Security Concerns About Multimedia Technologies

Bryan Kay Carter
November 22, 2000

Introduction

With today's trend in high speed Internet connectivity many new and wonderful functions are being applied to this fast moving technology. The advent of xDSL, cable modems, and even new bi-directional satellite capabilities bring these high speeds to the homeowner at an ever-affordable cost.

As the homeowner now has this kind of access to the Internet, corporate managers are trying to find ways that they can leverage this speed and functionality. As they do, they feel that they can improve their customer serviceability levels by embracing these new technologies.

They often read press statements that are similar to the following:

"The market will also smile on players that successfully embrace the technology for everyday business. Just as the Internet is changing the way every company does business, the arrival of broadband access will change every Internet Company's strategy."[1]

Several of these new functions deal with things such as video-conferencing, internet telephone, internet chat, instant messaging, and collaboration software such as CUseeMe Network's CuseeMe software, and Microsoft's NetMeeting.

Several players have made inroads into these areas with a great deal of success. Regardless of whether they have been profitable or not, they have proven that these technologies work and that they will provide added benefit to those that embrace them. One Internet phone service named Dialpad.com, makes the following claim on their web site at http://www.dialpad.com.

"More than **11 million** people are using Dialpad to make free, long-distance calls." [2]

As corporations see these new technologies take hold, they are asking questions regarding how they can take advantage of them. As these decisions take place, it is important that we take the time to review the concerns about security related to this functionality.

The Basics

Many of these new functions have become prevalent due to the introduction in 1995 of the H.323 and T.120 protocol sets. These sets include many lower level protocols that pertain to individual functionality within the broader context of the packages. For example, Microsoft NetMeeting provides video and audio conferencing, chat, file transfer, virtual whiteboards, etc. Each of these sub-functions uses some combinations of these lower level protocols. The focus of this paper however will remain at the upper level on H.323 and T.120 themselves. The security concerns of the overall protocols are inherited to some degree by the lower levels.

The protocols

Table 1 depicts the ports and functions required by the H.323 and T.120 protocols. As you can see there are wide ranges of channels that must be connected in order for the functionality to exist.

H.323

80	Static TCP	HTTP Interface (Optional)
389	Static TCP	ILS Registration (LDAP)
522	Static TCP	User location Service
1503	Static TCP	T.120
1718	Static TCP	Gatekeeper Discover
1719	Static TCP	Gatekeeper RAS
1720	Static TCP	H.323 Call Setup
1731	Static TCP	Audio Call Control
8080	Static TCP	HTTP Server Push (Optional)
1024 - 65535	Dynamic TCP	H.245 (Call Parameters)
1024 - 65535	Dynamic UDP	RTP (Video Data Streams)
1024 - 65535	Dynamic UDP	RTP (Audio Data Streams)
1024 - 65535	Dynamic UDP	RTCP (Control Information)

T.120

1503	Static TCP	Call Setup
1024 - 65535	Dynamic TCP	Call Response

Table 1

Due to this high number of channels, they are very difficult to process using firewalls. Calls and connections can be generated from the external side of the firewall. Most current day firewalls do not inherently allow this and therefore must be “opened” to permit the connectivity. Proxies do not add a great deal of hope as the connections are developed using dynamic high-end ports. This essentially means that all of the upper ports need to remain open in order to support the protocol.

The T.120 protocol is also inherently dangerous due to the fact that it provides for such functions as file transfer, whiteboard, chat, and application sharing, rather than applications such as video conferencing, which are not as dangerous. The number of hacks that have been implemented using these protocols continues to increase.

Neither the H.323 nor the T.120 standard requires or enforces any type of authentication mechanism.

A good example of this dilemma is Microsoft's instruction for setting up NetMeeting. They recommend that all TCP and UDP ports above 1024 be allowed through the firewall. This then opens the local network to all of the possible attacks based upon these ports. See the Microsoft Technical documentation at
http://www.microsoft.com/TechNet/netmting/reskit/netmtg2/chpt4.asp

Possible solutions

Many of the packages like NetMeeting offer the option of an external Gatekeeper machine. This is a machine that is placed on the external side of the firewall and configured to support these protocols. A single point of entrance between this machine and your internal network can then be established. This allows internal users to initiate calls to external users. External users can initiate calls to the inside user by connecting to the gatekeeper machine. Although this can provide some relief, these gatekeepers have limitations that generate some additional problems for widespread corporate use. Generally speaking one gatekeeper machine cannot establish connections with another gatekeeper machine. If two companies have deployed gatekeepers to allow video conferencing they will not be able to communicate with each other using this method.

Another method is to place video conferencing and collaboration machines on the outside of the local network. These machines become highly vulnerable to attack, and should not contain any proprietary data on the machine itself. These machines can then be placed throughout the company in conference and boardrooms. This provides a lower level of risk while providing some of the functionality desired in a limited, and controllable fashion.

Other new products such as Cisco's Multimedia Network Manager are beginning to provide some resolution to these issues, as well as some of the network bandwidth, Quality of Service, and authentication concerns that are inherent in these protocols. Watch for new generation proxies that will incorporate some of the gatekeeper functionality into their core.

Summary

These protocols are here to stay, and we need to push to have them secured. We need to be cautious as we implement these technologies so we don't create greater risks to our corporate data. At higher risk are those companies that don't feel they can cost justify the expense of high-end firewall technology. The security industry needs to be involved in the RFC process that creates these new protocols. This would make security one of the first concerns in the process, not an afterthought.

A very complete reference about using H.323 with firewalls and proxies is located at: http://support.intel.com/support/videophone/trial21/h323_wpr.htm

References

1 – Lashinsky, Adam "Fortune Investor - The Wired Investor: Picking the Winners in Broadband" June 7, 1999 - Vol. 139, No. 11
URL: http://www.fortune.com/fortune/investor/wired/1999/06/07/index.html (November. 22, 2000)

2 – DialPad Home Page November 22, 2000
URL: http://www.dialpad.com (November 22, 2000)

3 - SURFkit for Network managers Showcase - H.323 and Firewalls: Problems and solutions
URL: http://www.sec.nl/persons/ivana/Showcase/SKIN/h323_firewalls.html (November 21, 2000)

4 – MS Netmeeting 2.1 Resource Kit – Updated January 12, 2000
URL: http://www.microsoft.com/TechNet/netmting/reskit/netmtg2/chpt4.asp (November 22, 2000)

5 – Zwickey, Elizabeth D., Cooper, Simon, Chapman, D. Brent "Building Internet Firewalls – 2nd Edition" Chapter 19 – Real-Time Conferencing Services
O'Reilly & Associates, publisher – ISBN: 1-56592-871-7

6 – *Kotha, Sam, Cisco Systems, Inc. "*White Paper - Deploying H.323 Applications in Cisco Networks" July 1, 2000
URL: http://www.cisco.com/warp/public/cc/pd/iosw/ioft/mmcm/tech/h323_wp.htm (November 22, 2000)