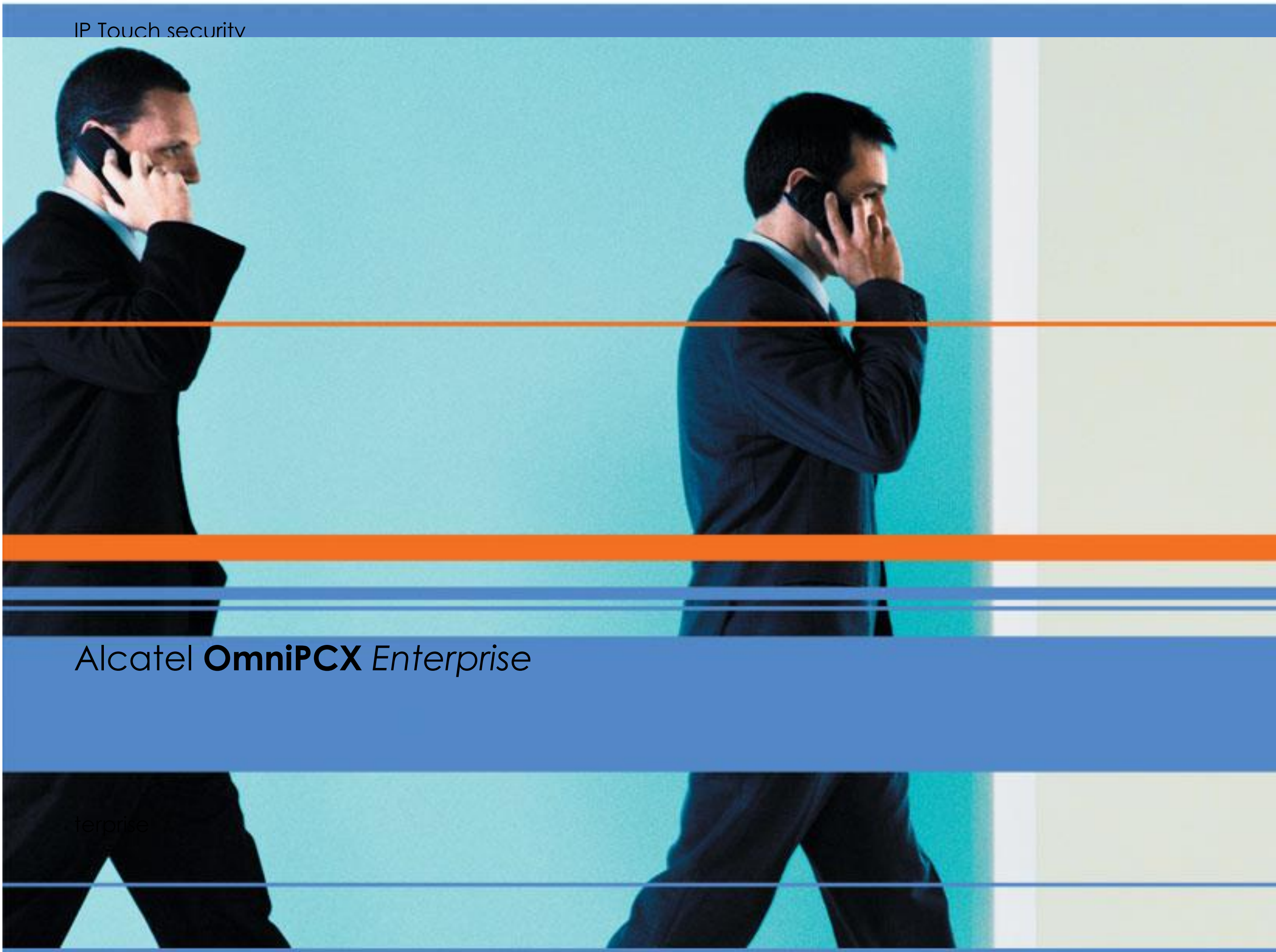
IP Touch security



Alcatel **OmniPCX** *Enterprise*

terprise

IP Touch Security

VoIP communications security: analysis of threats 8AL020033391DRASA ed 1

Security of VoIP communications in OmniPCX Enterprise: Analysis of threats and mitigation.

1. Introduction

IP communication systems bring new security challenges unknown in legacy "Time Division Multiplex" networks.

Security is often an issue put forward by customers to justify not adopting or delaying migration to IP telephony.
Furthermore, in order to migrate to IP, some specific customers will require unprecedented security levels.

Among the risks identified on IP are of course Denial Of Service attacks (see resource (1)), which could have an huge impact on the availability of the system, but also risks of eavesdropping conversations.
As IP networks are "shared" networks, IP flows could be captured either by sniffing directly on the path or by redirecting the flow to a sniffer by using Man In the Middle attacks and identity spoofing.
The risk is also increased because the tools necessary to perform theses attacks can be found easily by anybody on the Internet and any user with a PC could become a threat to the confidentiality of communications.

There are solutions to limit risks of capturing IP communications flows on IP at the infrastructure network level (LAN switching, Voice and Data VLAN partitioning, ...), these are not always easy to implement and do not answer all security threats .
Therefore VoIP encryption (i.e securing at the application level instead of network level) is a more robust solution to protect confidentiality of VoIP communications, as an alternative or complementary to some infrastructure level security.
VoIP encryption brings an additional layer of security to the network layer: even if the flow is captured, it is not possible to decrypt it.

This document identifies the different threats that can put the security of communications at risk , the solutions implemented on the network infrastructure or on OmniPCX Enterprise level that allow to mitigate or suppress the consequences of an attack.

2. Eavesdropping of VoIP media communications

One of the major security issues with real time media is interception of communications flow.

The way to eavesdrop Voice communications on Ethernet medium is to:

- intercept traffic on the Ethernet network
- decode the file in order to replay it on an audio device .

A number of tools exist to intercept and decode traffic on Ethernet/IP. These "sniffers " are
generic tools like Ethereal or are "hacker" type tools, but still freely downloadable on the Internet.
Here is a non comprehensive list:

- Ethereal http://www.ethereal.com/
- Ethercap http://ettercap.sourceforge.net/
- Arp-sk: http://www.arp-sk.org/
- Dsniff http://www.monkey.org/~dugsong/dsniff/
- VoIPong http://www.enderunix.org/voipong/
- Vomit, ….

2.1. *Intercepting voice traffic on LAN made of Ethernet hubs*

Threat:
Ethernet was originally a shared medium. This means that any terminal that was connected to Ethernet could "listen" to the traffic flowing on the medium. Therefore intercepting traffic on a "hub" LAN is easy, if the attacker is on the same IP subnetwork than a target user.
Intercepting traffic on another IP subnetwork is not possible through this way.

Solution: LAN switching
Using LAN switches ports to connect IP phone devices will route traffic from end device to end device. 3rd party will not have direct access to this flow even if it is connected on the same LAN.
LAN switching for VoIP is also mandatory for QOS reasons so that this risk does not exist.

2.2. Intercepting traffic on LAN made of Ethernet switches: port mirroring

Threat : Port Mirroring
Port mirroring allows to replay all the traffic flowing on a Ethernet port on another Ethernet port.
Capturing the traffic is then an easy task.

Solution a: Port mirroring is not accessible to an end user and requires access to the switch management. So if it is not considered as a risk, there is nothing to do.

Solution b: Encryption of voice communications will not prevent the communications of being intercepted but it will not be possible to decrypt it without knowing the encryption key (which is not accessible to an attacker).
Encryption is provided by IP Touch Security.

2.3. Intercepting traffic on LAN made of Ethernet switches: ARP spoofing

Threat : ARP spoofing allows an attacker to intercept traffic from a target user by poisoning the ARP cache of the target device, replacing the MAC@ of the destination IP@ (typically the router) by its own MAC@.
There are a number of tools that use ARP based attacks to intercept traffic: see list in previous chapter.

Solution a: at infra level (LAN switches), Dynamic ARP Inspection (DAI) controls that @IP/@MAC
associations are legitimate.

Solution b: Voice and data VLANs (with ACLs)
As ARP does work only inside an IP subnetwork, using separate subnetworks for voice and data would not allow a user with a PC to intercept traffic on a different IP (voice) subnetwork.

Implementing Voice and Data VLANs is helpful for QOS enforcement by VLAN, to protect from broadcast storms coming from the data VLAN etc… but it is questionable for security because of a PC could intrude in the Voice VLAN through VLAN hopping.

With VLAN hopping, a user with a PC could ~~to~~ to tag the Voice VLAN ID and intrude in the Voice VLAN.
Once there, it is possible to intercept calls using ARP spoofing attacks.
Because LAN switch ports supporting IP telephones with voice/data VLAN have to accept 802.1 q frames, this could also be used by an attacker.

Some vendors are able to override 802.1Q tagging from PCs on the PC port of the telephone, but if the user takes the LAN cable from the phone and connect it to the PC he will be able to tag, except if some sort of "strong" authentication is performed (802.1X).

Therefore protecting against VLAN hopping is not easy to achieve.

Solution c:
Alcatel IP Touch phones do not accept Gratuitous ARP, which normally change the ARP cache of the Ethernet device. They only update ARP cache when they decide to do it. This does not protect against any ARP based attack but mitigates this risk.

Note: an infra level solution, like binding a MAC @ to a LAN switch port, does not protect against ARP spoofing attacks.

Solution d:
Analog to ARP spoofing, if attacker as physical or telnet access to an IP phone, it could modify the IP phone parameters in order to redirect the flows to the attacker device (which acts as a router)
This threat is mitigated by Alcatel IP Touch having an administrative password to access to element configuration. Modifying IP parameters like subnet mask or default router is not possible without having this admin password.
Modifying these IP parameters by Telnet is not possible either.

Solution e:
There are a number of means to avoid that a data flow is being intercepted. But this is not guaranteed and a number of the solutions described above could have some drawbacks and constraints on the manageability of the infrastructure.
An alternative solution is not to avoid that the flow is captured but avoid that the capture flow can be exploited by the attacker. This is done by encrypting the voice media flow through SRTP and future proof Encryption algorithm (AES), an encryption key long enough (128bits) and last but not least a performing random generator for encryption keys, so that there is some predictability on the key which would simplify decryption. Moreover, if key is changed for every communication, security is even stronger.
Encryption also allows to protect fax communications. But tools to rebuild a fax are not (yet) common.
Encryption is provided by IP Touch Security solution.

3. Unauthorized access to Call Control flows

3.1. *Eavesdropping Call Control*

Threat: Eavesdropping call control information flowing between an IP phone and a Communication Server.
Eavesdropping could give access to sensible user information such as:

- user password for accessing protected feature on OmniPCX Enterprise (substitution virtual office,..)
- user passwords -, for accessing applications using voice medium –voice mail or email through Text To Speech, telephone numbers -who calls who-,
- voice encryption keys to endpoints

- An attacker could also get information on the source and destination IP addresses for a RTP flow and be able to sniff RTP media.

Eavesdropping call control requires the same tools as described before (ARP spoofing)

Solution a: on infrastructure level, idem as for media (see previous chapter)

Solution b: encryption of call control signalling protects the confidentiality of information : what has been intercepted is not readable by the attacker

3.2. Modifying the Call control information between IP Phone and Com Server

Threat: Modifying the information exchanged between IP phone and Com Server could allow to activate features on an IP phone without this being requested by the end user or by the Call Server. This is done through a Man in the Middle attack.

- The most simple one is to intercept a set of frames packets and to replay them to the IP phone some time after. This could lead to unexpected behaviour on IP phone and is more to considered as Denial of Service attack.
- More sophisticated attacks could be launched if the attacker understands the call control signalling protocol. For instance displaying a message on the phone display.
- It could for instance modify the IP addresses sent to endpoints to set up the RTP flow, so that an attacker could reroute the RTP flows to his machine and then eavesdrop conversations.
- An attacker could theoretically also set up a call between an IP phone in a meeting room and its own hacking device in order to listen discretely to the live conference without of course being detected .
- An attacker could also call a user through an intercom type call: victim's telephone hangs up automatically without ringing, allowing for discrete listening in the room.

Solution: Integrity and anti-replay on call control between Com server and IP phone ensure that messages between IP phones and Com server is not modified by third party. This is based on the use of a symmetric key that has been negotiated (through IKE) when the signalling session is open between Com server and IP phone. That key will be used for authentication and integrity of the call control signalling.

3.3. Theft of identity that allows an attacker device to be recognized as a legitimate IP phone for Com Server

Threat : A attacker machine could spoof the identity of a legitimate IP Phone in order to get access to its account and steal resources on the Communication Server (toll fraud for instance, that is making long distance calls without being charged).

Solution 1: Because of the use of a proprietary call control protocol whose specs have been distributed only to trusted partners, the risk of theft of resources is minimal even with basic authentication.
This would not be the case with SIP endpoints , where SIP soft client are available freely and could theft the identity of legitimate SIP endpoints.

Solution2: Use "strong" authentication provided by IP Touch Security. OmniPCX Enterprise use a strong authentication mechanism between IP Touch phones, Com servers and IP Media-gateways. It is strong because there is no human manipulation of secrets and secrets are stored in hardware, therefore not accessible to an attacker.
All IP Touch phones are secured by default
For SIP endpoints, implement "http basic authentication".
For all other IP endpoints category, not capable of authentication, give only limited rights (non too-free calls ,like international calls, are barred or accessible only through additional password).

4. Threats to IP phones during initialization phase

IP phones are plug and play devices for obvious reasons like simplication of management. There are vulnerable to a number of attacks until there are up and running on the network, because they need to access a certain number of servers to download and get what is needed for them to work. There are also weak on a security stand point.

The following does not address direct attacks to the IP Phones element themselves but attacks to their environment that can be done when the phone reboots and is therefore more vulnerable.

An attacker has not to wait for an IP phone to reboot to launch an attack. It could make a phone reboot through brut force attack and then exploit vulnerabilities described below.

4.1. DHCP spoofing (DHCP server insertion attack)

Threat: When IP phone reboots it is first sending a DHCP request to retrieve its IP parameters (when not statically configured). DHCP request are broadcasted so they can be intercepted by anyone on the LAN. IP phone is therefore vulnerable to a DHCP offer that is sent by a rogue DHCP server. This rogue DHCP server can then send to IP phone an IP router address that will allow to reroute IP phone traffic through the attacker device.

Solution :
When transiting through the router, DHCP request are transformed by router into unicast traffic to the legitimate DHCP server. So a rogue DHCP server could only be inserted on the same IP subnetwork than the victim.
The solution is at the infrastructure level, by using a feature called DHCP snooping. DHCP snooping only allows to insert DHCP server on identified ports. DHCP answers are blocked on all other ports.

Note: if no DHCP answer is received on IP Touch phone, IP touch will start up with previously IP allocated address (in case DHCP server faces a flooding attack).
As OmniPCX Enterprise does not use DNS, it is no subject to DNS based attacks like DNS poisoning.

A secured IP Touch phone will take into account parameters sent by a rogue DHCP server.

- If it is not able to contact its Com Server it will reboot (for instance if router IP address is a fake address).
- If it is capable to contact its Com server, it will be secured (through authentication, integrity, encryption), the IKE protocol used to negociate keys being protected against MiM attacks.

4.2. TFTP server spoofing (tftp server insertion attack)

Threat:
After the DHCP process, an IP Touch phone will try to download its configuration file using the tftp server address sent by the DHCP server.
The tftp server could be a spoofing tftp server. The risk is that the tftp files that need to be downloaded are not the right one.

Solution: Although there are basic mechanism to check the consistency of downloaded files by IP Touch phones, with IP Touch Security solution, IP Touch phones control the integrity and signature of the files that are downloaded. These files are signed either by Alcatel (binaries) or by the SSM component (config file) .
If the files are spoofed ones or not existing, IP touch phones will continue the boot process with their previous configuration.

5. Features and Benefits of IPTouch security solution on OmniPCX Enterprise.

The following chapter describes the features of IP Touch security and the benefits of using this solution.

5.1. Hardware based encryption for High Quality VoIP

Encryption requires heavy processing constraints on IP Systems. Heavy processing translate generally in increased delays. It is important than for real time VoIP communications, encryption does not impact delays.
In order to provide both High Quality VoIP with encryption, Alcatel and Thales have chosen a hardware encryption solution for Com server and IPMGs, capable of handling thousands of simultaneous signalling sessions and tenths of VoIP RTP flows (more than 100 per Security Module) with less than 1ms transit delay , which is not sensible in the VoIP context.

Hardware encryption is 20 to 100 times faster than the software equivalent, depending on size of packets.
For IP Touch phones, encryption is done in firmware but this has no impact on delay, as IP touch range has been natively designed with spare capacity to support heavy constraints due to encryption.

Benefit is also that deploying IP Touch security solution on an existing OmniPCX Enterprise system, does not require reengineering of the IP telephony solution which would translate in replacing servers or add additional blades in IPMGs cabinets. All the IP touch range is also "encryption ready" and any new or already installed IP touch device can benefit from IP Touch security.

5.2. Dedicated Hardware based security for future proof encryption (to avoid cracking)

1) As handling IP communications call control and security on the same platform has some advantages, it also holds some risks to the security of the solution. On software platforms, secrets are stored on hard drives and are susceptible to be intercepted by on way or another.

Thales and Alcatel have chosen to separate call control and security of communications to ensure that the solution will not be cracked one day or another, by compromising the private keys.
For instance, private keys used for signing start-up files are buried into the hardware of the Security module and therefore not accessible.

2) Another feature that will ensure that the security is future proof is the dual Thales-Alcatel approach.

Alcatel and Thales have based the solution on a set of asymmetric keys pairs partly owned by Thales, partly owned by Alcatel. The private keys never leave Alcatel or Thales premises.

Thales is a third party (tiers de confiance) for Alcatel: security modules are personalized by Thales in the path from factory to customer, ensuring that there are no leakage of private keys either at the factory or in the customer premises.

All the keys used by the IP Touch encryption solution will be computed/negotiated based on these key pairs (included Calculated PSK used for authentication), without needing intervention of a third party, which can lead to compromising of secrets if not well performed.

3) Quality of encryption is of course dependent on the type of encryption used (AES) and the length of the key (128 bits). But the vulnerability often lays in the quality of the random and the "seed" used to calculate the encryption key.

Thales has implemented a superior randomgenerator in every equipment of the IP Touch security solution (Security modules, IP touch, Com server), in order to provide a solution that will be future proof.

5.3. Protection against encryption deactivation for better control of security by customer

NOTE: Encryption can be activated on IP phones on a **system only if a SSM is present**
If SSM is not present, IP phones will run in a mode without authentication, nor encryption (call control signalling and media), except if they have run on a secured system before and not being reinitialized from a security standpoint.
Furthermore, even if SSM is present, the Com Server software is protected by an "IP Touch security" software lock, which presence is mandatory to activate "IP Touch security".

Encryption and integrity of call flows is useless if security can be deactivated too simply.

There are 2 ways that hackers could use to deactivate security on an generic IP phone

- Getting access to the system management and deactivating security by a click on a mouse.
- By making an IP phone reboot (through DoS attack) and let it start in a non secured mode

Hardware security based IP touch security also avoids that security of communications is deactivated either by mistake or intentionally to put IP communications at risk.
The only reason to deactivate IP communications security is because of disaster recovery. This is described later on in the serviceability chapter.

Here are the following actions taken to avoid that security can be deactivated
- The fact that the system is secured or not is indicated in a config file called LAN PBX.cfg and not in the configuration database of the OmniPCX. This file is signed and stored on a tftp server . IP phones get their IP addresses and tftp server address from the DHCP server. They contact the tftp server and are secured before they even reach the OXE server.
- The tftp server can be different from the OmniPCX Enterprise server. Therefore the fact that the system is secured or not is physically independent of an action done on the OmniPCX Enterprise. This gives customer a way of controlling the security of its communications independently of the Business Partner managing the OmniPCX Enterprise.
- Removing the SSM (that is bypassing it), is not sufficient to deactivate security. A new LANPBX file must be posted on the tftp server indicating securely to IP phones than security is deactivated (otherwise the system will not work).
- Removing a MSM in front of an IPMG is not sufficient to deactivate security on that IPMG. A change must be done in the configuration database of the OmniPCX to indicate that this specific IPMG is no more secured (otherwise the system will not work).

- IP touch phones are also secured by default on a secured system. This avoids that security could be deacticated on a specific IP touch without user seeing it by accessing the configuration database of OmniPCX Enterprise.
- If IP touch is secured and reboots, it will reinitializes in a secure manner: it will validate the signature and integrity of the config file before taking itinto account. If not, it will initialize with its last (secure) configuration informations. This ensures that the IP touch phone is not vulnerable after a reboot: once the IP Touch phone is secured, if it reboots it can not be unsecured by a pirat PC on the network thanks to a secure initialization.

5.4. Additional layer of protection of CS and Media Gateways by Security Modules for better availability

Security Modules are in charge of authentication, integrity and encryption of IP communications flows.

Security Modules are inserted between IP communications end points and the LAN network where threats are coming from. Therefore they can also provide additional protection in availability of Com Server and IPMGs.

Whether encryption or not is done on a flow crossing the module is either native (e.g. the call control signalling) or based on IP addresses and ports (source or destination)(eg. protected or unprotected IPMGs)
Other type of traffic (management) crossing the Security Module is normally not processed and sent in clear through the module.

Nevertheless, at the cost of additional management in OmniPCX Enterprise, security modules can also block traffic to/from specific IP addresses and ports (impact on performances and configuration to be assessed on a case by case basis).

E.g. OmniPCX Enterprise is connected to a CTI server. This traffic is in clear. SSM will block any CTI traffic coming from an IP address different from the legitimate server.
It has the advantage over Trusted Host /TCP wrapper to also process UDP traffic and can also be implemented at the MSM.
At the SSM and MSM side, it also tighten voice/data partitioning to avoid that someone having access to either IPMG or Com Server (e.g. remote maintenance), could rebound to access fraudulously other servers in the LAN of the customer.

Better availability through Operating Sytem bio-diversity:
The Security Modules offer good performance on a availability standpoint (protection against DoS)
The IP Touch security solution is based on a robust and field proven security device: Mistral product has got the Common Criteria EAL 3 certification.
Security Modules are using a hardened micro-OS, of course different from the Linux of the OmniPCX Enterprise. Therefore SMs could block attacks based on potential

vulnerabilities identified in OmniPCX's Linux (with corrections that possibly have not been implemented yet on the customer server).

5.5. *Best balance between security and serviceability, with no impact on Total Cost of Ownership*

Management of keys and customisation of keys is generally a time consuming process for customer team in charge of security, and could therefore have a negative impact on Total Cost of Ownership of the IP telephony solution.

For instance, managing certificates in IP phones to integrate a PKI based authentication scheme, will require a secure and heavy process to create a certificate in an IP phone.

This is not the case with IP Touch security. Authentication is based on a calculated PSK that do not require any customization of IP Touch phones when they are installed on a secured IP telephony system. IP Touch phones are "plug and play", whether they are running on a standard or secured system.

6. Glossary:

>CS	Enterprise Communications Server
>IPMG	IP Media Gateway
>SSM	Server Security Module
>MSM	Media Security Module
>PSK	Pre Shared Key
>IPSec	IP Security
>IKE	Internet Key Exchange
>SRTP	Secure Real Time Protocol
>AES	Advanced Encryption Standard
>ESP	Encapsulating Security Payload
>HMAC	Hashing for Message Authentication Codes
>SHA-1	Secure Hash Algorythm

7. Ressources

8AL020033160TCASA –security- DOS attacks
Available on Alcatel BPWS : http://www.businesspartner.alcatel.com/

actes.sstic.org/SSTIC05/ILTY__Im_Listening_to_you_via_VOIP/SSTIC05-Bareil-VOIP_Projet_ILTY.pdf(cut and paste the link)

NIST special publication 800-58 January 2005
"Security considerations for VoIP Systems"
csrc.nist.gov/publications/ nistpubs/800-58/SP800-58-final.pdf
(cut and paste the link)

Miercom: 2004 a VoIP Security assessment (May 2004)
http://www.miercom.com/

Hervé Schauer Consultants : http://www.hsc.fr/
20 juin 05: Présentation "Sécurité de la Voix sur IP "
http://www.hsc.fr/ressources/presentations/csm05-voip/index.html.fr