H.323 device security

The security of H.323 devices falls into four broad categories:

- Physical security. Studio systems will be in well-known locations, and shared by many users, although only administered by a small set of people. Controlled access will rely on lock and key methods, and supervised attendance. H.323 systems should have local passwords set to protect systems settings, where users are able to access such settings (e.g. via keyboard or remote control)
- Operating system security. Many H.323 terminals are based on standard operating systems, e.g. Windows® NT. Such terminals may have weaknesses tied to those operating systems. It is thus important to apply best practice as described by JANET CSIRT [JCSIRT [1]] and similar advisory bodies and services. It is prudent to check such systems by using common and freely available port-scanning software (e.g [NESSUS [1]] or Security Administrators Integrated Network Tool (SAINT?) [SAINT [1]]).
- Access control. H.323 devices will usually require remote management (either for upgrades and configuration changes, or to control active conferences) that requires secure access control and authentication methods.
- Firewall security. This is discussed in the later firewall section. However, note that at least some services need to be allowed to connect to the H.323 equipment, and firewalls cannot protect against flaws or bugs in those services that may compromise security. Also, not all firewalls are able to protect against denial of service attacks.

There may be specific issues with certain types of H.323 equipment. These are discussed below.

Accounting for H.323 use

A site's H.323 equipment is a resource that is likely to have required some expense in terms of capital outlay and staff time to set up and maintain. Where QoS methods are used by a site to give priority to H.323 traffic, accounting is desirable, such that accurate records are kept of who used the equipment and when.

The charging policy for use of facilities is a site issue, and is not in scope for this guide. Many sites may decide to make use of the studio H.323 equipment as cheap as possible (or free) to promote its use, but for some sites the bandwidth used will be a valuable resource (especially colleges with relatively low bandwidth links to JANET or their Regional Networks).

An H.323 gatekeeper device can control the bandwidth allocated to a conference participant; thus it may be that sites with low bandwidth links prefer to use lower bandwidths for H.323 videoconferences.

Authentication to use H.323 services

Ideally the use of and access to H.323 terminal equipment would be controlled by methods (e.g. certificates) that identify users. In practice, IP addresses are used as a weak form of authentication in the vast majority of H.323 terminals, as they are with most other devices. There is no public key or certificate (e.g. X.509) infrastructure deployed in UK education and research that could allow user (certificate)-based authentication.

Indeed in the case of studio systems the IP address of the system will most probably be static, but a wide range of people will use the equipment. Thus the IP-based admission control for devices such as MCUs only identifies a particular studio, not the studio's users. In the case of desktop systems, it is more likely that one user will commonly use the same IP address, though by no means a cast-iron way to perform identification.

Identification of sources will be important, not least to enable the QoS provision in the first instance. In the WVN [WVN [1]] each site has an IP address allocated from a central subnet; all Premium IP QoS is only applied to that subnet, where traffic comes from dedicated interfaces on site access routers.

However, H.323 device management does require some form of password authentication, as outlined in the next subsection.

H.323 device management

A site may need to manage H.323 terminals, gateways, gatekeeper or MCUs, although in most cases a site's H.323 infrastructure will probably be limited to a studio-based H.323 terminal and, perhaps, a gatekeeper.

Management of H.323 devices is generally offered by:

- Telnet access using a login and password;
- web (HTTP) access with username and password;
- Trivial File Transfer Protocol (TFTP) upload with username and password.

The use of Telnet or HTTP sessions, as opposed to SSH or Secure Hypertext Transfer Protocol (HTTPS) sessions, means that usernames and passwords for equipment access are sent in plain text over the network. It is thus important that management of the device(s) in question is performed locally, over some dedicated infrastructure, or at least over a fully switched network where the chances of access information being snooped are minimised. In some cases devices may be upgraded or hold configurations served by TFTP, or performed via FTP. In such cases the security of the TFTP server is important, lest default settings on the equipment be changed.

Other problems to look out for include the use of default usernames and passwords, which are public knowledge, and a potential problem if not changed when the equipment is installed, e.g. 'admin' and 'GWrv' is a combination used in one particular piece of equipment. Related security bulletins are not uncommon, e.g. [ISSPOLY [1]].

A site should use filtering at a border firewall to block external access to management interfaces where not required from external locations.

MCU-specific issues

MCUs are not discussed in this document. The Janet Videoconferencing service includes provision of MCUs for use by JANET sites participating in H.323 conferences.

For reasons stated above, cascaded MCU architectures do not work efficiently, thus sites should not deploy MCUs, except for purely local use.

Gatekeeper-specific issues

It is anticipated that most sites using Janet Videoconferencing service will run their own gatekeeper, although in some cases (e.g. external guest sites, or sites new to H.323 videoconferencing that have a Coder/Decoder (CODEC) terminal but are yet to deploy a gatekeeper) Janet Videoconferencing gatekeeper may be used. Functions offered by the gatekeeper include:

- address resolution between E.164 numbers and IP addresses - if H.323 calls are placed by name, these need to be resolved to network layer addresses to allow the network connection to be made;
- admissions control and call authorisation (ITU-T Recommendation Q.931) based on policies set up by the gatekeeper administrator;
- bandwidth control, for example by limiting the number of sessions and/or participants to allow the best opportunity for existing sessions to perform well;
- zone management, handling requests from clients in its administrative zone;
- call management (this is a proxy function), and handling release afterwards.

A port scan of a gatekeeper device may typically show FTP, Telnet and HTTP access available, as well as H.323 call set-up ports and User Datagram Protocol (UDP) network management and Simple Network Management Protocol (SNMP) services. There is no reason generally to allow off-site access to the general service ports on the gatekeeper (FTP, Telnet, HTTP or SNMP), so these should be blocked at the site firewall where possible. If possible, unused services should be turned off on the gatekeeper.

Measures to help improve security related to gatekeepers include disabling multicast IP discovery of gatekeeper(s). It is safer to manually configure gatekeeper addresses in site deployments to remove the possibility of rogue gatekeepers being introduced.

As with MCUs, ensuring device software or firmware is kept up to date, especially where security vulnerabilities may have been announced and fixed in updates. Operating System (OS) updates should be applied, though the vendor should be consulted as to whether security updates may impact the operation of the equipment itself. Gatekeepers should be regularly port-scanned to ensure only desired services are being advertised.

Denial of service

If a large or important conference has been scheduled, the inability of one or more participants to take part due to a loss or Denial of Service (DoS) can be critical. While experience shows that DoS attacks on JANET backbone equipment is rare, and thus attacks on JANET H.323 backbone infrastructure (MCUs and gatekeepers) should also be rare, attacks on terminals may pose a problem.

One defence is to run an Intrusion Detection System (IDS); these are available commercially, but many open source packages such as Snort® [SNORT [1]] are of good quality. Such packages can detect patterns of traffic that are likely to lead to problems for the end system. This might include network patterns such as a SYN flood attack (which may cause the receiving TCP stack to fail) or it may be a pattern taken from a known attack on an application, or it may detect port-scanning activity. For H.323 units, the network layer DoS attack detection is certainly useful. A number of firewall products also include a certain amount of intrusion detection capability.

An IDS may also be beneficial in detecting other forms of attacks in a site, e.g. specific attacks on web servers, or use of certain types of peer-to-peer file sharing software. In addition to attacks on equipment, there may be other failures that should be checked against, from component failure to configuration issues (e.g. layer 2 network issues where Ethernet half/full duplex negotiation is not handled properly by equipment).

Links
[1] https://community.ja.net/library/videoconferencing-booking-service/references-0