Encryption, IP security (IPsec) and VPNs

H.320 (ISDN) videoconferencing users have been accustomed to assuming that videoconference sessions are private, thanks to the point-to-point circuit-switched nature of their ISDN calls. The ISDN network is not so readily accessible to the public, and thus not as liable to be snooped.

In contrast IP networks are built open and end-to-end mode of operation over many interconnected networks, some of which are ?trustworthy? (like the JANET and Regional Network backbones) while others are not (e.g. overseas networks where a conference participant is connecting from a non-JANET site). The potential for IP snooping exists, albeit with a low risk. In contrast to other services, e.g. e-mail or interactive access by a researcher with a laptop using Wireless LAN in an overseas conference, H.323 is relatively secure because the end stations are deployed in well-controlled, Ethernet switched networks with trustworthy education and research networks interconnecting them.

In this section we discuss the encryption options available for deployment in the context of H.323 services. In practice, encryption is not being used now, with the possible exception of T.120 with NetMeeting®. However, an understanding of the general issues of encryption is useful for those operating H.323 systems.

Encryption requirement

While use of switched Ethernet networks on sites reduces the chances of snooping, as can choice of site topology (e.g. by plumbing the H.323 terminal directly to the site edge router), end-to-end session privacy can only be truly offered by use of session encryption.

It should be noted that very few, if any, current H.323 conferences use data encryption. It may be desirable for some types of conference, e.g. discussing confidential patient data in research meetings, but, as with use of e-mail, plain text transmission is the norm.

H.323 includes its own encryption standard called H.235, but implementation in H.323 terminals is currently rare. Some H.323 proxy equipment, including that from Cisco®, supports H.235, so it may be possible to establish secure sessions between proxies if a site happens to use such a proxy, but that would still leave data transmitted within the site exposed to snooping. Proxies are often deployed either out of necessity (the internal site network uses NAT) or to ?simplify? security requirements (H.323 sessions are trusted only to the proxy, which then relays data to real terminal endpoints).

Data encryption using T.120

One piece of encryption technology that is available for H.323 is the support for T.120 encryption in the Microsoft® NetMeeting® product. It is possible to use NetMeeting® T.120 ?out of band? without audio or video enabled, to purely share data (e.g. a PowerPoint®

presentation) via an encrypted session, while a separate H.323 conference call is being run between multiple studio-based systems.

At the time of writing the JVCS-IP does not support the use of software-only CODECs such as NetMeeting®, due to the difficulties caused in multipoint videoconferences. However, this is being kept under review and may change in the future.

H.235 encryption

H.235 [ITU] can be used to encrypt video, audio, terminal-to-gatekeeper signalling (H.225), call signalling (H.225) and system control (H.245) as of Version 2 of the H.323 standard [PACK]. It includes some methods for authentication and key management. In theory, end-to-end and hop-by-hop (e.g. proxy-to-proxy) security is possible.

H.235 covers not just encryption, but the broad scope of authentication, integrity, privacy, and non-repudiation. Authentication is provided by admission control of endpoints via the zone gatekeeper. Data integrity and privacy are provided by encryption. Non-repudiation ensures that no endpoint can deny that it participated in a call. H.235 is able to use existing standards such as IPsec and Transport Layer Security (TLS) [TLS].

The general problem with adoption of H.235 is that client (terminal) implementations are rare, and thus it is unlikely that two H.323 session participants will be able to make common use of the standard. Thus H.235 is something that is not of practical use now, but as the JVCS-IP matures, client implementations may emerge that enable its adoption and use. Thus when procuring equipment, it is worth enquiring about H.235 roadmaps from vendors.

Virtual Private Networks (VPNs)

A network layer VPN using IPsec offers a solution by which hosts or networks that lie in remote locations can be allowed to communicate in secure, private networks over a public network (such as the Internet). This is a method commonly applied to corporate customers by ISPs.

IPsec [IPSEC], may be used to encrypt data between IP devices, usually from gateway (router) to gateway (router), but also often host to gateway (the classic ?road warrior? scenario of a travelling businessman wanting secure access back to their home corporate network). A security association needs to exist between VPN devices, which can be established on the fly, or by static, manual configuration. The latter is far more common in general VPN deployments.

There are in fact two different types of session encryption, defined by Request for Comments (RFC) 2401 [RFC2401], and RFC2406 [RFC2406]. The two modes are:

- **Tunnel mode.** Generally used gateway-to-gateway, the encrypted IP header and databeing tunnelled inside a point-to-point connection between the gateways. Tunnel mode adds packet overhead due to the extra ?wrapper? IP header, but it also hides the identities of the communicating hosts thus a snooper would just see traffic between gateways, and not know which hosts were communicating. The encryption only applies between gateways, so hosts on the internal network behind the gateway maybe able to snoop the non-encrypted site traffic.

Image not found file:///var/privatewebfiles/privatefiles/public_images/VC%20H.323%20Security%20Figure%204.JPG

Figure 4: Tunnel mode encryption

- **Transport mode.** Here the encryption is applied end-to-end and only the payload is encrypted. This means security is established along the full path of thecommunication, so even hosts inside the site will not be able to see any nonencrypted traffic. However, snoopers will be able to detect which IP hosts are communicating. Sites running NAT internally will not be able to use transport mode as both ends of the connection need globally routable IP addresses, and NAT would break the security association. This is a strength of IPv6; there are enough addresses, and there is a requirement for a full implementation to support Authentication Header (AH) and Encapsulating Security Payload (ESP) headers for security. The AH provides the mechanism for assuring the identity of the sender of the data [RFC2402], the ESP provides encryption (privacy) of the data [RFC2406] in the context of IPsec [RFC2401]. Encryption applied end to

  Image not found file:///var/privatewebfiles/privatefiles/public_images/VC%20H.323

  endPublic InternetFigure 5: Transport mode encryption

In practice, an H.323 session will always need to be protected using tunnel mode IPsec, because the H.323 terminals do not usually themselves have the ability to run transport mode IPsec (since they are usually dedicated H.323 devices in the case of studio systems).

Thus if a site is interested in using encryption for some H.323 sessions, it should deploy a VPN (tunnel mode IPsec) gateway in series with the H.323 terminal as topologically close to that H.323 equipment as possible. Such a device may not need to always be used, but if some point-to-point sessions are required to certain locations, the option exists to ?turn on? IPsec (the gateway is configured to use encryption to certain destination network prefixes, otherwise traffic passes through as normal, unencrypted). Such a device/gateway could also host network performance and monitoring tools to allow the site H.323 terminal to be monitored as closely as possible to the device itself. The JVCS-IP will include some measure of link monitoring.

A problem faced in using VPNs is that all session participants would need to share security associations, and have appropriate gateways. Thus while deployment of a VPN for a point-to-point H.323 session would be (relatively) simple to achieve, establishing a VPN for a multiparty conference would require VPNs to span MCUs and other H.323 devices, a task which is potentially very complex.

It is certainly worth noting that JANET offers no general VPN services, thus to expect VPNs to be used on the JVCS-IP is at present somewhat unrealistic, especially given the VPNs may need to span any combination of end sites (200 universities, and possibly many hundreds of colleges). It is also worth noting that use of encryption in general is not common on JANET, and between JANET sites. Many web services are beginning to use SSL encryption, but e-mail is almost invariably sent plain text, even with confidential or private contents (despite the availability of encryption methods such as PGP).

Open source session encryption tools: FreeS/WAN

Here we briefly describe some open source tools that can be used to establish a VPN or IPsec connection for an H.323 session. A fuller list of general tools is given in the reports of the UKERNA VIP Project. Commercial products also exist, e.g. from CheckPoint® [VPN] and Symantec® [SYMVPN], but these can be costly to acquire if only required for H.323 use.

FreeS/WAN [FREE] is an open source IPsec implementation that runs on the Linux® platform. It uses Internet Key Exchange (IKE) [IKE] for key exchange, through a daemon called Pluto. The ?S/WAN? name stands for Secure Wide Area Network. It includes the ability to run ?opportunistic encryption?, such that any two FreeS/WAN gateways will encrypt data when traffic is observed flowing between them.

One of the key objectives of the FreeS/WAN project is, in the designers? words, to ?help make IPsec deployment widespread by providing source code which is freely available, runs on a range of machines including ubiquitous cheap PCs, and is not subject to US or other nations? export restrictions?. FreeS/WAN was tested as part of the VIP Project [VIP], and performed well. It would seem to be a good, low-cost solution for sites wishing to investigate H.323 session encryption (and VPN deployment in general), living up to its designers? goals.

A major new version release, v2.0, is due very shortly at the time of writing (v2.00-pre2 is the latest advanced version, with v1.99 being the current stable version). The FreeS/WAN site[FREE] includes pointers to mailing lists where support is readily available.

Performance impact of encryption on H.323 sessions

One aspect to consider if using a VPN is the effect on performance of the H.323 sessions. In trials run within the VIP Project, tests were run using FreeS/WAN in tunnel mode between two gateway devices (commodity PC routers), with H.323 terminals directly attached.

Client applications ran on a Pentium® 3 and a Celeron® 400 desktop, with Pentium® 3 866MHz, 128MB PCs running SUSE Linux® 7.0 and FreeS/WAN 1.8. While throughput was affected, UDP tests showed an approximate 10Mbit/s throughput was achievable, and there was no perceivable subjective impact on the actual H.323 session in terms of quality. The encryption was verified by snooping the session with Ethereal [ETH][V2S]. The performance obtained was significantly improved upon previous tests run two years earlier on lesser equipment at the University of Wales, Aberystwyth, thus one can assume performance on a new ?entry-level? rack-mount PC router (running at 2GHz or more) would be improved further.

Security implications with IPv6

IPv6 deployment is still in its early stages [IPv6]. UKERNA introduced a pilot IPv6 service on the JANET backbone in 2003 (dual-stack IPv4 and IPv6 running together), with a native service becoming available to sites, subject to Regional Network provision, during 2004. IPv6 has advantages over IPv4 including much expanded address space, and the requirement for implementation of AH and ESP headers in fully compliant (RFC2460) IPv6 stacks.

The OpenH323 project [OPEN] now has IPv6 functionality, which is used by the Linux® open source GnomeMeeting H.323 compliant application [GNOME]. While not all videoconference endpoints may use IPv6, it may be possible to have dual-stack gateways or MCUs to enable IPv6 participants to join a session with IPv4 users, in a similar way that ISDN users can be bridged into a videoconference. However, this is not something for general

H.323 deployment in the immediate future.

One interesting issue IPv6 does raise is the use of RFC3041 Privacy Addresses, through which IPv6 hosts (that would otherwise have the same host part to their IPv6 address when statelessly autoconfiguring in multiple networks) can dynamically change their IP (source) address periodically to reduce the chances of network location-based tracking occurring. This feature is seen as a privacy advantage for IPv6, but it does mean that IP source address-based filtering may not be so easy to operate.

Proprietary encryption

There are some proprietary encryption methods offered by some vendors. Unfortunately in general these are not interoperable, and are thus generally only of use in closed homogeneous systems.

In future revisions of this guide we will report on IP-based encryption options for widely deployed systems such as those from Tandberg and Polycom. Microsoft® NetMeeting® includes data encryption features [NMSEC]. The T.120 data channel can be encrypted (this includes the chat and shared whiteboard accessories). There is
no built-in encryption option for the audio or video streams.

Summary

There is no widely available, scalable and interoperable method to enable encryption between H.323 systems participating in JVCS-IP conference calls. H.235 is still in its relative implementation infancy. VPN solutions exist, and can typically be deployed gateway to gateway (site to site), but do not scale to a JANET-wide platform for secure communications.

It is thus not a surprise that very little, if any, use is made of encryption today for H.323 conferencing over JANET. However, one should also bear in mind that other applications, in particular e-mail, are also routinely used without (PGP) encryption.

Unless the subject matter of a conference call is highly confidential or sensitive, unencrypted H.323 sessions will remain the norm. Site managers should review H.323 encryption policy alongside other encryption policies.
