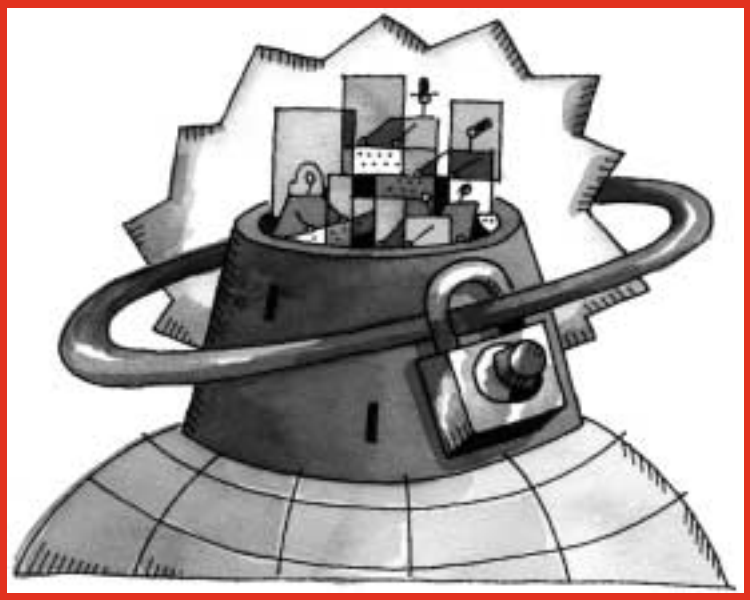
;login:
THE MAGAZINE OF USENIX & SAGE
December 2002 • volume 27 • number 6

Focus Issue: Security

Guest Editor: Rik Farrow

inside:



USENIX & SAGE
The Advanced Computing Systems Association &
The System Administrators Guild

security threats to IP telephony-based networks

by Ofir Arkin

Ofir Arkin is the founder of the Sys-Security Group, a non-biased computer security research and consultancy body. In his free time he enjoys doing computer security research. His publications and work is available from the group's Web site, *http://www.sys-security.com.*

ofir@sys-security.com

Introduction

Privacy and security are mandatory requirements with any telephony-based network. Although not perfect, over the years a certain level of security has been achieved with traditional telephony-based networks.

On the other hand, IP telephony-based networks, which might be a core part of our telephony infrastructure in the near future, introduces caveats and security concerns which traditional telephony-based networks do not have to deal with, long ago forgot about, or learned to cope with.

Unfortunately, the risk factors associated with IP telephony-based networks are far greater than traditional telephony-based networks.

The security concerns associated with IP telephony-based networks are overshadowed by the technological hype and the way IP telephony equipment manufacturers push the technology to the masses. In some cases IP telephony-based equipment is being shipped although the manufacturer is well aware of the clear and present danger to the privacy and security of the IP telephony-based network its equipment is part of.

This article highlights the security risk factors associated with IP telephony-based networks and compares them, when appropriate, with the public switched telephony network (PSTN) and other traditional telephony-based solutions.

What Is IP Telephony?

IP telephony is a technology in which IP networks are being used as the medium to transmit voice traffic.

IP telephony has numerous deployment scenarios and architectures which the following terms are usually associated with:

- *Voice over IP* (*VoIP*) – describes an IP telephony deployment where the IP network used as the medium to transmit voice traffic is a managed IP network.
- *Voice on the Net* (*VON*) or *Internet telephony* – describes an IP telephony deployment where the IP network used as the medium to transmit voice traffic is the Internet.

With any IP telephony-based deployment scenario, the underlying IP network will carry data as well as voice. The term *Converged Network* is used to describe networks which carry both voice and data. This is in contrast with the current *Public Switched Telephone Network* (*PSTN*), where voice and data are being carried on physically separated networks.

Different protocols play different roles in IP telephony. With any IP telephony-based network, several types of protocols will be responsible for different aspects of a "call":

Signaling protocols perform session management and are responsible for:

- Locating a user – the ability to locate the called party.
- Session establishment – the ability to determine the availability of the called party as well as its willingness to participate in a call. The called party is able to accept a call, reject a call, or redirect the call to another location or service.

- Session setup negotiation – the ability of the communicating parties to negotiate the set of parameters to be used during the session, including, but not limited to, type of media, codec, sampling rate, etc.
- Modifying a session – the ability to change session parameters during the call, such as the audio encoding, adding and/or removing a call participant, etc.
- Tearing down a session – the ability to end a session.

Media transport protocols are responsible for the digitization, encoding (and decoding), packing, packeting, reception, and ordering of voice and voice samples.

IP telephony-based networks also make use of other protocols and technologies which are common to any IP-based network, such as DNS and quality of service,

A Generic Call-Setup Process

When a user places a call on an IP telephony-based network, the signaling protocol its IP phone supports will locate the called party either directly or by using other servers on the network, determine the called party's availability and willingness to participate in a call, and negotiate the parameters to be used during the call.

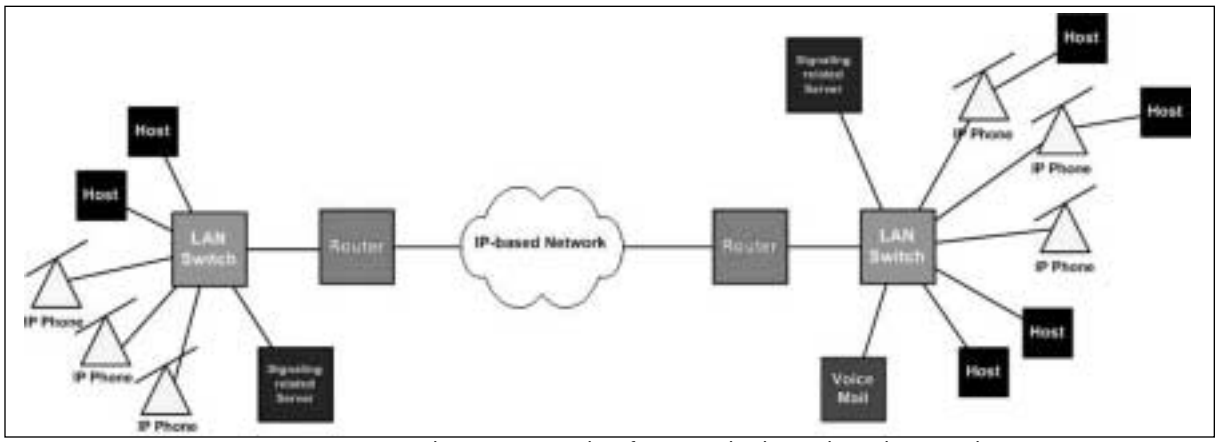


Figure 1: A very abstract example of an IP telephony-based network

The actual voice samples are carried by a media transport protocol, such as the Realtime Transport Protocol (RTP), which samples human speech according to the parameters negotiated by the signaling protocol during the call-setup process. Some, but not all, of the media protocol's operations will be controlled by the signaling protocol.

During the call, when needed, the signaling protocol is used to change a call parameter. It is also responsible for tearing down the call.

The signaling information might traverse several signaling-related servers, while the voice samples are being sent directly between call participants.

Parameters other than security and privacy, must be taken into account when designing an IP telephony-based solution. They include but are not limited to:

- Availability
- Speech quality
- Quality of service
- Scalability

Although these parameters do not seem to be linked with security, the ability of a malicious party to interfere with the operation of the network will pose a direct threat to its availability and therefore will downgrade its role as critical infrastructure.

1. A phreaker is one who engages in phreaking, cracking phone systems.

2. A softphone is telephony-based software running on a PC.

Why IP Telephony Is at Risk

IP telephony brings the terms "phreaker"[1] and "hacker" closer together than ever before. Several characteristics of IP telephony make it easier for a hacker to try to compromise and/or control different aspects or parts of the IP telephony-based network.

Compared to the PSTN, IP telephony-based networks face a greater security threat as a result of a combination of key factors outlined below.

Use of the IP Protocol

Since IP telephony is using the IP protocol as the vessel for carrying both data and voice, it inherits the known (and unknown) security weaknesses that are associated with the IP protocol.

IP Networks Are Common

IP networks are easily accessible, allowing more people to explore security issues, and for security vulnerabilities when found to be published or otherwise disseminated. This is unlike the obscurity which characterizes the PSTN.

Signaling and Media Share the Same Network

Although they might take different routes, signaling information and media (voice samples), with IP telephony-based networks, share the same medium: the IP network. Unlike the PSTN, where the only part of the telephony network the signaling and media share is the connection between the subscriber's phone and its telephony switch (thereafter the signaling information will be carried on a different network physically separated from the media – the SS#7 network), with IP telephony no such isolation or physical separation between voice samples and signaling information is available, increasing the risk of misuse.

The Placement of Intelligence

With the PSTN the phones are no more than a "dumb terminal" where the telephony switch holds the actual intelligence. With some IP telephony-signaling protocols (e.g., the Session Initiation Protocol – SIP), some or all of the intelligence is located at the endpoints (IP Phones, softphones,[2] etc.). An endpoint supporting this type of signaling protocol will have the appropriate functionality and ability to interact with different IP telephony components and services as well as different networking components within the IP telephony-based network. A malicious party using such an endpoint, or a modified client, will have the same ability to interact with these components. This is in contrast to the PSTN, where a phone is only able to interact with its telephony switch.

The ability of an endpoint to interact with more IP telephony-based elements and network components poses a greater risk of misuse for an IP telephony-based network compared with the PSTN, where the switch a phone is connected to is the most likely to be attacked.

No Single Authority (Entity) Controls an IP Medium (the Network)

With several IP telephony architectures, the signaling and media information will traverse several IP networks controlled by different entities (e.g., Internet telephony, different service providers, different telecom companies). In some cases, it will not be possible to validate the level of security (and even trust) that different providers will

enforce with their network infrastructure, making those networks a potential risk factor and an attack venue.

The Nature of Speech

Without adequate speech quality, subscribers/users will avoid using IP telephony solutions. Speech quality with IP telephony is a function of several key factors, such as latency (delay), jitter (delay variation), and packet loss. With the PSTN some of these factors were long ago dealt with or are a non-issue.

A good example is jitter. During a call setup with the PSTN, a dedicated communication path between several telephony switches, also known as a trunk, is set, allowing a voice passage between the call participants. Since this is a dedicated communication path, voice traffic between the call participants will take the same route during a call. Therefore jitter is less likely to occur.

The number of factors affecting speech quality, and the ways to stimulate those conditions, are far greater with IP telephony-based networks than with the PSTN.

Unacceptable speech quality is an availability problem, which jeopardizes the critical infrastructure tag IP telephony has.

IP Telephony Infrastructure

The IP telephony infrastructure is usually put together from standard computer equipment and in many cases is built upon known operating systems, which are fully functional. The IP telephony infrastructure components interact with other computer systems on the IP network. They are thus more susceptible to a security breach than the equipment combining the PSTN, which is usually proprietary equipment whose operation is somewhat obscure.

Components of the IP Network

Networking components and the other computer equipment (e.g., network servers) combining to make up the IP network that serves the IP telephony infrastructure are the same common components found in many other IP networks. They offer other attack venues.

IP Telephony Protocols

IP telephony-related protocols were not designed with security as their first priority or as a prime design goal. Some of those protocols added security features when newer protocol versions were introduced. Other IP telephony protocols introduced some security mechanisms only after the IETF threatened not to accept a newer version of the protocol if security was not part of it. Despite such demands and an effort to introduce "decent" security mechanisms within some IP telephony protocols during their design phase, in some cases inappropriate security concepts were adopted only to satisfy the IETF. Some of those security mechanisms were simply not enough, regarded as useless or impractical, giving a false sense of security to the users of these IP telephony protocols.

An example of a security technology that might cause more harm than good is encryption. Encryption affects voice quality, since it adds delay on top of the usual delay experienced with an IP telephony-based network. Although some IP telephony-related protocol specifications mandate the use of encryption, it is sometimes simply not feasible to use encryption with those protocols. An example is the draft version of

IP telephony-related protocols were not designed with security as their first priority or as a prime design goal.

the new RTP protocol, which mandates the use of triple-DES encryption. We should not forget that most IP phones today are not powerful enough to handle encryption.

VPN technology is another good example of a security-related technology that degrades voice quality. Where we have more than two or three encrypted IP telephony "tunnels," voice quality is usually unbearable, the result of current encryption technologies combined with realtime multimedia demands.

Some security mechanisms offered by different IP telephony protocols might break the protocol functionality and even the functionality related to an IP telephony-based network.

IP telephony protocols are open to malicious attack to the degree that the attacker would be able to compromise and/or control different aspects or parts of the IP telephony-based network. The PSTN enjoys some level of obscurity in relation to security, the kind of obscurity which is not possible for a set of protocols using an openly developed IP telephony solution.

The fact is that IP telephony-based protocols are still going through several development cycles. The requirements for privacy and security are not being correctly balanced with what is feasible.

Supporting Protocols and Technologies

IP telephony protocols pose a threat to the security of IP telephony-based networks, but so do the supporting protocols and technologies that are usually part of an IP network; among these, we can name application protocols (e.g., DNS, quality of service) and internetworking technologies (e.g., Ethernet, Token Ring), and the list is long. Taking advantage of a supporting protocol or a technology being used in the IP network serving the IP telephony-based components might allow a malicious party to control different aspects or parts of the IP telephony-based network.

Physical Access

With IP telephony, physical access to the network or to some network component(s) is usually regarded as an end-of-game scenario, a potential for total compromise. A malicious party gaining physical access to the network or to a network element will have several key advantages over one having a similar physical access to PSTN equipment. This is a direct result of the way IP networks work, the placement of intelligence in some IP telephony-based networks, and the boundaries of physical security and access with the PSTN.

For example, if a malicious party is able to gain unauthorized physical access to the wire connecting a subscriber's IP phone to its network switch, the attacker will be able to place calls at the expense of the legitimate subscriber while continuing to let the subscriber place calls at the same time. With the PSTN, a similar scenario would unveil the malicious party when the legitimate subscriber took the handset off hook.

Design Flaws with IP Telephony Protocols

The IP telephony-related protocols contain several design flaws – not easily identified, but costly – that would allow an attacker to cripple an IP telephony network. One such flaw is a signaling protocol that does not maintain knowledge of changes made to the media path during a call. If one is able to abuse the media path, the signaling path will remain unnotified and clueless about the changes performed to the media path.

Another example is a signaling protocol that does not have an integrity-checking mechanism.

AVAILABILITY, OR LOW-TECH IS VERY DANGEROUS

IP telephony-based networks face a serious risk of availability. The availability risk does not result only from availability-based attacks against protocols, endpoints, network servers, and/or the kind of attacks designed to reduce the quality of speech or that target simple equipment malfunction(s). The main risk, and one that is even more basic, is the lack of electricity to power endpoints (e.g., IP phones) and other elements making up an IP telephony-based network or infrastructure.

NO ELECTRICITY? – NO SERVICE!

The electricity availability problem may strike anywhere along the path from one subscriber to another, anywhere on the network. While service providers would have to have redundancy and means to solve power-down problems as part of their license terms (at least in most Western countries), for a corporation, a small-to-medium business, or an individual subscriber this problem is more critical.

For a business the question of redundancy and power down means additional cost and economic burden, but for the subscriber at home it might mean life and death.

For a subscriber the phone is the critical infrastructure. Whenever things go wrong, the first thing most people do is to use their phone to get help. An IP phone depends on power. With most IP phones, power can be drawn either from a direct connection with an electricity outlet, or if the network infrastructure and IP phone supports it, from the LAN (power-over-LAN). If electricity is cut either to the subscriber's house (or any other location an IP phone is being used at) or to the network switch the subscriber's IP phone is connected to, the IP phone is useless.

For a subscriber, an IP phone simply cannot be depended upon as a critical infrastructure component if no electricity backup solution is available.

REDUNDANCY

If one IP telephony element fails within an IP telephony-based network and there is no redundancy, there is no availability either.

It all comes down to the economic burden of supporting availability in an IP telephony-based network.

Taking into account the other availability risks and targets within IP telephony-based networks, availability becomes one of the biggest concerns.

DIFFERENT IP TELEPHONY ARCHITECTURES

Although sharing the same basic threats, various deployment scenarios and IP telephony architectures differ from each other by the overall risk factor presented and the attack venues a malicious party might use. Securing IP telephony-based solutions is more complicated and challenging than securing the PSTN, where the major security issue is fraud.

IMPROPER IP TELEPHONY NETWORK DESIGNS

The currently offered network designs for the implementation of IP telephony-based networks do not provide proper mechanisms to defeat several basic hazards to the IP telephony network.

We can name a couple of examples:

IP telephony equipment (devices) is not being authenticated to the network, and this makes the work of the phreaker easier; in some cases, by plugging a rogue device to the network, free phone calls can be made.

In many IP telephony-based networks an IP phone's (that is, the user's) actual location is not checked against the credentials it uses. It is not enough that the network switch is able to perform "port security" and bind the port connected to an IP phone with the phone's MAC address. There should be a mechanism to correlate between the credentials presented, the MAC address the phone is using, and the physical port on the network switch it is connected to.

Non-Trusted Identities

Without the proper network design and configuration of an IP telephony-based network, one cannot trust the identity of another call participant. The user's identity, the "call-ID" information (i.e., a phone number or other means to identify a subscriber in IP telephony-based networks), is easily spoofed using any one of a variety of scenarios. An identity-related attack might occur anywhere along the path signaling information is taking between call participants.

A malicious party might use designated software to perform digital impersonation, adding to the attacker's arsenal of available tools, when spoofing an identity of a call participant or a targeted call participant, where the voice samples might have been gleaned from the IP telephony-based network itself.

Unlike IP telephony-based networks, spoofing identities with the PSTN is a much harder task to perform, and is usually performed only at the endpoints, where someone other than the intended subscriber answers the subscriber's phone, for example, or a calling party claims to be someone he/she is not.

What Is at Risk?

Everything is at risk. With IP telephony there is even greater meaning to the phrase that the security of a particular architecture is only as good as its weakest link. Multiple venues exist for a malicious party to choose from in order to launch an attack against an IP telephony-based network. Most disturbingly, in most cases it is only a question of subverting one network server or one IP telephony element (e.g., IP phones)[3] to achieve complete control over an IP telephony-based network or its functionality.

Conclusion

Each and every potential security threat examined within this article has shown that IP telephony-based networks face a greater risk of being breached than the Public Switched Telephone Network. Unfortunately, mitigating the risks highlighted within this article is not simple.

When examining the current IP telephony-based protocols and network designs, it is clear that both need to undergo major changes.

3. For more information, please see *http://www.sys-security.com/html/projects/VoIP.html*.