Global Information Assurance Certification Paper

Telephony in a Packet Switched Environment

Practical Assignment: GIAC Security Essentials Certification (GSEC)

GSEC Practical Assignment (1.4c)

Option 1

Author: Denis J. O'Toole

January 2005

Submission Date: 10th January 2005

Synopsis

This document is an attempt to discuss and identify various security matters related to modern telephony over a packet switched network, more commonly known as Voice over IP (VoIP). Topics covered include IP Telephony architectures, the security concepts of VoIP Availability, Integrity and Confidentiality and a exploratory section on the future direction of VoIP.

Table of Contents

Introduction

Availability, Integrity and Confidentiality [1] is the war cry of the seasoned information security professional. Mitigating risk within an establishment is usually an attempt to protect profits and the investments within, we are a staunch ally. The trend toward packetised telephony over IP (Internet Protocol) is efficient and makes financial sense. Reducing the need for specialists to maintain separate infrastructures and fully utilising current infrastructure seems to be a godsend.

Packetised voice network solutions are full of paradoxes, most are of a technical nature, and some social aspects may be thrown in for good measure. The end user may be bullied into authenticating for network services such as email or internet access, but how does one insist on similar polices for a telephone? Generally speaking, users will not stand for it.

IP Telephony Architectures

As a security officer, one should be made aware that every organisation in the business world will not have the same VoIP deployment. This may be for a number of reasons, usually due to financial constraints, but that is not always the case. As VoIP becomes more prevalent, it is not just the medium to large organisations that are utilising the technology, SOHO (Small Office, Home Office) customers are warming to these tools as well.

POTS (Plain Old Telephone Service)

Currently, or in the very recent past, office and inter-office telephony was achieved by the use of a PBX (Private Branch eXchange) or an ACD (Automatic Call Distribution) system. Both of these systems basically consisted of a central call processor and a switching array. These systems operated on a principle known as TDM (Time Division Multiplexing) allowing each phone circuit to be switched. Typically these circuits consisted of 64Kbit/s ISDN (Integrated Service Digital Network) channels, possibly in groups of 24, making up a T1 connection.

For data communications, a separate infrastructure using packet switching technology provided connectivity and resources for computing and workflow needs.

In conjunction with the processor and switching matrix, user telephones were most likely directly connected via an MDF (Main Distribution Frame). Other devices may also be connection to the PBX such as; voice mail servers (VMS) and interactive voice response (IVR) systems.

Some organisations would use other business and administration tools which interact with the PBX, such as CTI (Computer Telephony Integration), NMS (Network Management System), CRM (Customer Relationship Management)

applications or administration terminals.

POTS Security Analysis

- Availability; POTS may be considered quite secure from external parties. The PSTN (Public Switched Telephone Network) is built on proven, reliable technology.
- Integrity; All incoming voice traffic came from a known, single source (your telephone company) and each telephone was physically, directly connected to the MDF. Elements of repudiation exist by the implementation of Caller ID (CID) and Malicious Call Tracing (MCT).
- Confidentiality; By ensuring MDF and telephone companies secure the physical access to wiring hubs, eavesdropping can be prevented by unauthorised personnel.

Mitigating infrastructure risk with POTS;

It is possible that the VMS and IVR applications are communicating over the data network. Most definitely CTI, CRM, NMS and administrative terminals are using the data network infrastructure. These applications are quite common in larger organisations and more than likely, are being administered by technicians with limited knowledge of information security.

General threat mitigation techniques for server hardening in conjunction with network separation, utilising VLAN's and packet filtering, and access control methods can be used to greatly reduce risk in most instances. It is implicit that standard security practises for server hardening are applied. These include the removal of unwanted services, and HIDS (Host intrusion detection system). It is beyond the scope of this paper to suggest specific mitigation techniques for each of the application instances listed herein.

Packet Switched Telephony

Voice server operation can be generally described as "The conversion of …voice conversations into packets, streaming them between endpoints utilising Internet Protocol" [3]. Architecturally however there are differences as to how this is achieved.

IP Enabled

An IP enabled solution will contain the same external connectivity with a telephone company PSTN via a switched circuit mechanism. A simplified description of IP enabled architecture is the addition of IP technology to a traditional PBX via additional hardware or add-on card. Internally, users may now connect via the traditional physical, directly connected method, or via the data network infrastructure.

A network supported IP enabled technology is usually leveraged with existing TDM based equipment by adding the necessary accessories, such as IP

adapters. Typically phone IP adapters will share data connectivity with the workstation computer via a network hub or switch, provided by the adapter. Dependant on the vendor specifications, such adapters may cause Quality of Service (QoS) issues as the IP migration rollout continues.
IP enabled technology may also be used for Inter-office telephony, allowing the data infrastructure between offices carry both voice and data traffic, eliminating the need for dedicated switched circuit lines.

Overall, IP enabled PBX or ACD is a lower cost upgrade solution, allowing a lower risk transition between TDM and IP telephony. Migrating to IP enabled architecture is generally a proprietary solution, possibly limiting future investment into a single vendor.

IP Centric

Functionally IP Centric and IP enabled infrastructure are similar with the exception of internal TDM technologies. The IP centric voice server acts as a media gateway, possibly converting TDM signalling to packetised voice streams. Another alternative to TDM is VoN (Voice over the Net) (to be discussed in a later section).

The media gateway consists of a number of different services, primarily consisting of a call control service. Other services may be hosted, such as a call queuing, music on hold (MOH) and call accounting. These services may be distributed amongst several physical servers.

IP Centric architecture is consistent for call routing (IP only), leveraging the data infrastructure and may provide greater freedom in a mixed vendor equipment environment.

VoIP Availability

The International Information Systems Security Certification Consortium (ISC^2)[1] describe availability as having two facets;

1. Denial of Service (DoS)
2. Loss of data processing capabilities, as a result of natural disasters or human actions.

In general terms, DoS may be the result of unauthorised intruders or equipment misconfiguration. In the use of VoIP however, in conjunction with the above definitions, a DoS may be the result of an under engineered solution, substandard infrastructure or inadequate planning, the result of any combination being an unusable service. The second facet of ISC^2's definition should be part of any organisations BRP (Business Resumption Plan) and is out of the scope of this paper.

Quality of Service (QoS)

The most covered topic in VoIP technology is QoS. QoS for networking is described as "a goal…to provide guarantees on the ability of a network to deliver predictable results." [6].

Other relevant areas of VoIP QoS are throughput and latency. On physically shared media, such as an Ethernet cable VoIP is viewed as normal data without the use of packet prioritisation or VLAN techniques, and so may suffer from network congestion and dropped packets, the phone user hearing broken, stuttered or incoherent speech.

Using a VLAN allows the virtual separation of voice and data traffic by the use of special Ethernet frame tags (IEEE 802.1Q), which also has confidentiality benefits. Complementing traffic differentiation via VLAN, frame prioritisation (IEEE 802.1p) is implemented to give preference to voice traffic over normal data, somewhat alleviating voice quality problems.

Codecs

Abbreviated from enCOder / DECoder, the VoIP codec is an important aspect of the overall VoIP performance. The wrong codec choice can not only yield bad network performance, but also have user perceptive quality issues. The most popular codecs used in VoIP are; G.711 & G.729a, both having different bandwidth requirements, packet loss tolerance and packetisation intervals.

The codec configuration options include the packetisation interval in milliseconds. Cisco's default packetisation rate [8] for G.711 is quoted as 50 packets per second or 1 packet every 20ms, generating a bandwidth of 80kbps. Comparing those figures with G.729a with the same packetisation interval generates 24kbps.

Careful consideration of voice network traffic should determine which codec one tends to use, ultimately for optimised performance there is a trade off between packet loss tolerance and packetisation interval.

Power Sources

In most VoIP architectures, a reliable power supply is an availability issue. IP telephones not utilising PoE (Power over Ethernet) will require an external power source, making a power outage an effective DoS. Often power is an overlooked as an availability issue, as a legacy POTS telephone required no external power.

Insuring power interruptions do not affect telephony services may be an expensive undertaking, providing a UPS (Un-Interruptible power supply) per telephone handset probably impractical. Conversely, the protection of core network infrastructure is standard practice. A solution to this conundrum is PoE (IEEE 802.3af), allowing IP phones to be powered via the 'spare' twisted pair in a 4-pair Ethernet cable [7]. To be effective, phones must have a direct physical connection to the PoE capable switch. The PoE switches must, in turn be

supported by an appropriate and adequate backup power supply.

Software

Something to keep in mind with VoIP technology is that the call processing server, accounting server, IP telephones, soft phones (Computer Programs acting as an IP Telephone), IP adapters and other services comprising the VoIP infrastructure all have software components including the TCP/IP and other, higher layer stacks (Refer to OSI layer for reference).

Software patching and upgrade management techniques should be employed where possible. A prudent analyst may examine the possible upgrade methods for each infrastructure element. In some cases, as with some vendor IP enabled solutions, software upgrades can only be done by having physical access to telephone, literally requiring disassembly and re-programming, a task requiring some specialised technical knowledge.

The accessibility of specialised technicians, generally supplied through a vendor should be investigated, as a timely incident response to exploited software vulnerabilities may greatly influence availability.

Risk assessment tools are very few tools, making it difficult to assess and diagnose current vulnerabilities with VoIP, perhaps as market share increases, the demand for such tools will deliver.

Voice Over the Net (VoN)

VoN is an alternative to using a PSTN as an 'upstream' telephony provider. Such Internet Telephony providers have a subscription service like traditional PSTN provides, though VoIP calls are routed over the internet to 'hop-off' points, where a destination call processing service may convert the call to the local PSTN network if required.

There have been points of view debating the generally availability and reliability of a VoN system. Academic research has quoted availability factors as "…a call success probability at around 0.5% and a call abortion probability at about 1.5%, resulting in a 98% net availability" [4]. This information was for Internet calls and is quite impressive, however is not to the same standard of a PSTN, generally four 9's (99.99%).

VoIP Integrity

Integrity will for the most part be mitigated by access control systems, a method used to determine authorisation. Access control systems disallow unauthorised users and equipment gaining access to resources. Using some of the techniques used to increase availability, we can extend their uses to include integrity.

Access Controls

Access control should be implemented in such a way that threats such as the installation unauthorised equipment (rogue devices), networks and services are substantially mitigated. Using the principal of least privilege is the most successful way of achieving this.

Authorisation can only take place once authentication requirements have been satisfied. Authenticity may be attempted in several ways; by something known (passwords), something in possession (e.g. a token), something they are (biometrics) or a combination of any of the aforementioned. In practice biometrics would make IP telephony cost prohibitive but company policies and requirements will commonly dictate how elaborate the authentication mechanism is.

User Authentication

Password authentication is the most rudimentary access control used in information technology, so it makes sense that users should be forced to authenticate themselves before being permitted to access the voice network, as they normally would to access the data network and associated resources.

Authentication in IP telephony is used to instruct the call processing service which IP address maps to which telephone extension. Company policies will most likely require the personnel non-repudiation element, requiring a user to be related to a telephone extension.

Equipment Authentication

Equipment authentication is a little more straightforward. IP telephones utilise Ethernet protocol for the Data Link layer, and as such have a unique identifier know as a MAC (Media Access Control) address.

On modern Ethernet switches, switch ports can be locked to specific MAC addresses, effectively allowing a single piece of equipment access to the network at OSI layer 2.

OSI Layer 3 access can also be restricted by implementing a DHCP service (RFC 1531) exclusively for use in the voice network, limited access control can be achieved by either statically mapping a MAC to an IP address, or by allowing IP addresses to be requested if a MAC is known by the server.

An ideal solution for equipment authentication would be to provide more than one identification mechanism, such as a hardware predetermined SecurID string, further preventing some miscreant from penetrating the voice network using known IP and MAC spoofing techniques.

Network Segregation

Further access control enforcement can take place by the use of a careful

network design. Ensuring each voice network segment has its own IP address range, packet filters can be deployed at segmented borders in an attempt to prevent unauthorised traffic from traversing past the filter and into the voice network core.

VoIP Confidentiality

Confidentiality relates to the non-disclosure of information or resources to an entity that does not have prior authorisation or authenticity. Protection of information has historically been obtained through the use of an encryption, though is some cases this may be impractical or in some cases illegal.

As network technology evolved both network security and network vulnerabilities have as well. Looking back into the recent past, the introduction of a switched network brought about a false sense of security, as traffic broadcast domains were reduced to a switch port and conventional network analysers no longer saw every network packet pass their promiscuous mode interface adapter. With the introduction of utilities such as Ettercap [9] and DSNIFF switched networks were no longer safe. In conjunction with these tools, early Cisco VoIP phones were susceptible to phone call intercepts using a tool known as VOMIT (Voice Over Misconfigured Internet Telephone). Without encryption and with a known voice codec (G.711) a motivated individual could easily capture and replay any voice conversation. There is most definitely a need for secure transmission.

Encryption

As VoIP and indeed networking has evolved, the need for encryption has been addressed. There are encryption standards for the three of the five top OSI layers, namely, the Session (SIP & SSL) Transport (SRTP/TLS) and Network (IPSec) layers. Depending on the level of security required encryption can be implemented at each level, please keep in mind the amount of protocol overhead added at each layer.

In VoIP communication however we have a somewhat of a dilemma. There is a need for encryption to ensure the confidentiality of data, but there is also a need for low latency in voice streams as traffic needs to be encrypted and decrypted on-the-wire.

In early implementations of secure IP telephony voice encryption was achieved with a Network layer encryption using IPSec with a choice of DES, 3DES and AES encryption types, but as time has progressed the IETF set a new encryption standard with SRTP (Secure Real-time Transport Protocol), RFC3711. SRTP at the moment only supports AES and does not specify a key exchange protocol. Due to this deficit on SRTP, the current industry standard is to use an exchange method known as ‘MIKEY’, currently in draft status with the IETF [11].

End to End point encryption is the ideal solution to secure VoIP however as

stated earlier may be detrimental to performance.

Legal ramifications

In most countries around the world there is a requirement for the surveillance of known and suspected criminals. The implications of encrypted voice transmission at the minute are unclear as the legal system struggles to understand the national implications of this new technology.

Future Developments

Mobile IP

Mobile IP is recent IETF standard (RFC 3344) giving IP connectivity to cellular devices such as 3GPP, taking wireless networking to a new level. With the advent of terminologies like fixed home addresses and care off addresses, mobile IP complicates security matters further, very much exacerbating the need for security development in not only VoIP but internetworking in general.

Other Enhancements

It is inevitable that future use of VoIP technology will demand more than is currently available. Proposed enhancements being researched are adding features such as file transfers and video conferencing. As our appetite for new technologies grows we as security professionals need to find new ways of mitigating risk.

Conclusion

Voice over IP is a strongly supported industry as millions of dollars are spent of R&D into new technologies we can believe VoIP has an infinite longevity. As technology changes our risk mitigation strategies must change with them. Sensible and well constructed risk mitigation techniques can reduce the burden of VoIP to nothing more than another network data service.

.

Bibliography

1. Hansche, Berti, Hare. "Official (ISC)^2 Guide To The CISSP Exam" (2004)
2. Unknown. "VoIP Security" 2003 International Network Services
   URL:http://www.ins.com/downloads/datasheets/sec_solution_voip_security_ds.pdf
3. Gharakhanian, A. "Which VoIP Architecture Makes Sense for Your Contact Center?" August 2002 Vanguard Communications Corporation
   URL:http://www.computertelephony.org/uploads/wpapers/227_49.pdf
4. Jiang, W. & Schuzrinne "Assessment of VoIP Service Availability in the Current Internet" December 2002 Columbia University, Department of Computer Science
   URL:http://moat.nlanr.net/PAM2003/PAM2003papers/3897.pdf
5. Provos, N. "vomit – voice of misconfigured internet telephones" (2004)
   URL: http://vomit.xtdnet.nl/
6. Mitchell, B. "Wireless/Networking QoS" 2005 About Inc.
   URL: http://compnetworking.about.com/od/networkdesign/l/bldef_qos.htm
7. Unknown. "What is Power-Over-Ethernet (PoE)?" 2004 Hyperlink Technologies
   URL: http://www.hyperlinktech.com/web/what_is_poe.php
8. Szigeti, T. & Hattingh, C. "Quality of Service Design Overview" Dec 17 2004 Cisco Press. URL: http://www.informit.com/articles/article.asp?p=357102
9. Ornaghi, A & Valleri, M. "Ettercap" 25 January 2001
   URL: http://ettercap.sourceforge.net/
10. McClure, S. & Scambray, J. "Switched Networks lose their security advantage due to packet-capturing tool"
    URL:http://www.infoworld.com/articles/op/xml/00/05/29/000529opswatch.html
11. Arkko, et. al. "MIKEY: Multimedia Internet KEYing" 28 October 2004
    URL: http://www.ietf.org/internet-drafts/draft-ietf-msec-mikey-dhhmac-07.txt
12. Millard, E. "E-Business Legal Dilemmas Loom in 2004" January 23, 2004
    URL: http://www.vonage-forum.com/article626.html