Converge! NETWORK DIGEST

Security in VoIP Networks – Stronger than TDM!

by Haim Melamed, Director, Channel Marketing

AudioCodes

3/29/2006

The move from TDM networks to VoIP has created a new challenge for network operators end enterprises – security. Unlike in TDM networks, where the telephony network was almost completely isolated from the data network and the internet – most VoIP networks have many interface points with the data network, along with the dangers in the internet world. A poorly designed VoIP network can easily be exposed to security threats such as denial of service attacks, computer viruses and data theft. On the other hand, the technologies available today, in addition to a well designed network, can offer even better security than we had in the TDM world.

Security is not a new concept for telephony managers. Telephony networks were always exposed to security threats like eavesdropping, impersonation, fraud and denial of service – similar to that of data networks. Moving away from a separated, dedicated TDM network to the well known, widely used IP network has exposed the telephony networks to a growing number of hackers, originating from the data world. While hacking in the TDM telephony world was limited to a small group who required physical access and dedicated equipment, the VoIP world is more accessible to a large community of internet hackers who are using readily available software tools.

VoIP networks are based on the well known IP protocol, using the popular Windows, Linux or Unix based call manager and application servers, and are directly connected to the internet.

Taking these factors into account, it seems that VoIP networks are inherently more vulnerable than TDM voice networks. That assumption is true for a badly designed, insecure VoIP network - however if designed and secured correctly, a VoIP network is more secure than a typical TDM telephony network.

While investigating the differences between VoIP networks and TDM telephony networks, there are a number of security threats that need to be addressed:

Eavesdropping – the ability to listen to another party's telephone conversation without authorization

Impersonation – the ability to imitate someone while having a telephone call with another party

Fraud (Call Theft) – the ability to make a call on the network without paying

Local denial of service – the ability to block phone calls from or to a specific location in the network

Network denial of service – the ability to collapse the network or large portions of a telephony network

Eavesdropping

It is simple to eavesdrop on a traditional TDM telephony network. The fact that TDM telephony networks are isolated networks operated by service providers, built and designed to carry telephony conversations only, has created no need for any protection from eavesdropping. The only protection a TDM telephony network has against eavesdropping is the physical protection. Anyone can potentially hook into a telephone conversation. The easiest place to eavesdrop is at the point of the "last mile". Tapping into the two wire analog line connected to the phone, and listening to the phone call without anybody acknowledging it, is all that is required. The phone calls on the traditional TDM telephony networks are not encrypted or protected.

Unprotected VoIP networks are easy to eavesdrop, but more difficult than in TDM telephony. Listening to a VoIP call requires tapping into the IP network, at the last mile or at another point on the network, and copying out the specific IP session between the two endpoints.

Protecting a VoIP network from eavesdropping is simple. Using standard IP protocols like IPSec and SRTP, allows effortless implementation of end-to-end encryption of any phone call in the VoIP cloud. Encryption protocols (such as 3DES and AES), developed for the data world, are easy to implement as they are becoming a de-facto standard in any IP-phone and desktop today.

A well managed VoIP network over IPSec VPN, or the SRTP protocol, is virtually protected against eavesdropping. Tapping into such a network will result in useless information. Achieving the same level of security in TDM telephony is actually almost impossible, and is much more expensive to implement.

Impersonation

TDM telephony networks have no built-in authentication and identification. The end terminal – the phone gets its identity and phone number from the access port it is connected to (PBX or Class 5 Switch). In addition, any PBX port can host more than one physical phone - all sharing the same number. These attributes make impersonation in the TDM telephony network as easy as eavesdropping. All you need to do is tap into the line, connect to the two wires in the last mile, or into a trunk, and nobody will ever be able to prove who the actual initiator of the call was.

Unprotected VoIP networks are more susceptible to impersonation. Since IP networks are geographically independent, the interested party can impersonate from anywhere on the network and act like he is someone else.
Protecting a VoIP network from impersonation is relatively easy. IP systems have many built in identification methods and options. Physical MAC addresses of the IP phone, IP addresses, usernames and passwords, VPN tunnels and many other methods can make sure that only the authorized party can make a call on the VoIP network.

A well managed VoIP network implementing all or some of those features wisely, is practically protected against impersonation. Achieving the same level of security in TDM telephony is actually almost impossible, and is much more expensive to implement.

Fraud (Call Theft)

Fraud is a way of making a phone call without paying for it. That makes this security threat very common and it is actually the most common threat in the TDM telephony world.

An illegitimate user of the telephony system attempting to commit fraud is identical to the issue of impersonation. TDM networks and unsecured VoIP networks are exposed to this threat, while a well designed and managed VoIP network can be virtually secure from this threat.

Another version of fraud can be a legitimate user trying to manipulate the system and create long distance or other expensive calls without paying for them. This threat is the same for both TDM telephony and VoIP systems, and can be handled similarly. In most networks, this is handled by the billing system, which detects fraud attempts and blocks the user account.

Local Denial of Service

TDM telephony networks are built in a wired point-to-point configuration such that service to a specific user is always provided by a specific switch. Damage or attacks inflicted on the access infrastructure (copper wiring) is fatal to the service. VoIP networks can be built in a flexible multipoint-to-multipoint distributed manner. The VoIP Softswitch is a virtual network entity that can be backed up easily in another location. In addition, network connectivity can also be backed up via another route. A well designed VoIP network can ensure no single point of failure, and protect itself against failures and local denial of service attacks.

Network Denial of Service

Network denial of service attacks is the only threat that almost all TDM telephony networks are naturally protected against. Most TDM telephony networks are robust, isolated networks, using proprietary protocols purposely designed to allow close to 100% availability. The call servers in the network (Telephony Switches) run proprietary operating systems that are not accessible from anywhere outside the network.

Unprotected VoIP networks are vulnerable to denial of service attacks. Softswitches and IP PBXs are IT systems running on operation systems like Windows and Unix, and are connected to IP networks (some also to the public internet). As such, they

are vulnerable to computer viruses, and IP-based denial of service attacks.

A VoIP network should be well designed and managed to protect itself against network denial of service attacks.

Currently, most VoIP networks are separated from the IT data networks. Using technologies such as VLANs and MPLS, these networks are not accessible from the data network. The call servers must be protected from viruses and worms like every other mission-critical server. In addition, redundancy must be applied to allow service continuity in case of a failure.

A main advantage of the VoIP network is the easy integration between telephony and computer applications. PC-telephony applications, unified messaging and various applications make the connection between VoIP and the data network imminent. Therefore, VoIP networks must be carefully connected to the data network and potentially the internet, using specialized appliances such as SBCs and firewalls, to prevent unauthorized use of this connection for denial of service attacks.

Standard IP-based protocols like SNMP, Telnet and HTTP are used to control and manage VoIP networks. These can also be abused for denial of service attacks. Therefore, service provider and enterprises must use the secured versions of these protocols to protect themselves against attacks.

Summary

Contrary to thoughts in the marketplace, TDM telephony networks are likened to unprotected, badly designed VoIP networks. Both are vulnerable to security threats.
However, unlike the TDM telephony networks that are inflexible and expensive to protect, a VoIP network can easily and inexpensively be protected against most security attacks, eventually achieving a network that is more secure than the TDM network.

About the Author

Haim Melamed is Director of Channel Marketing at AudioCodes.

Haim Melamed has 15 years' experience in the networking industry and is currently the Channel Marketing Director at AudioCodes. He is specifically responsible for the worldwide marketing of AudioCodes' solutions via channel partners. Before joining AudioCodes, Haim worked at Cisco Systems for seven years, where he led the technical and marketing activities in the Israeli, Cypriot and Maltese markets. Before joining Cisco, Haim worked for 3 years in the communications division of Team Computers and Systems, one of the leading Israeli IT systems integrators, as the pre-sales support manager. Haim Started his career at the computer center of the Israeli Defense Force, where he served for 4 years as a network architect and a project manager.

About AudioCodes

AudioCodes

AudioCodes Ltd. (NASDAQ: AUDC) enables the new voice infrastructure by providing innovative, reliable and cost-effective Voice over Packet technology and Voice Network products to OEMs, network equipment providers and system integrators. AudioCodes provides its customers and partners with a diverse range of flexible, comprehensive media gateway and media processing technologies, based on VoIPerfect™ – AudioCodes' underlying, best-of-breed, core media gateway architecture. The company is a market leader in voice compression technology and is a key originator of the ITU G.723.1 standard for the emerging Voice over IP market.