Why E.T. Can't Phone Home?
Security Risk Factors with IP Telephony based Networks

Ofir Arkin
Founder
The Sys-Security Group
ofir@sys-security.com
http://www.sys-security.com

November 2002

Abstract

IP Telephony based networks, which might be a core part of our Telephony infrastructure in the near future, introduce caveats and security concerns which traditional telephony based networks do not have to deal with, have long forgotten about, or have learned to cope with. The security risk is usually overshadowed by the technological hype and the way IP Telephony equipment manufacturers push the technology to the masses. This paper highlights the different security risk factors with IP Telephony based networks.

Contents

Figures

1.0 Introduction

Privacy and Security are mandatory requirements with any telephony based network. Although not perfect, along 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, introduce caveats and security concerns which traditional telephony based networks do not have to deal with, have long forgotten about, or have learned to cope with.

Unfortunately, the risk factors associated with IP Telephony based networks are far greater compared to 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 manufacture 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 paper 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.

2.0 What is IP Telephony?

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

IP Telephony has numerous deployment scenarios and architectures in 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 packetized voice 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 packetized voice is the Internet

With any IP Telephony based deployment scenario the transport medium, the IP network, is able to carry data as well as voice. It is in contrast with the *Public Switched Telephony Network* (*PSTN*) where voice and data are being carried on physically separated networks. The term *Converged Network* is used to describe networks which carry both voice and data.

2.1 The IP Telephony Protocols

Different protocols play different roles with IP Telephony. With any IP Telephony based solution several types of protocols will be responsible for different aspects of a 'call':

- **Signaling Protocols**, performs session management and 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, this includes, but not limited to, type of media, codec, sampling rate, etc.[1]
  - **Modifying a session** – The ability to change a session's parameter(s) 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 call (and the session)

- **Media Transport Protocols**, responsible for the digitization, encoding (and decoding), packing, packeting, reception, and ordering of voice and voice samples

[1] A session will be established between call participants after the called party will agree to participate in the call ("answer the phone").

Like any other application that uses IP, IP Telephony will make use of other protocols and technologies which are associated and common with any IP based network.

2.2 A Generic Call Setup Process

When a user places a call on an IP Telephony based network, the signaling protocol its IP Phone uses, and the IP Telephony based network supports, will locate the called party, either directly or by using other signaling servers (and in some case other signaling protocols) on the network and will determine the called party's availability and willingness to participate in the call. If the called party accepts the call request the signaling protocol is used to negotiate the set of parameters to be used during the call and a session will be established between the call participants.

Speech will be carried by a media transport protocol, such as the *Real-Time transport Protocol* (*RTP*), which will sample the human speech with the appropriate codec according to the parameters negotiated by the signaling protocol during the call setup process. Some, but not all, of the media transport protocol's operation will be controlled by the signaling protocol.

During the call, when needed, the signaling protocol will be used to change a call's parameter(s). The signaling protocol is also responsible for tearing down the call.

Signaling information sent between different participants of a call might traverse through several signaling related servers until it reaches another participant(s), while the packetized voice is usually sent directly between call participants.

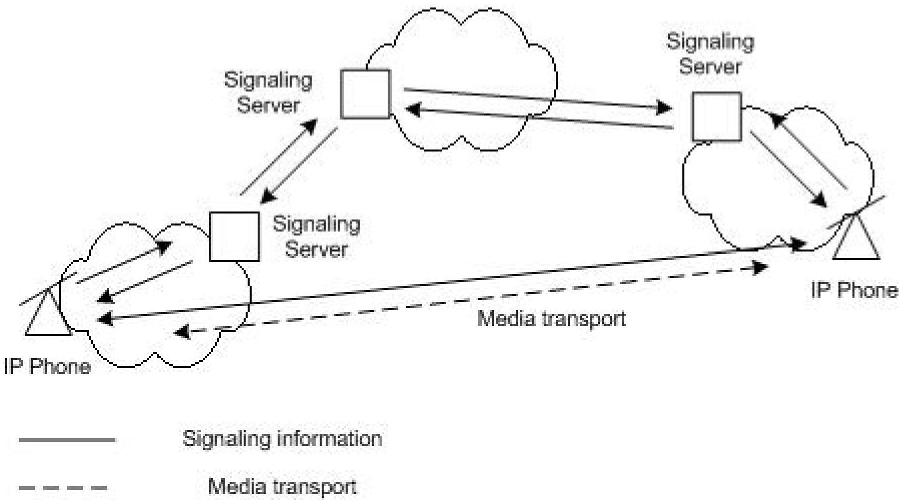

Figure 1: An abstract example of an IP Telephony-based Network

2.3 Different IP Telephony based Architectures

2.3.1 A Carrier

A Carrier can use IP Telephony as part of its infrastructure (i.e. core network) and/or as part of its service offerings.

Any telephony architecture which connects an IP Telephony based network(s) with the PSTN has to have elements which will translate signaling information and packetized voice between the IP Telephony IP network, the PSTN and vice versa. Several types of gateways are used:

- A *Media Gateway* (*MG*) – A network element which converts audio signals carried on telephone circuits into data packets carried in packet switched networks, and vice versa
- A *Media Gateway Controller* (*MGC*) – A network element used to control a Media Gateway
- A *Signaling Gateway* (*SG*) – A network element which converts SS#7 signaling information from the PSTN into formats understood by the IP Telephony elements in the IP network and vice versa. A signaling gateway also provides an accurate view of the IP Telephony-based elements of the IP network to the SS#7 network and vice versa

The IP Telephony signaling protocols are divided into the following categories:

- Protocols used between a Media Gateway and Media Gateway Controllers (i.e. MGCP, Megaco), also known as *Gateway Control Protocols* (*GCP*)
- Protocols used between a Media Gateway and a Signaling Gateway (i.e. SCTP, M2UA, M3UA)
- Protocols used between Media Gateway Controllers to initiate a session between users (i.e. the *Session Initiation Protocol - SIP*)
- Protocols used within the IP Network (i.e. SIP)

A Carrier using IP Telephony as part of its core network and/or service offerings would enjoy significant cost savings resulting from:

- **Lower equipment cost** – With traditional telephony networks one vendor would be selected to build an entire telephony network supplying a Carrier with proprietary hardware, application software, operating systems, training, and future development of services and enhancements. It would bind the Carrier with the vendor for a long term since it would not be cost effective for the Carrier to replace the proprietary equipment, or let a third party implement new services and/or enhancements (the vendor's equipment is proprietary therefore it would take more time for a third party to develop new services and/or enhancements compared with the vendor's own development team).

Compared with traditional telephony networks, IP Telephony equipment is combined from standard computer equipment which is mass produced and therefore is less expensive than the proprietary hardware traditional telephony networks are built from. But the main advantage for a Carrier building an IP Telephony based infrastructure is the ability to use different vendors to build, or supply, different parts of the IP Telephony based network as well as the ability to easily replace or add elements to the network.

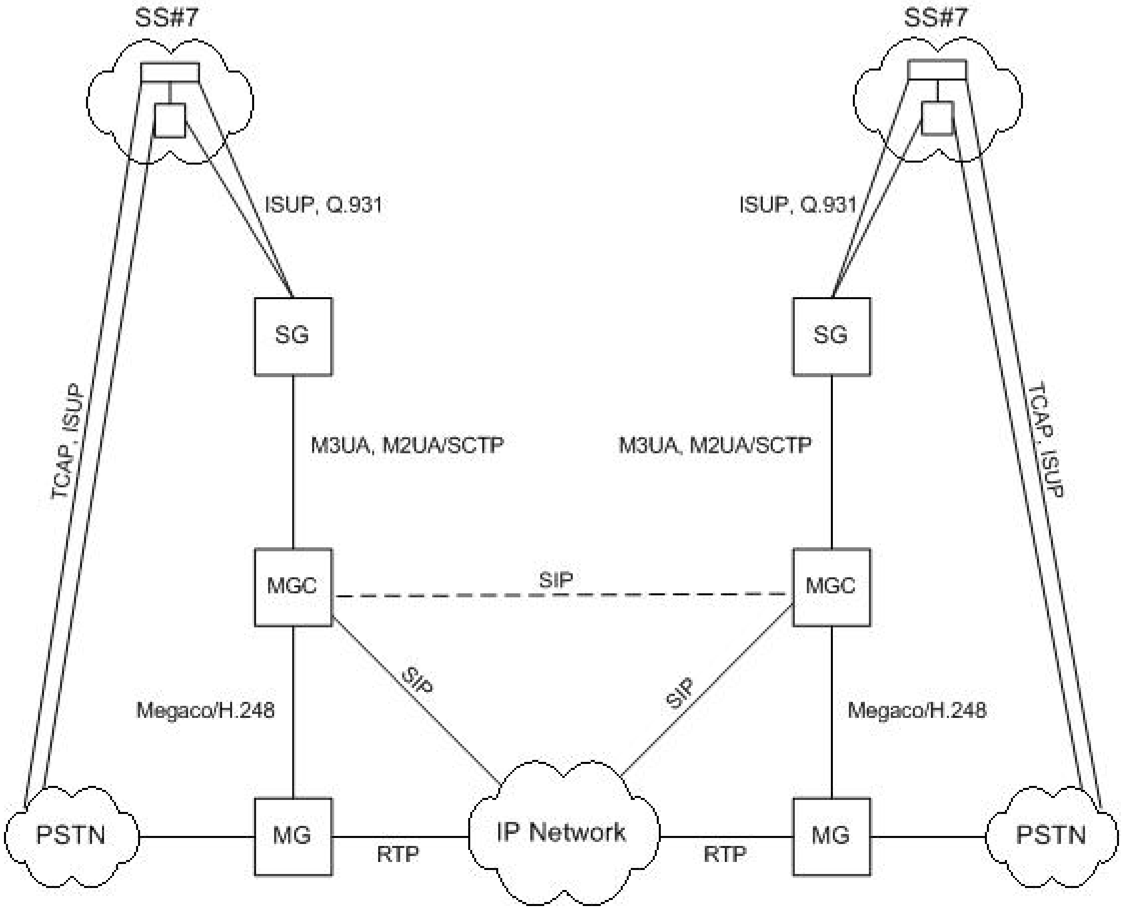

Figure 2: An example of a VoIP-based network connected to the PSTN with the relevant telephony protocols[2]

- **Lower bandwidth requirements** – Unlike traditional telephony that is limited to the usage of ITU recommendation G.711 codec scheme, and therefore transport voice at the rate of 64kbps, IP Telephony based networks can use other

[2] Converged Network Architectures: Delivering Voice and Data Over IP, ATM, and Frame Relay, Oliver C. Ibe, John Wiley & Sons.

sophisticated coding algorithms that will enable speech to be transmitted at lower rates such as 32kbps, 16kbps, 8kbps, etc.

Unlike traditional telephony networks with IP Telephony based network an accepted codec scheme can be negotiate, enabling the usage of a variety of codec schemes and the ability to easily introduce new codecs in the future. With traditional telephony codecs other than the ITU recommendation G.711 codec scheme cannot be used unless all telephony switches within the telephony network will be upgraded.

Since a large portion of a Carrier's operational costs are associated to its transmission capabilities, using IP Telephony as part of a Carrier's infrastructure can significantly reduce bandwidth requirements and save money.

- **The ability to introduce new services** – With traditional telephony networks new services are either not possible to be introduced or are hard to implement due to several constraints with the way traditional telephone networks are built. A Carrier using IP Telephony as part of its service offering will enjoy the ability to implement, and introduce, new services to its subscribers which will increase the Carrier's revenue.

- **Quick time-to-market** – The IP standards are more open and flexible than the telephony standards enabling a Carrier with IP Telephony as part of its infrastructure to implement new features and new services quicker.

2.3.2 An Internet Telephony Service Provider (ITSP)

An *Internet Telephony Service Provider* (*ITSP*) belongs to the new bread of telephony service providers. An ITSP uses IP to provide low cost voice connections through the combinations of the Internet, leased lines, and the PSTN.

An ITSP uses the Internet as the main transport medium for carrying packetized voice and signaling information to and from its subscribers. Both the ITSP and its subscribers will be connected to the Internet; the ITSP via a fast dedicated link(s) while the subscribers using their existing connections to the Internet (dial-up, xDSL, etc.) via different *Internet Service Providers* (*ISPs*).

A subscriber is able to use different methods in order to place a call, all requiring the subscriber to present its credentials before the call request will be processed. A subscriber is able to use a softphone, which is a telephony based application installed on a PC, an IP Phone, or any other hardware based solution (i.e. different phone adapters) to place the call.

An ITSP's infrastructure includes support for authentication, billing and other required features. The ITSP uses voice gateways placed in different countries, and connected to the ITSP's IP backbone through leased lines, as hooks to the local traditional telephony networks in the countries the voice gateways are deployed in. The ITSP will direct a call request to the appropriate voice gateway according to the number dialed. The voice gateway will translate the packetized voice (if the call request was acknowledged by the called party) and signaling information carried by IP-based protocols to information that can be carried by protocols used with traditional telephony networks and vice versa.

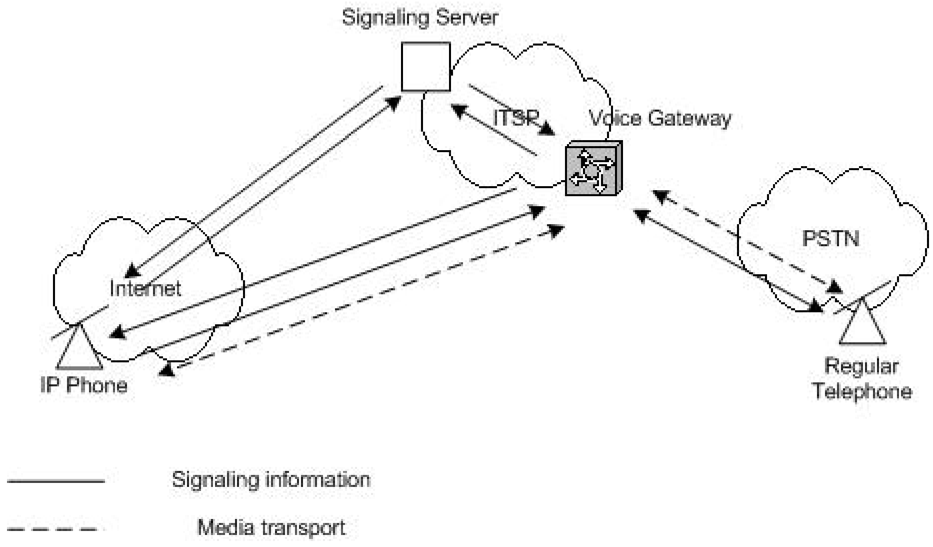

Figure 3: An abstract example of an ITSP architecture

Because the Internet is its main medium to transmit packetized voice, an ITSP does not have to build a full blown telephony infrastructure and therefore enjoys significantly lower maintenance costs compared with traditional carriers enabling the ITSP to offer low cost long distance and international phone rates.

The problem with the ITSP module of operation is the usage of the Internet as "part" of the ITSP's infrastructure, and therefore the inability to ensure quality of service (enough bandwidth, no congestion, etc.) which might lead to a reduced quality of speech.

2.3.3 A Corporate

Most of the existing IP Telephony based solutions and products are aimed at the corporate market where the cost reductions associated with deploying an IP Telephony based solution are the highest.

Instead of running two separate networks for data and voice, a corporate can use one IP based network to run both. Usually the data and voice will be virtually separated using technologies such as *Virtual LANs* (*VLANs*).

Instead of using the traditional telephone network to place calls between different corporate branches it is possible to save the long-distance charges, imposed by the PSTN, when using the same dedicated leased lines (or VPNs over the Internet) used by an organization to transmit data between its branches to carry packetized voice as well.

Corporate employees working from remote offices will be able to easily remotely connect to the corporate data and voice network. It would enable remote employees to receive and make phone calls at a remote location if they are at the office using the same phone number.

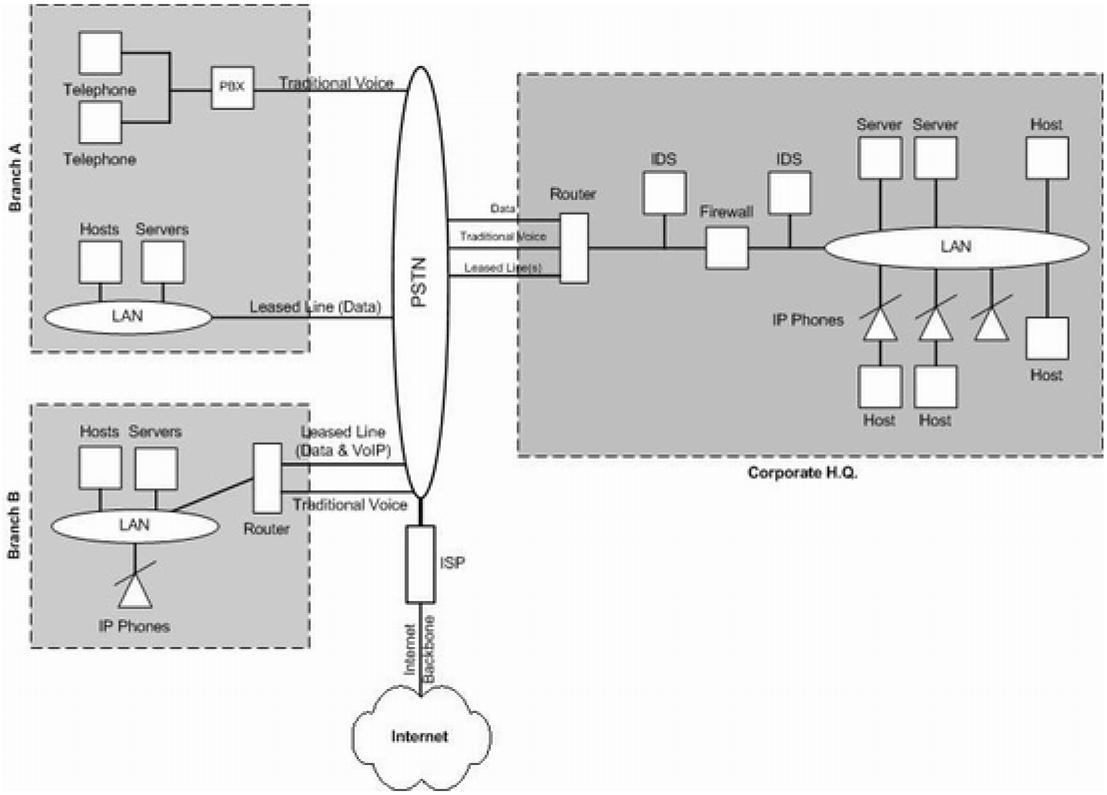

Figure 4: An abstract example of an IP Telephony solution within a corporate

Another benefit, which is common with all IP Telephony based solutions, is the ability to integrate voice and data applications. For example, dialing a phone number from a PC, checking voice mail using an e-mail client, etc. which are most valuable and useful in a corporate environment.

2.4 Other Important Parameters with IP Telephony

When designing an IP Telephony based network different parameters, other than security and privacy, must be taken into account. They include but not limited to:

- **Speech quality** – Without adequate speech quality IP Telephony based solutions will not be adopted. Speech quality with IP Telephony is a function of several factors such as latency (delay), jitter (delay variation), packet loss, and other. With traditional telephony networks some of these issues are long dealt with, or are a non-issue.

- **Quality of service** – Combined from a number of parameters quality of service is a major concern with IP Telephony based networks. Whenever a subscriber wishes to place a call the subscriber should be able to do so while the appropriate bandwidth should be preserved. If large data transfers occur in the same time, priority must be given to the voice traffic over the data traffic to prevent queuing, latency and packet loss from occurring. Even if the converged network is congested it should not affect the voice traffic. In order to be able to prioritize traffic and reserve bandwidth IP Telephony based networks should use *quality of service* (*QoS*) based solutions.

  Unfortunately not all IP Telephony based solutions are able to maintain quality of service (i.e. Internet Telephony).

- **Availability** – Rated as the second most important issue with IP Telephony after speech quality, availability is a must. Availability must be maintained at the same ratios as with traditional telephony. For example, Carrier grade Telephony networks are available 99.999% of the time. It means a downtime of only 5 minutes per year. Carrier grade Telephone operators who wish to rely on IP Telephony based technology to offer telephony services are required to have the service available exactly as it is today – 99.999% of the time.

- **Scalability** – An IP Telephony based network is required to be scalable and to support hundred of thousands of concurrent connections/calls as it is today with circuit switched telephony networks and solutions. An IP Telephony based network needs to maintain the ability to grow with demand.

Although the parameters discussed within this section do not seem to be directly linked with the security of an IP Telephony based network, the ability of a malicious party to interfere with the operation of an IP Telephony based network will pose a direct threat to its availability (i.e. various *denial of service* (*DOS*) attacks).

3.0 Security Issues with IP Telephony-based Networks

IP Telephony allows the terms "Phreaker"[3] and "Hacker" to come closer then ever before because of the convergence between telephony and IP. Several characteristics of IP Telephony make it easier for a phreaker/hacker to try to compromise and/or control different aspects or parts of an IP Telephony based network.

The security threat associated with IP Telephony is far greater than with regular telephone networks. It is combined from a number of different factors that needs to be evaluated before any deployment of IP Telephony based solution. A number of key factors raise the security threat level and are enumerated within this section.

3.1 The Usage of the IP Protocol

IP Telephony is using the IP protocol as the vassal for carrying voice; therefore it inherits the known, and unknown, security weaknesses that are associated with the IP protocol.

3.2 IP Networks Are Common

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

3.3 The Signaling Information & Packetized Voice Share the Same Network

With any IP Telephony based network, although they might take different routes, the signaling information and the packetized voice share the same medium, the IP network. Unlike the PSTN, where the only part of the telephony network both the signaling and voice will share is the connection between the subscriber's phone to its telephony switch, where thereafter the signaling information will be carried on a different network physically separated from the voice (the SS#7 network), with IP Telephony no such isolation or physical separation between signaling information and packetized voice is available, increasing the risk level of misuse.

3.4 Voice & Data Share the Same Network

With any IP Telephony based deployment the underlying IP network is able to carry data as well as voice. It is in contrast with the PSTN where voice and data are being carried on physically separated networks.

[3] A Phreaker is one who engages in phreaking, cracking phone system(s).

Although several technologies can be used to virtually separate voice and data when they share the same IP network, such as *virtual LANs* (*VLANs*), these technologies and other measures might be bypassed and defeated increasing the risk level of misuse.

Interference with the operation of the voice network is possible utilizing the data network (and vice versa), since both virtual networks will be sharing the same network equipment. For example denial of service attacks launched from the data network targeting shared network equipment such as a switch.

3.5 The Placement of Intelligence

With traditional telephone networks the phones are no more than a "dumb terminal" where the telephony switch holds the actual intelligence. The phones are able to interact only with the telephony switch they are connected to.

With some IP Telephony signaling protocols (i.e. SIP) some, or all, of the intelligence is located at the end-points (IP phones, softphones, etc.). An end-point, using or supporting this type of a signaling protocol(s), 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 end-point, or a modified client, will enjoy the same interaction abilities.

The ability of an end-point to interact with different IP Telephony elements and network components poses a greater risk of misuse for IP Telephony based networks compared with traditional telephone networks where the telephony switch, a phone is connected to, is the most likely to be attacked[4].

3.6 No Single Authority Controls an IP Medium

With some IP Telephony architectures signaling information and packetized voice will traverse several IP networks controlled by different entities (i.e. Internet Telephony, different service providers, different telecom providers, etc.).

In some cases it will not be possible to determine the level of security (and even trust) different providers enforce with their IP Telephony based networks, making those networks a potential risk factor and an attack venue for malicious entities (i.e. compromising a provider's IP Telephony based network might lead to attacks on signaling information and packetized voice sent from another provider).

[4] Traditional telephone network are also exposed to fraud.

3.7 The Nature of Speech

Without an adequate speech quality IP Telephony based solutions will not be used. Speech quality with IP Telephony is a function of several key factors such as latency (delay), jitter (delay variation), packet loss, and other. With the PSTN and traditional telephone networks some of these factors are long 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 it is a dedicated communication path, voice traffic between call participants will take the same route during the entire call. Therefore jitter is less likely to occur.

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

Although unacceptable speech quality might be categorized as an availability problem, in some cases the ability to stimulate those conditions is a result of a security breach (i.e. the ability of a malicious party to directly control some characteristics of the IP Telephony based network).

3.8 The IP Telephony based Network Components

3.8.1 The IP Telephony Components

IP Telephony components[5] within the IP Telephony based network will usually be combined from standard computer equipment, and in many cases built using known operating systems, which are fully functional. The IP Telephony components interact with other computer systems on the IP network, and are more susceptible to a security breach than the equipment combining the PSTN which is usually proprietary equipment which also means its way of operation is somewhat obscure.

3.8.2 The Other Components

Other than the IP Telephony enabled elements the IP Telephony based network will also be combined from common components found in any other IP network such as networking components, network servers, etc.

They make another attack venue possible.

[5] Components with IP Telephony functionality.

3.9 The IP Telephony-based Protocols

3.9.1 Design without Security in Mind

An IP Telephony based protocol designed within the *Internet Engineering Task Force* (*IETF*) will be developed by a specific working group within the organization.

Most of the IP Telephony related protocols were not designed with security in mind or as a prime design goal. Some security related capabilities were introduced with newer versions of some IP Telephony based protocols. With other IP Telephony related protocols security mechanisms were introduced only after the IETF threatened not to accept a proposal for a newer version of a protocol if security mechanisms will not be introduced.

While demands had been made, reality turned out to be different.

While an effort was made to have some "decent" security mechanisms with some IP Telephony related protocols, in some cases security concepts which are not appropriate were adopted. Some of these security mechanisms are simply not enough, regarded as useless or impractical, giving a false sense of security to the users of these IP Telephony protocols.

3.9.2 Design Flaws with IP Telephony Protocols

Several design flaws exists with IP Telephony related protocols that would allow a malicious attacker to cripple an IP Telephony based network. These design flaws are not easily identified, but when knowledge is acquired the severity of those issues is high.

For example, a signaling protocol which is not maintaining knowledge about changes made to the media path during a call. If one is able to abuse the media path, the signaling path will not be notified and will not have a clue about the changes performed to the media path during the call.

A malicious attacker can intimately learn IP Telephony protocols to the degree the attacker would be able to compromise and/or control different aspects or parts of the IP Telephony based network. The PSTN enjoys some aspects of obscurity when dealing with security, the kind of obscurity which is not possible for a set of protocols combining an IP Telephony based solution, which are openly developed.

The matter of fact is that IP Telephony based protocols are still going through several development cycles. The author's opinion is that the requirements for privacy and security are not being correctly balanced with what is technically feasible.

3.10 The Supporting Protocols & Technologies

Not only do the IP Telephony based protocols pose a threat on the security of IP Telephony-based networks, but also the supporting protocols and technologies which are usually part of an IP network. We can name application protocols (e.g. DNS, Quality of Service), internetworking technologies (e.g. Ethernet, Token Ring), and the list is long.

Taking advantage of a supporting protocol or a technology used with an IP Telephony based network might allow a malicious party to control different aspects or parts of the network.

3.11 Physical Access

With IP Telephony physical access to the wire, the network or to a 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 wire, the network or to a network element will be able to have several key advantages over a similar scenario with the PSTN and traditional telephone networks. The advantage is a direct result of the way IP networks work, the placement of intelligence with some IP Telephony based networks, and the boundaries regarding physical security and access posed 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 in the same time allowing the subscriber to place calls without interference. A similar scenario with the PSTN would unveil the malicious party when the legitimate subscriber will take his phone's handset off hook.

3.12 Availability, or Why Low-Tech is Very Dangerous

Availability is one of the must important issues which IP Telephony needs to deal with. If IP Telephony technology is to be taken seriously availability must be maintained as it is today with traditional telephone network. For example, the downtime of a Carrier's telephone network is 5 minutes per year, which means availability of 99.999%.

Traditional factors[6] are not the only availability related risks with IP Telephony based networks.

3.12.1 No Electricity? – No Service!

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

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

For a subscriber the phone is a critical infrastructure. Whenever things go wrong, and help is needed, the first thing most people would do is to use their phone to get help. An IP Phone

[6] Availability-based attacks against protocols, end-points, network servers, and/or the kind of attacks designed to reduce the quality of speech, or target simple equipment malfunction(s)

needs 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 using Power-over-LAN technology. 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 dependent as a critical infrastructure component if no electricity backup solution is available.

3.12.2 Redundancy

Availability is also affected by failure and malfunction of IP Telephony based elements within an IP Telephony based network. Therefore redundancy is required to overcome situations were such a malfunction will cause a service outage. Redundancy has its own price, an economical burden which will usually be the main factor in deciding if redundancy will be supported and to what degree.

3.13 Improper IP Telephony Network Designs

Most of the current offered network designs for the implementation of IP Telephony based networks do not offer proper mechanisms to defeat several basic security threats to IP Telephony.

We can name several examples:

- IP Telephony based elements are not being authenticated to the network. This makes the work of the new age 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 no correlation is performed between an IP Phone's (a user's) physical location to the network credentials it uses. It is not sufficient that a network switch will be configured to use "port security" and bind the port connected to an IP Phone with the IP 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 the IP Phone is connected to

3.14 Improper Adoption of Security Technologies

In an effort to overcome security threats which are associated with Telephony and with the usage of IP, some security related technologies from the IP world were adopted. Unfortunately not all of the adopted technologies are appropriate and beneficial for IP Telephony.

The use of *Virtual Private Network* (*VPN*) technology is a good example for a security technology that currently does more harm than good. When using a VPN to encrypt signaling information and packetized voice sent between two locations the encryption/decryption process adds additional latency on top of the experienced latency and degrades the speech quality. Higher utilization of the VPN directly contributes to a poorer speech quality. It is the affect of current days known encryption technologies combined with real-time multimedia demands.

One solution might be the usage of encryption directly between call participants without the intervention of elements in the IP network. But this would highlight other issues that will need to be addressed (i.e. firewalls will lack the ability to filter voice related traffic according to unique parameters used with the protocols, end-devices would have to use more powerful CPUs, etc.).

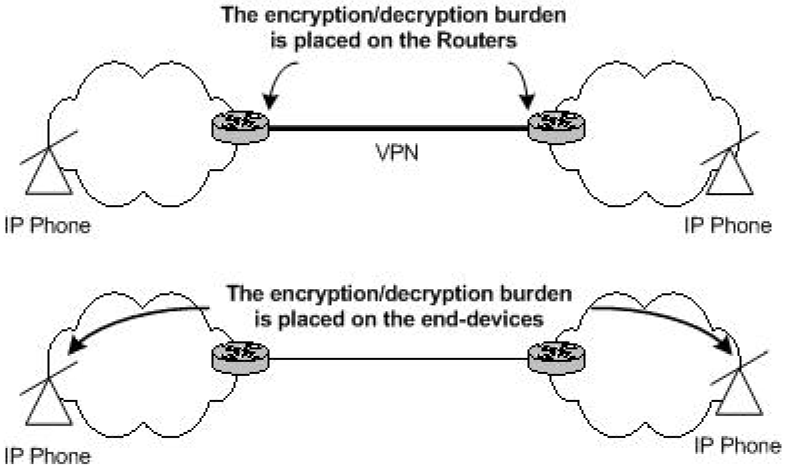
The encryption/decryption burden is placed on the Routers
VPN
IP Phone
IP Phone
The encryption/decryption burden is placed on the end-devices
IP Phone
IP Phone

Figure 5: An example with the usage of Encryption

3.15 Different IP Telephony Architectures

Although sharing the same basic threats, different deployment scenarios and different IP Telephony architectures differ from one another with the overall risk factor presented, and the attack venues available for a malicious party.

Securing IP Telephony based solutions is more complicated and challenging than securing the PSTN, were the major security threat is fraud.

A good example would be the ITSP module of operation where the signaling information exchanged between the subscriber and the ITSP will be encrypted while the packetized voice exchanged between the call participants will be sent in the clear.

3.16 Non-Trusted Identities

Without a 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 (e.g. a phone number or other means to identify a subscriber in an IP Telephony based network), with IP Telephony based networks is easily spoofed using one of a variety of methods. An identity related attack might occur anywhere along the route 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, usually performed only at the end-points (e.g. phones) when someone else other than the intended subscriber answers the subscriber's phone, or a calling party claims to be someone he/she is not.

4.0 What is at Risk?

Everything is at risk.

With IP Telephony there is a greater meaning to the phrase that a security of a particular architecture is as good as its weakest link. Multiple attack venues exist for a malicious party to choose from in order to mount an attack against an IP Telephony based network.

In order to achieve complete control over an IP Telephony-based network or of its functionality in some cases a malicious party might have to subvert only one network element (e.g. IP Phones[7]).

4.1 Vulnerable Targets with IP Telephony-based Networks

A malicious party can take advantage of multiple attack venues when targeting an IP Telephony based network. Different IP Telephony based architectures will have different risk factors, but all will share the same basic set of vulnerable targets:

- The information exchanged between call participants
- Identities
- IP Telephony elements
- IP Telephony functionality
- Network elements, Servers, Hosts, and IP functionality within the IP Network

4.4.1 The Information Exchanged Between Call Participants

One of the most valuable information sources for a malicious party is the information exchanged between call participants – the signaling information, controlling various aspects of a call, and the packetized voice.

The call related information exchanged between call participants is exposed to a number of possible attacks. First and foremost signaling information and packetized voice can be eavesdropped (i.e. rough devices in the network, specialized software, etc.), altered, jammed and actively modified.

Successful attacks targeting the information exchanged between call participants might lead to:

- "**Call Tracking**", logging of the source and destination of all numbers dialed
- "**Call Hijacking**", directing a participant or participants of a call to a node not representing an intended recipient
- **Availability problems** (i.e. denial of service)

[7] For more information please see http://www.sys-security.com/html/projects/VoIP.html.

- **Privacy breaches** (i.e. the ability to record the conversation, unknowingly being a part of a conversation, etc.)

Although abusing the information exchanged between call participants usually requires a malicious party to have access to the wire or to a network element, other venues exist for the attacker to produce similar results (i.e. compromising a network element within an IP Telephony network). If the compromised element is essential to the IP Telephony functionality of the network the end result might be a total compromise of the Telephony functionality. For example, unauthorized access to an IP Telephony signaling server would allow a malicious party to collect all signaling information exchanged between call participants routed through the signaling server; actively modify signaling information exchanged between call participants, and total control of all calls which their signaling information is routed through the compromised server.

In order to gain unauthorized physical access to the wire a malicious party might target different parts of an IP Telephony based network. Not only are the IP Telephony equivalents of the 'last mile'[8] and the 'local loop'[9] a target, but the entire IP Telephony network.

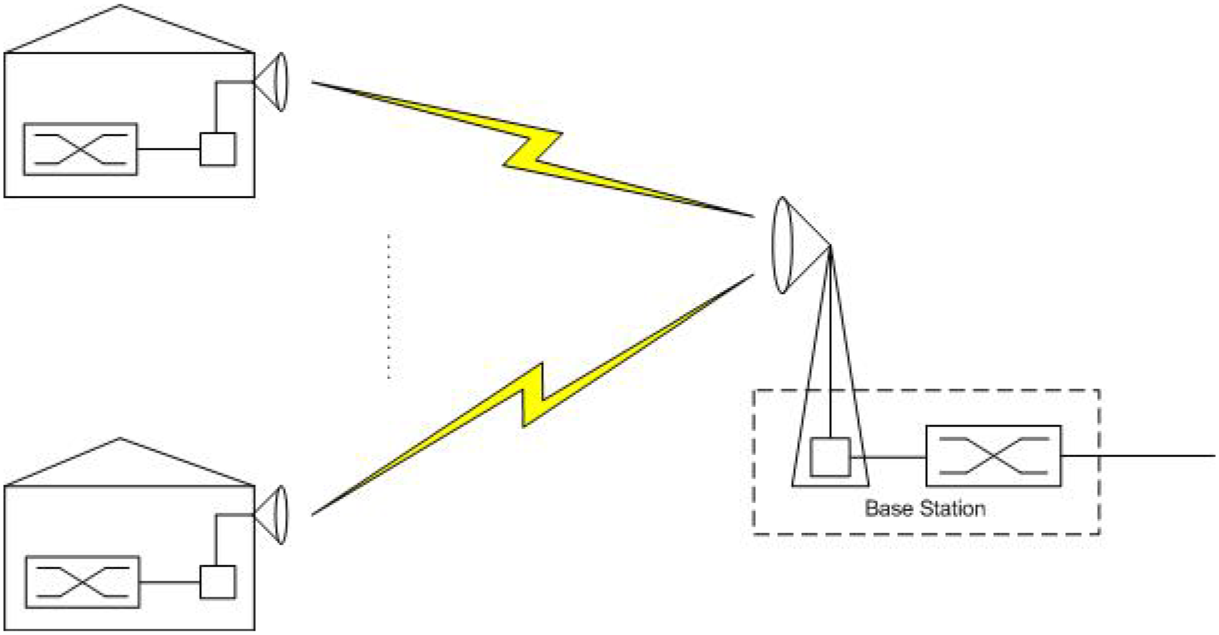

Figure 6: An example of LMDS deployment

[8] The last-mile is defined as the link between a subscriber to the telephone company's central office switch.

[9] The pair of cooper wires physically connecting your telephone with a central office switch is known as a *local loop*.

Creative ways can be used to gain unauthorized access to the wire. For example, if *Local Multipoint Distribution Service* (*LMDS*) technology is being used as part of an IP Telephony based network transmission medium. If encryption is used between a Base Station to a residential transceiver it will cripple the connection so badly that several LMDS equipment manufactures admits it will be useless to use (price vs. performance vs. available bandwidth). If the link between the Base Station to the residential transceiver will not be encrypted, than any malicious party using the right equipment will be able to gain unauthorized access to data and voice passing through[10].

In the case physical access to the wire is gained, simple computer equipment will be needed, were the malicious party is not likely to be spotted and discovered due to the nature of IP communication.

4.4.2 Spoofing Identities

By spoofing one or more of the following identities: a call participant, an IP Telephony element (i.e. an IP Phone, an IP Telephony based server, etc.), a network element or any other entity within the IP network, a malicious party might be able to perform:

- "**Call Hijacking**", call requests that will be redirected to another node instead of the intended node representing the destined participant. This might be achieved by impersonating to an end-point, registering as the destined participant with a 'registration' service, redirecting call requests using a signaling protocol's response code(s), manipulating outgoing call requests by impersonating to an IP Telephony entity (e.g. server), etc.
- **Hijacking of the signaling path**, by adding a rough device to the route taken by signaling information sent between call participants
- **Active modifications** to the signaling information and/or to the packetized voice exchanged between call participants
- **Availability related attacks**, for example, call requests that will be rejected
- **Integrity and authenticity problems**, for example, the real legitimate user, which a call destined to its end-point, was hijacked, denying a conversation ever took place
- **"Toll Fraud"**, a malicious party might impersonate as an IP Telephony signaling server and "request" an end-device to perform authentication before dealing with its call request. Using the end-point's IP Telephony network credentials the malicious party will be able to authenticate to any IP Telephony based server as well as to place free of charge phone calls. The malicious party will have the ability to perform any other functionality the end-point's network credentials allows within the IP Telephony based network (e.g. registering as the destined participant with a 'registration' service, performing "Call Hijacking", etc.)
- There are other interesting outcomes which are possible

A malicious party might use designated software to perform digital impersonation, adding to its arsenal of available tools, when spoofing an identity of a call participant or a targeted call

[10] Commercial software for sniffing traffic (radio) is available for this type of communications.

participant, where the speech samples might have been gleaned from the IP Telephony network.

If an appropriate encryption scheme and digital certificates are not being used by IP Telephony elements during the entire duration of a call, then there are no means to validate a call participant's identity. The 'Call-ID' information cannot be trusted since it can be easily spoofed (i.e. one can choose any 'Call-ID' information for its IP Phone to display since it is part of any IP Phone's userland configuration).

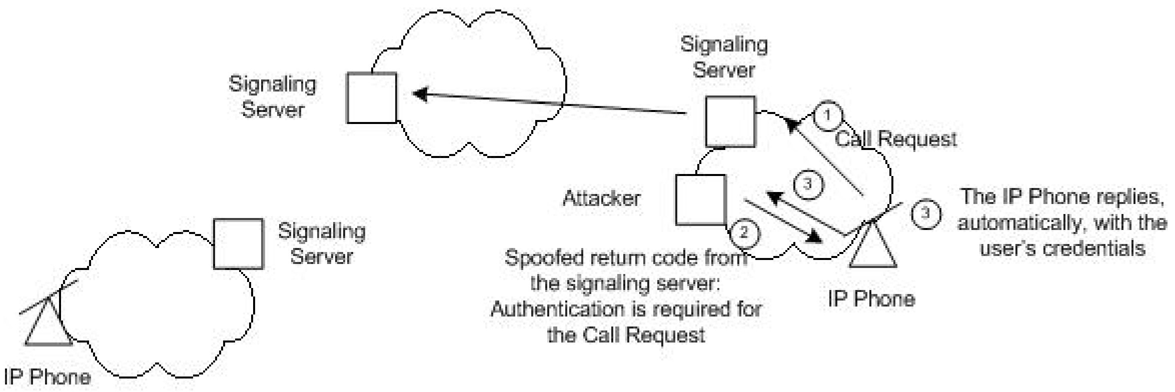
Signaling Server
Signaling Server
Signaling Server
1
Call Request
Attacker
3
The IP Phone replies, automatically, with the user's credentials
3
2
Spoofed return code from the signaling server: Authentication is required for the Call Request
IP Phone
IP Phone

Figure 7: Toll Fraud example

4.4.3 IP Telephony Elements

Any network element with IP telephony functionality is a target for an attack. If a malicious party will be able to compromise such a device the attacker will usually gain such privileges that will allow the attacker to completely control the telephony functionality of the element.

4.4.3.1 An End-Point is the Target (IP Phone, Softphone, etc.)

A malicious party able to compromise an end-point IP Telephony based device (i.e. an IP Phone, a softphone, or any other client software or hardware) will be able to control any aspect of the device's operation. Compromising such an end-point can be done remotely or through physical access gained to the device. A malicious party might modify the operational aspects of such an end-point device[11]:

- The underlying operating system stack might be altered so the presence of the attacker will not be noticed

- A modified firmware with malicious modifications might be uploaded and installed

[11] For a more information http://www.sys-security.com/html/projects/VoIP.html.

- Modifications made to the IP Telephony application software or to the end-point's network settings might allow:
    - Incoming call requests to be redirected to another end-point without giving any notification to the user of the compromised end-point
    - Calls to be monitored
    - Signaling information and/or packetized voice to be routed through another device and to be tapped and/or modified
    - The availability of the end-point will be jeopardized. For example, rejecting any call request(s) automatically or eliminating any visualization affects triggered by an incoming call (i.e. sound, vision, etc.). Calls can also be interrupted unexpectedly (some IP phones would allow this from a web interface)
    - There are other possible outcomes

- Back doors might be implemented

- Any user credentials stored on the end-point device might be extracted

- And a wealth of other scenarios and issues

Unauthorized access gained to an IP Telephony end-point device might be a result of a compromise of another element on the IP network, or from information gleaned from the network (e.g. IP phones which use HTTP Basic authentication to allow users and administrators to authenticate to the IP phone's web server).

4.4.3.2 An IP Telephony Server is the Target

A malicious party might target IP Telephony based servers which provides the IP Telephony network with certain telephony based functionality. Compromising such an entity will usually lead to the total compromise of the IP Telephony network the telephony server is part of.

For example, if a signaling server will be compromised a malicious attacker will be able to totally control the signaling information for different calls which their signaling information is routed through the compromised server. Having control over the signaling information will allow an attacker to change any call related parameter.

Viruses, Worms, and Malicious Code

If an IP Telephony based server is using common computer equipment and operating system it might be a target for viruses, worms, and even malicious code. For example, some IP Telephony networks using the Cisco Call Manager servers were affected by the 'Nimda' worm which has crippled their functionality and the availability of the IP Telephony networks they served.

4.4.4 IP Telephony Functionality

A malicious entity might choose to target a certain functionality provided by an IP Telephony element. By attacking the particular functionality an attacker might be able to subvert the IP Telephony network's functionality or interfere with its availability.

4.4.5 Network elements, Servers, Hosts and IP Functionality & Technology within the IP Network

Any network element, network server, and host being part of an IP Telephony based network's infrastructure are a potential target for an attack. Gaining unauthorized access to the network, and to the information exchanged, might be an easier task for a malicious party when the attack targets would be networking elements, network servers, or hosts with access to the IP Telephony network.

Most of the IP networking gear, and computer equipment, used by IP Telephony based networks will be found in most of today's IP networks. Security issues discovered with IP networking gear and computer equipment (e.g. operating systems) and software can be easily adopted in targeting the same components, present in IP Telephony based networks.

A malicious party can take advantage of a particular protocol, functionality or IP technology used within the IP Telephony network. A malicious party enjoys a wealth of attack venues to choose from and is not limited with the attack methods and its arsenal of tools.

5.0 Conclusion

Securing an IP Telephony based solution is not a trivial task. One must evaluate the security risks associated with an IP Telephony based solution, and try to find a proper remedy, before any deployment. Asking the right questions during (and before) the design phase will save later embarrassments when the IP Telephony based solution will be deployed and operational.

It is crucial to understand the different threats with IP Telephony. New technologies and their first implementations usually suffer from poor security. It usually takes several design cycles for a new technology until an adequate level of security is achieved. IP Telephony is still not at that stage with its development.

6.0 Related Work and Reference

6.1 Advisories

Arkin Ofir, “More Vulnerabilities with Pingtel xpressa SIP-based IP Phones”, August 2002
http://www.sys-security.com/archive/advisories/More_Vulnerabilities_with_Pingtel_xpressa_Phones.pdf

Arkin Ofir & Anderson Josh, “Multiple Vulnerabilities with Pingtel xpressa SIP Phones”, July 2002
http://www.sys-security.com/archive/advisories/a071202-1.txt

6.2 Papers

Arkin Ofir, “The Cisco IP Phones Compromise”, September 2002
http://www.sys-security.com/archive/papers/The_Trivial_Cisco_IP_Phones_Compromise.pdf