Global Information Assurance Certification Paper

Securing Cisco AVVID VOIP

Mark Travers

November 13, 2000

Introduction

This paper will discuss security issues related to the implementation of a basic Cisco AVVID (Architecture for Voice, Video and Integrated Data) VOIP (Voice-over-IP) solution. This will include a brief overview of a basic Cisco AVVID VOIP solution, how to secure the Cisco Call Manager 3.0, Cisco IP Phones (i.e. Cisco IP Phone 7960) and how to secure the VOIP on the Local Area Network and over Wide Area Network links.

Cisco AVVID VOIP Overview

The basic Cisco AVVID Voice-over-IP solution has a Cisco Call Manager 3.0, which performs the roll of a traditional PBX, Cisco IP Phones and Cisco Gateways, which translate between the VOIP on the Local Area Network and the phone company (PSTN) connections. The Cisco Call Manager 3.0 is software that runs on Microsoft Windows 2000 Server on a Cisco provided Compaq server. It comes as an all in one software installation, that loads Microsoft Windows 2000 Server, Microsoft SQL 7 and the Call Manager 3.0 software. The Cisco IP phones attach to the Local Area Network and can be set to use DHCP or static IP addresses. The Cisco IP phones can use external power supplies or can get power over the data network, if you are running Cisco 6500 switches with power enabled port cards. Cisco is also developing the Cisco IP SoftPhone, which is a software phone that runs on a PC, but it has not been released yet. The voice streaming can be implemented with the G.711 protocol (utilizes 76K to 83K of bandwidth) or G.729a protocol (utilizes 17K to 26K of bandwidth). In addition, if you are running Cisco switches and routers, QOS (Quality of Service) can be enabled so that voice traffic gets priority over data traffic. The integration to the phone company provided voice lines is implemented in two ways depending on whether you have analog phone lines (POTS) or a voice T1. With analog phone lines (POTS), you would utilize analog gateways such as the Cisco VG200 or Cisco 2600/3600 IOS routers. With a voice T1, you would utilize a digital gateway such as the Cisco DT24+. Cisco also offers the Cisco uOne (Universal Messaging Server), the Cisco IP Interactive Voice Response (IVR), the Cisco WebAttendant and the CiscoWorks2000 Voice Manager, but they will not be included in this paper.

Securing the Cisco Call Manager

As stated above, the Cisco Call Manager 3.0 software runs on Microsoft Windows 2000 Server that is pre-configured by Cisco and is installed

automatically when you install the Cisco Call Manager 3.0 software. According to Cisco's TAC (Technical Assistance Center), they have configured it with sufficient security measures. But, it does not include Microsoft Windows 2000 Server Service Pack 1 or any of the latest security patches. Again, according to Cisco's TAC, Cisco's development group is testing Microsoft Windows 2000 Server Service Pack 1 and the security patches, but there is no timeline for issuing these updates. In addition, they strongly recommend that you do not install them yourself. This could cause the Cisco Call Manager 3.0 software not to run correctly or to fail completely. The Cisco Call Manager 3.0 also utilizes Microsoft Internet Information Server 5 and Microsoft SQL 7, but Cisco TAC also does not recommend loading any security patches for these either. Therefore, the best way of securing this server is to give it a private non-Internet addressable address and to make sure you have good perimeter security on the Local Area Network.

Securing IP Phones and VOIP on the LAN

The best way to secure the Cisco IP phones is to again put them on private non-Internet addressable addresses and to make sure you have good perimeter security for the Local Area Network through the use of Firewalls (i.e. Cisco PIX 520 Firewall) and Intrusion Detection Systems (i.e. Cisco Secure Intrusion Detection System). The ports to secure are tcp ports 1720 and udp port range 16384 to 16484. Also, block all ports to the Cisco Call Manager 3.0, since the Cisco Call Manager 3.0 does not need access to the Internet. If you are going to allow access to the Cisco Call Manager 3.0 from the Internet for Web Administration, which is not recommended, then block all ports other than port 80. At minimum, block all the ports you would normally block for a Microsoft Windows 2000 Web server and port 1433, the port used for access to the Microsoft SQL 7 database.

Securing VOIP over WAN links

When securing Voice-over-IP over Wide Area Network links, there are several factors to account for. It is recommended that you run the G.729a protocol for the voice stream over the WAN link, because of its lower bandwidth requirements. In addition, you will also want to run the QOS (Quality of Service) features on your Cisco IOS routers to make sure that the voice stream has priority over any other data on the WAN link. But, G.729a can be sniffed by any G.729a codec-capable device, so you will want to encrypt the voice stream. Cisco recommends that you do not use a tunnel (i.e. GRE Tunnel), because the QOS on the routers will not be able to recognize the voice stream and therefore would not give it priority. They recommend that you encrypt the voice stream using the Crypto commands available in the Cisco IOS routers. This way the voice stream is encrypted, but the router can still recognize it as a voice stream and the QOS (Quality of Service) will continue to give it priority. Again, you will want to secure tcp port 1720 and udp port range 16384 to 16484 via access-lists

on your Wide Area Network routers. There is another option and that is to setup a Layer 2 Wide Area Network link with an ISP that provides Layer 2 connectivity. Then your traffic is kept private and secured without the added configuration complexity of using the Crypto features in the Cisco IOS routers. Cisco does not recommend running Voice-over-IP over a VPN connection using the Cisco VPN 3000 Concentrator Series products, because the QOS (Quality of Service) features will not work.

References

Cisco Systems - Technical Assistance Center – Case Numbers A849347, A849398 and A849798 http://www.cisco.com

Cisco Systems - "Technical Considerations for Converging Data, Voice, and Video Networks" URL http://www.cisco.com/warp/public/cc/so/neso/vvda/avvid/tecon_wp.htm (July 3, 2000)

Cisco Systems - "Voice over IP - Per Call Bandwidth Consumption" URL http://www.cisco.com/warp/public/788/pkt-voice-general/bwidth_consume.html

Cisco Systems - "Cisco VG200: Cisco IP Telephony Voice Gateway" URL http://www.cisco.com/warp/public/cc/pd/ga/prodlit/vg200_ds.htm (June 30, 2000)

Cisco Systems - "Cisco Digital IP Telephony Gateway: DT-24+" URL http://www.cisco.com/warp/public/cc/pd/ga/prodlit/dt24_ds.htm (June 30, 2000)

Cisco Systems – "Quality of Service Overview" URL http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/qos_c/qcdintro.htm (August 22, 2000)

Microsoft Corporation - "Secure Internet Information Services 5 Checklist" URL http://www.microsoft.com/technet/security/iis5chk.asp (July 7, 2000)

Black, Kevin - "Securing Microsoft SQL Server" URL http://www.itsecurity.com/papers/black.htm