Call snooping, recording and unwanted guests

It is theoretically possible that in an H.323 conference an ‘outsider’ could snoop the session, recording or relaying an apparently private conference (by inspecting data in transit) or that a snooper is able to silently join a conference (by connecting to an MCU). For an attacker, gathering data ‘on the wire’ is safer as it reduces the chance of detection and being later traced.

We should clarify that such interception, while possible, is likely to be very rare in conferences involving purely JANET sites. Indeed we are not currently aware of reported incidents of such snooping occurring in existing UK H.323 networks, including the WVN. As described below, there are public domain tools available to record or relay H.323 Real Time Protocol (RTP) streams. It is also possible for call set-up information to be snooped, allowing sessions to be silently joined via a gatekeeper/MCU.

In this section we describe the problem, in the next section we present potential solutions. The most obvious counter-measure is encryption, but the standard defined for H.323 for encryption, H.235, is not widely deployed, and very rare to find on H.323 terminal equipment. VPN-style solutions may work well point-to-point, but would be complex to deploy in conjunction with MCUs, while work on Secure Real-Time Protocol (SRTP) [RTP [1]] is still in the early stages.

With or without encryption in place, switched Ethernet networking should be used on paths between H.323 device locations and site access routers.

H.323 session snooping or recording

In an H.323 session, the audio and video data are each transmitted in their own RTP stream. An H.323 client terminal receives the RTP data from its peer or the MCU such that it can play back the picture and sound to the terminal user(s). It is thus quite possible for an attacker/snooper to capture all the data and replay the video, given appropriate software.

Tools exist that may perform a significant part of the task, including the OpenH323 Project code [OPEN [2]]. Successful RTP recording has been reported !!REFERENCESEUSS] through use of the Digital Network Analyser 323 [FIREBERD [3]], an H.323 enabled packet sniffer that is capable (amongst other things) of capturing RTP audio in an H.323 call and replaying it on the soundcard of a local machine. RTP reflectors are also widely available, including a number of reflectors written for Access Grid sites (where multicast to unicast RTP reflection is often necessary), e.g. Quickbridge [QBRIDGE [4]] as currently used for UK Access Grid nodes which do not have a native IP Multicast service.

Clearly, software to snoop, reflect or record RTP-based non-encrypted H.323 conferences is readily available. Capturing a long conference may require many gigabytes of data, but because the audio is a separate RTP stream, a snooper need only record that to gain the bulk

of the important data in terms of information disclosure.

Note that an MCU is a critical point for snooping, because video and audio data from every participant will be sent to the MCU, which then chooses which streams to relay to all viewers. Thus if you can snoop at the MCU, you can see all participants. But conversely, you only need to be able to snoop at any one location to be able to capture the whole conference. One should feel confident in trusting the security of infrastructure at JANET C-PoPs, but there may be particular weaknesses where non-JANET sites are involved in conferences, and data travels over (relatively) unknown overseas networks, Internet Service Providers (ISPs) and sites.

Other available data

In addition to the RTP data comprising the video and audio of a conference, the call set-up exchanges between the H.323 terminal and the gatekeeper and MCUs are also sent over the network ‘in the clear’ (unencrypted) and thus liable to be snooped.

By monitoring such traffic, e.g. to ports 1719 and 1720, it is possible to gather information such as software versions being used, conference access identifiers, and the IP addresses of gatekeepers and MCUs. Such information may, possibly coupled with other sources of information, allow an attacker to later join a conference without detection.

Controlling access to conference sessions

It is very important that unwanted participants are not able to join sessions, particularly without detection. Some form of access control should thus be implemented (at least by source IP address), and sessions should be monitored (at the MCU) to check which devices are connected. Such features are commonplace in most MCU equipment.

Although unlikely, it may be possible for an attacker to take a genuine H.323 terminal offline, and replace it with their own device answering on the same IP address. This would require local site knowledge, and almost certainly the masquerading device to be at the ‘victim’ site. By utilising the Global Dialling Scheme (GDS) and E.164 numbering scheme (as used by JVCS to dial out), we provide a further step that would have to be implemented by any intended ‘snooper’. There would be a requirement for the ‘snooping’ endpoint to register with the local gatekeeper with an identical E.164 address in order to join the videoconference. As stated previously in this guide, access control is one reason why in Janet Videoconferencing, the MCU calls the participant terminals, rather than vice-versa.

Booking system considerations

Although most sites will only use the JANET Videoconferencing Booking Service, it is important that where any publicly-viewable booking details are displayed, they do not reveal any useful information to potential attackers or snoopers, e.g. IP addresses of devices, conference sessions IDs, etc. However, such information may also be of use to diagnose conference connectivity problems, thus a balance between security and maintenance needs to be struck.

Summary

H.323 session interception and recording is theoretically possible. The trusted nature of the

JANET and MAN backbones, taken together with prudent use of dedicated links, Ethernet switching or VLANs within a site, makes the likelihood of an incident occurring very low. There have as yet been no reported incidents in existing UK academic H.323 networks such as the WVN.

Links
[1] http://community.ja.net/library/janet-services-documentation/references-further-reading-0#RTP
[2] http://community.ja.net/library/janet-services-documentation/references-further-reading-0#OPEN
[3] http://community.ja.net/library/janet-services-documentation/references-further-reading-0#FIREBERD
[4] http://community.ja.net/library/janet-services-documentation/references-further-reading-0#QBRIDGE