Published on *Jisc community* (https://community-stg.jisc.ac.uk)

Overview of H.323 security issues

There are many aspects to the security of H.323 videoconferencing systems. Some of these are shared with H.320 ISDN-based systems, e.g. the physical security of the equipment itself. The greater focus with IP-based systems lies in the ability for attackers to ‘snoop’ the conferencing data in transit, or to attack the H.323 components themselves over the Internet, leading to a loss of service or other undesirable consequences.

For all risks, the likelihood of the risk should be considered, and the impact gauged. While software tools exist to capture and relay H.323 traffic (as discussed in a later section), there are very few, if any, known cases of such non-lawful interception happening in conferences between JANET sites (the JANET and Regional Network backbones are relatively trustworthy, leaving the sites themselves as the only real risk).

As emphasised in H.323 Security in Perspective [1], the risks should be put into perspective. However, the maintainer of an H.323 system should be aware of the nature of the threats.

Issues for consideration

The spectrum of security issues to consider for H.323 includes:

- Physical device security. This includes physical access to the videoconferencing room (the potential for theft or vandalism) as well as methods to prevent users altering critical system settings.
- Local analogue snooping. Even in an IP-based system, local technical staff may easily ‘snoop’ on a videoconference via analogue connections from the local studio, depending on the exact configuration of the studio system. This may not necessarily be in the same room as the ongoing conference.
- Analogue video recording of conferences. It is extremely easy to video record an ongoing videoconference. This could be carried out, either unknowingly or knowingly to the participants, by a valid participant and may have security implications if the resulting tape fell in to the ‘wrong hands’. There are also Data Protection Act [DPA98 [2]] issues to be considered; the JISC Legal Information Service has some useful guidance on the DPA [JISC-DPA [3]].
- Security of devices over the network. General best practice should be applied for H.323 system security, just as with regular Internet device security – many H.323 systems are built on Windows® or other operating systems.
- Session eavesdropping by intruders. Where data is transmitted over insecure (nonencrypted) networks, attackers may be able to snoop the data in transit and view and/or record or redirect a copy of the video/audio data.
- Session hijacking by intruders. It is possible that an attacker could gain control of a session (via the MCU), or could silently join a conference. Note that the normal mode of operation for the JVCS IP offers only ‘dial-out’ for H.323 videoconferencing, from the

MCUs, reducing the likelihood of this threat.
- Network denial of service attacks. If any of the H.323 components are subjected to a denial of service attack, the quality of the conference may drop for all participants, or in the worst case, the conference may fail.
- Secure management of H.323 devices. Many H.323 devices may only be managed or upgraded over non-encrypted Telnet, Hypertext transfer protocol (HTTP) or FTP sessions. An attacker may thus be able to snoop passwords in transit and gain access to critical H.323 components.

These threats, and appropriate countermeasures, are described in subsequent sections of this guide.

While in many security domains authentication is an important issue, in videoconferencing the participants can be seen and heard, and thus generally recognised. In the context of Janet Videoconferencing, with the MCU calling out to pre-booked studios, there can be some confidence that the correct studios will be participating (although preventing unwanted additional participants joining is a separate issue). The same applies to ISDN.

Privacy requirements

While many may consider the academic domain to be one that is not necessarily in need of conference privacy or security, there are many videoconference sessions that users may feel protection, or indeed patient or subject privacy may require protection, e.g.:

- personal interviews for vacancies at the interviewing site;
- project review meetings;
- discussion of material covered by a Non-Disclosure Agreement (NDA);
- medical or other domains where confidentiality is critical.

A site should consider whether open e-mail is being used for discussion of these topics, or whether PGP is in use. The policy for security (privacy) of the data should be set by the owner of the data, and applied equally to e-mail, file retrieval and H.323 conferences regarding the data. In the vast majority of cases, e-mail is not encrypted, thus open H.323 sessions should not be a concern.

Note that Janet Videoconferencing does not currently support the option for session encryption. It may thus be the case that where confidentiality of data is critical, videoconferencing is still best performed over private (ISDN) links. The risk, and the resulting policy, is one for the participants to assess. If the videoconference is held between JANET organisations, the data will only cross the JANET backbone, the Regional Networks involved, and the site (campus) networks. If other sites (e.g. in the USA) participate, the conference data will be seen on links across the Atlantic. Considerations for potential data interception or recording are discussed later in this guide.

The H.323 suite of protocols includes H.235 security mechanisms for authentication, integrity, privacy (encryption) and non-repudiation (proof that a certain device took part in a session) [H235 [4]]. However, H.235 support in H.323 terminal equipment is currently still limited, despite the availability of a defined standard since late 1999 (albeit a standard under revision). While the Cisco® IOS (the operating system for its routers) does have some support for H.235, part of the reason for lack of implementation in clients may be concerns over performance issues

(for H.323 video and voice-only conferencing). It is the lack of client support that is critical; note that if any terminal in a conference is insecure, it weakens the security of the whole conference. Also, where multi-party videoconferences are run using MCU equipment, the MCUs also require H.235 support.

Specific H.323 security implementation issues

As described in Firewalls & Proxies [5], there are specific problems in implementing security policies for H.323 systems. One key issue is that the H.323 protocol does not use fixed, well-known TCP/IP (Transmission Commission Protocol/Internet Protocol) port numbers for communications. Instead the port numbers used are negotiated ‘on the fly’ by the application. As a result, a firewall cannot be configured to allow only the required ports through to the internal network, because those ports are not known in advance.

To solve this issue, some firewall vendors have implemented an H.323 ‘interpreter’ to their products that listens to the initial packet exchange to learn which ports to then open up for the subsequent conferencing data. However, this problem adds complexity to H.323 solutions, especially where the communicating sites run Network Address Translation (NAT) as well. Alternatively, more endpoints now have the ability to select fixed ports to be used that can in turn be configured on the firewall (but this is not yet widespread).

Source URL: https://community-stg.jisc.ac.uk/library/janet-services-documentation/overview-h323-security-issues

Links
[1] http://community.ja.net/library/janet-services-documentation/h323-security-perspective
[2] http://community.ja.net/library/janet-services-documentation/references-further-reading-0#DPA98
[3] http://community.ja.net/library/janet-services-documentation/references-further-reading-0#JISCDPA
[4] http://community.ja.net/library/janet-services-documentation/references-further-reading-0#H235
[5] http://community.ja.net/library/janet-services-documentation/firewalls-and-proxies