H.323 security in perspective

When considering the security of an H.323 conferencing system, it is important to place concerns over that security into perspective.

Privacy

Perhaps the most commonly considered security issue is the privacy of communication. In the case of e-mail applications, the vast majority of users send their e-mails ‘in the clear’, without any form of encryption or authentication being used. There is some use of privacy, usually in the form of Pretty Good Privacy (PGP) for e-mail, but usage is generally limited (at least in academic circles) to environments where confidential data (e.g. medical data in trials) is being transmitted.

The majority of web traffic is also not encrypted or authenticated. It is only generally when ecommerce sites are being used, or in the academic context perhaps sites where important passwords may be otherwise sent plain text, that Secure Socket Layer (SSL) type encryption is used. The web server certificate may also be viewed to check the asserted identity of the site (although most users recognise the ‘padlock’ as a sign of security without checking the certificate).

Interactive login and file transfer protocols also have secure equivalents. Instead of Telnet, Secure Shell (SSH) can be used, and instead of File Transfer Protocol (FTP) there is Secure Copy (SCP) or Secure File Transfer Protocol (SFTP). Here the main concern is leakage of accounts and passwords, that may in turn lead to wider compromises in a site. Many sites encourage the use of SSH and SFTP, and may themselves perhaps use SSH for applications such as secure remote backups.

Where H.323 conferences occur between JANET sites, the trusted nature of the JANET and Regional Network backbones make the only likely location of a snooping attack the participating sites themselves. Use of dedicated links, switched Ethernet or Virtual Local Area Networks (VLANs) can reduce the threat within a site significantly. However, if one participant is remote from JANET, the potential for snooping grows, depending on the integrity of the network between JANET and the remote participant. Snooping is discussed in Section 7.

In the context of H.323, current usage today is almost all unencrypted, similar to the usage of e-mail. In this document we present methods that may enable encryption within the H.323 protocol suite or by use of Virtual Private Network (VPN) overlays but for general usage privacy is no more a concern than it is with other electronic communication media in the academic community.

Authentication

One of the benefits of using a videoconferencing system is that it is obvious to the conference

participants with whom they are interacting. With e-mail, the apparent sender of a message can easily be forged. In an H.323 videoconference you have audio and visual contact with the other participants, and can thus (where known) recognise them directly.

Authentication of the terminal devices is a separate issue. Studio systems are inevitably shared, so the identity of the system does not necessarily correspond to the identity of a user for any given session. Any per-system authentication scheme only asserts the identity of the system being used, not the user at the system.

Unauthorised access

One of the classic security threats is unauthorised access. In the usual context this means someone is making use of a resource they do not have permission to use, in some cases stealing, altering or damaging information. Such ‘hacking’ incidents are not uncommon on the Internet.

In the case of H.323 systems there is the potential for end systems and other H.323 components to be accessed by such ‘hackers’, but careful consideration of equipment deployment, judicious use of firewalls, and care in the use of passwords ‘in the clear’ when managing such devices remotely can reduce the risk dramatically. Furthermore a ‘hacking’ incident on a dedicated H.323 end system is generally less likely to be dangerous than one on a desktop system, simply because of the restricted set of services running – the ‘hacker’ can only then affect the H.323 functionality.

A related risk is that of unwanted participants joining an H.323 session and listening in silently (muted). By using an H.323 architecture where the centrally managed MCU must call out to conference participants, such a risk is dramatically reduced.

Denial of service

There has been a growing number of denial-of-service security incidents on the Internet in recent months, well-known examples being the Blaster and Nachi worms. Such infections may cause severe network congestion, leading to systems failure (e.g. if a firewall cannot handle the volume of new connections being made) or degradation in service (e.g. packet loss leading to poor audio-visual quality in H.323 sessions).

However, the risks and threats are no lesser or greater for H.323 end-systems than any other desktop systems in a network. Best practice in software updates and firewall configurations should be applied to all systems. Many H.323 systems are dedicated units with less potential for compromise, but the quality of ‘desktop’ systems that may run a more complete operating system (e.g. Windows® XP) is rapidly improving.

Summary

There are security issues to be considered when using H.323 systems. In this section we have tried to illustrate the most common risks in the context of similar risks to other networked systems in a campus.

The reader should thus bear in mind that, as with all systems, security issues are important, but that in general use, H.323 systems do not require privacy any more than other applications such as e-mail, and the risks can be mitigated by similar steps that are taken for

a site’s general security policy (e.g. firewall implementation, software update regimes, etc.). This document does go into detail on security issues. This should not alarm the reader, given the classes of risk are really not different from other IP-based systems. A site should determine its policy for H.323 security alongside policy for other systems and services. Finally, it is worth noting that some security methods, in particular the use of switched Ethernet rather than bridged (hub-based) Ethernet, will improve network performance as a side benefit. It would be expected that most sites now make extensive use of switched Ethernet.
