screen advertisement.

In addition, these actions could be carried out selectively when, for example, the application detects that the user is connected to a specific conversational partner.

- **Potentially dangerous applications:** This group would include legitimate applications which, as a result of how they are used, could have a negative effect upon LIoIP systems. For example, security software could be used maliciously by being made to send images collected from the system to a potential attacker.

- **Malicious Tools:** These are applications specifically designed to damage computer systems. A tool like this could set up videoconferences using premium rate telephone numbers (private chat lines, for example) or even to connect the affected user with a scammer pretending to be a salesman, a trader or any other professional with the aim of obtaining information from the victim.

- **Spam:** Just as email systems are used to send unwanted bulk mail, LIoIP systems could be used to send graphic advertisements in bulk to a large user database created using information obtained in various ways and from different sources.

- **Tracking Cookies:** Just as browsers use this system to obtain information regarding page visits, LIoIP systems could be used to obtain information regarding each and every videoconference which takes place.

- **Videologgers:** In traditional systems, keyloggers are used to collect information inputted using a keyboard. Similar systems will be created for LIoIP. These systems could be called "videologgers" and they would be used to capture images at fixed intervals. In addition, the more advanced videologgers could directly record video signals, saving all the videoconference information as though they were creating a backup copy. Of course, both the static images and the videoconferences would then be secretly sent to an email address or even to other LIoIP systems. (One potential problem here is the speed at which images can be sent. However, speed is increasing and such images would quickly be sent unbeknownst to the user. Victims could even be selected according to the speed of their connection).

- **RoLIoIPs:** "Robots", usually known as "bots", just as with all technology, are bound to evolve. So in a LIoIP system a network of robots could be created with the aim of capturing images from the infected system. These robots could be called RoLIoIPs. These images would be stored in a database and used for identity theft (see below) etc... The administrator of the robot network could also send spam advertising images. In a way similar to techniques used today, spam messages

could also be sent using images supposedly from banks in order to obtain the victim's details through phishing.

- **Identity Theft:** A malicious code could be used to steal user information. In this way an attacker could capture static images from the person affected. These images could be used along with other data (collected using other methods) in order to create counterfeit documents.

Such an application could also divert a real image and substitute it for static images, making the user think there was a problem with transmission speed. The images used could be images of the user taken in the workplace, or at home etc... By combining these images with the identity stolen via the VoIP system, and using a voice filter, the attacker could secretly participate in a conversation using the information and image of any other user.

- **Spying:** Using images is the most typical spying technique known today. A malicious application which accesses a user's LIoIP system would be able to monitor all the system's movements and, by taking control of the camera, be able to see the environment in which the system is located. This scenario, if applied to a business context, would mean that an attacker could consult documents, see how and where they are filed, and even observe the roles and habits of the company personnel, irrespective of their rank within the organization.

- **DoS attacks against users:** In order to carry out an attack of this sort, a malicious code could look for contacts in databases, address books etc... and send images to ALL the contacts found. These images could be very high quality and high resolution, meaning that they would require more computer resources when they are sent. It is true that these images could only be sent to LIoIP users, but in principle all VoIP users are automatically able to use LIoIP. If this is not the case, we would be faced with a cross-system attack: in other words, a denial-of-service attack could be sent to a VoIP system via a LIoIP system.

Conclusions

The outlook is really quite daunting. However, two factors combine to make us safer from these hypothetical attacks. Firstly, as we mentioned above, the creators of malicious codes are not as knowledgeable as they could claim to be in the past. Programmers can no longer be quite as imaginative when creating malicious codes, and they can now only insert these codes if there is a vulnerability in the system.

The solution to such problems again lies with the installation of VoIP systems which are well-known for their security and effectiveness, and users must be constantly aware of any new security measures, immediately applying any patches recommended by the manufacturer.

On the other hand, we must not forget that these malicious codes targeting telephone systems must be made in a very specific way. Dedicated systems hold an advantage because manufacturers are very protective of their codes and API functions (if present). PCs which use VoIP systems are the clear target. These systems use standard operating systems (Linux or Windows). Information about how to access the resources of these systems is readily available, and the systems themselves have enough vulnerabilities to allow programmers to compromise them with malicious code. Fortunately, the systems mentioned use a wide variety of well-known antivirus programs which protect them against threats of this type.

In any case, today's Internet and the spreading of malicious codes means that classic antivirus programs react too slowly and cannot control the appearance of some codes which can install themselves in and damage VoIP systems. It only takes a few seconds for the number we have stored for our bank to be changed to the number of a fraudulent call centre. In these cases, disaster can strike quickly and with extensive consequences.

The solution cannot lie with classic concepts of protection against malicious code, as the propagation that is taking place today is too fast and can have disastrous effects. A malicious code detection system is required, and such a system would also need to detect codes attacking telephone over IP network systems. Any attempt to modify essential program parameters, or any attack on the system configuration etc... could be easily identified as malicious and stopped.

Until you install intelligent systems protecting your computer from unknown codes, you must constantly review the services you have installed and your telephone configuration or you may fall victim to fraud.