

*Employing IT-Level
Security for IP
Videoconferencing*



Employing IT-Level Security for IP Videoconferencing

Ira M. Weinstein
Wainhouse Research

January 2006



TANDBERG

Table of Contents

Introduction.....	1
IT Security Concepts Relevant to Conferencing	2
Authentication and Policy	2
Data Privacy	3
Internet Security (Firewall / NAT)	4
H.235 and H.460 Videoconferencing Security Recommendations	5
Conferencing-Specific Security Concepts.....	6
Device and Environment Management	6
Attendee Control	7
Content Security	7
A Typical Secure Videoconferencing Environment.....	8
Real World Examples	9
Guest Endpoint Access.....	9
Participant Control.....	10
Videoconferencing Security Futures	12
Conclusion	13
About Wainhouse Research	14
About the Author.....	14
About TANDBERG	14

List of Figures

Figure 1: Layers of Security	4
Figure 2: Typical Enterprise Security Implementation.....	8
Figure 3: Non-Secure vs. Secure Guest Endpoint Access	9
Figure 4: Non-Secure vs. Secure Participant Control	10
Figure 5: Non-Secure vs. Secure Participant Control Flowchart	11

Introduction

In recent years videoconferencing has morphed from an ISDN-centric to an IP-centric model. In fact, most videoconferencing systems today support IP networks out of the box, while ISDN network connectivity – once the de facto standard – has become an optional add-on. The addition of IP capabilities to videoconferencing systems and infrastructure devices has provided many performance, management, and cost benefits and has paved the way for large-scale deployments of videoconferencing within the enterprise.

The migration of IP video traffic (including device management and actual multimedia data) onto the IP data network has brought videoconferencing into the realm of the IT and network management staff. This, in turn, has spawned great interest in maintaining enterprise-level security within the videoconferencing environment.

Security professionals know that contrary to popular belief, most security violations come from internal rather than external sources, which means that protecting your network environment from outside intruders is simply not enough. Videoconferencing, with an often high profile user base and confidential meeting content, represents a new area of concern for IT / network managers.

Security professionals know that maintaining security requires protecting your network from both external and internal intruders.

This white paper focuses on the key security concepts that IT, network, and conferencing managers must consider in order to maintain security throughout their enterprise videoconferencing environment.

IT Security Concepts Relevant to Conferencing

In recent years a number of IT security concepts, including authentication / policy, data privacy, and internet security, have become increasingly important within the videoconferencing universe.

Authentication and Policy

Authentication is the process of identifying users and/or devices (such as videoconferencing systems) as they attempt to log in to the network or environment. Since a person's (or device's) right to access data, applications, network resources, bandwidth, etc., is based on his (or its) identity, it is vital that the identification process is completed properly and securely.

Identity Verification

The most important part of authentication is to ensure that the person or device asserting an identity and requesting rights is actually who or what they claim to be. In other words, is that user logging in as John Smith really John Smith? Is that system logging in really the London 22nd Floor Boardroom VC System? This verification can be accomplished using any of the following:

- 1) Password – Something the user or device provides or knows (like a password or pin number) that can be changed as required.
- 2) Physical Token – Something the user or device has (such as a security card / secure ID device / password generator) that provides passwords or codes that cannot be changed by the user.
- 3) Physical Attribute – Some part of the user's biometrics (fingerprint, handprint, palm print, facial recognition, retina / iris scan, voice recognition, etc.) or special signature within the device that is unique and difficult (if not impossible) to alter.

To increase the level of security, two or more methods can be used together, a process called two-factor authentication. For example, many enterprise organizations require users to enter both a user password and a secure ID password as a part of the network authentication process.

It's All Password Protection

The above methods may seem totally different, but each involves the transmission of one or more unique strings of data (either provided by the user or by a device) from the client computer or endpoint to an authentication / logon server. Unfortunately, these data strings are often sent without encryption in clear text, which may allow someone to capture the password characters during the transmission. The risk of password eavesdropping is especially high for HTTP / web-based applications and systems.

Two common methods are used to protect passwords during transmission: password encryption schemes (such as secure sockets layer or SSL, transport layer security or TLS, and Kerberos) and challenge / response mechanisms (including HTTP Digest Authentication or DAA, and NT LAN Manager or

NTCR). While there are advantages and disadvantages to each method, the key is that the passwords are not transmitted as clear text, making it virtually impossible to capture passwords during authentication.

Another important aspect of password protection is to ensure that passwords are not stored as clear text within user databases or authentication systems. Instead, passwords should be encrypted so that database or system administrators with access to these systems cannot easily view them.

A final, and often neglected, part of password protection is to take basic measures to keep passwords private, such as not leaving written passwords in public places (such as on post-it notes placed on monitors or under keyboards) and remembering to change passwords on a regular basis.

User and Device Policy

Once the user or device is authenticated, network policies determine the allocation of assets among users or devices. For example, policy determines whether a specified user can access a set of network drives or a network connection. Similarly, in the context of videoconferencing, policy determines items such as when an endpoint can place or receive calls, at which call speeds, and with which sites it can communicate.

In addition, policy determines the privileges or access provided to guest users and endpoints that have not been authenticated. For example, “guest” users may have access only to the public Internet, but not the company Intranet. Similarly, “guest” endpoints may be able to place IP video calls, but not receive IP video calls or access shared resources like video bridges or ISDN gateways.

Data Privacy

In the IT world, data privacy involves the encryption of the “payload” or meeting content traffic between the various systems within the network. This includes transmissions between client PCs, servers, and other devices. Considering that most security leaks usually originate within the client’s network (behind the enterprise firewalls), it is important to encrypt both internal and external data transmissions.

Like other network devices, conferencing systems transmit significant amounts of information over the network – especially while participating in a meeting or call. For example, a typical business-quality videoconferencing call might involve the transmission of more than 500 kilobits per second (kbps) of audio, video, and presentation / rich-media data between the participating sites. Depending upon the meeting topic and participants, this information could be of an extremely confidential nature. Data privacy for conferencing involves encrypting all forms of data traveling between the endpoints or locations, including audio, video, and associate presentation / rich-media data.

Most relatively current video systems display an encryption icon or graphic indicating that the current video call is encrypted. For example, TANDBERG videoconferencing systems display a padlock on-screen (in a manner similar to the way most Internet browsers indicate that the user is visiting a secure site) to indicate that end-to-end encryption is in place. As a rule, if the encryption graphic or message is not displayed on the screen, users should assume that the call *is not* secure.

Internet Security (Firewall / NAT)

Another key security element is the protection of the network from unauthorized access by external users. In most cases, this is accomplished through the use of one or more firewalls that filter traffic traveling between private (internal) and public (external) networks. In addition, many organizations utilize network address translation (NAT) to allow multiple users or devices to access the Internet using a single public IP address, which effectively hides the user's local IP address from external users and systems. When combined, firewalling and NAT provide a relatively strong barrier of protection against external intruders.

From a conferencing perspective, firewalls and NAT keep unauthorized users and systems from connecting to enterprise conferencing systems. Unfortunately, they can also hamper authorized, required connections between internal and external systems.

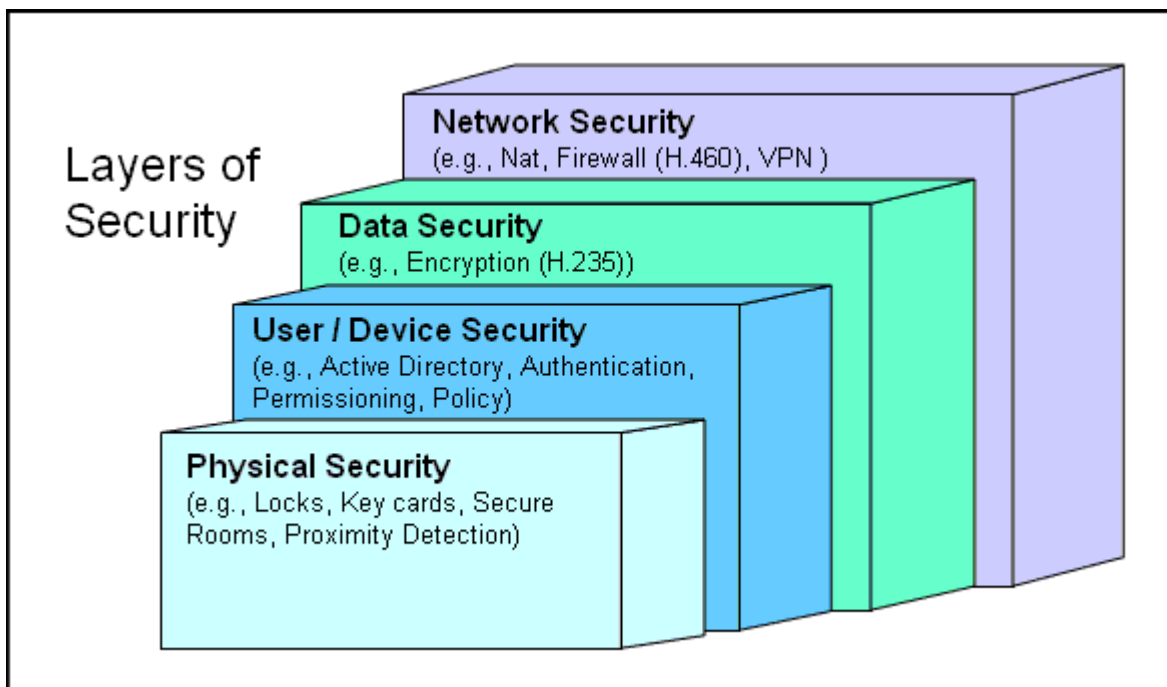


Figure 1: Layers of Security

H.235 and H.460 Videoconferencing Security Recommendations

These security concepts (authentication, policy, content privacy, and internet security) are addressed by the H.235 Annex D and H.460 ITU recommendations for videoconferencing. Specifically, H.235 describes the means for an H.323 video device to do the following:

- 1) Securely authenticate to the central log-on server using encrypted password(s)
- 2) Gain the ability to place and receive calls as per policy rules set by system administrators
- 3) Establish encrypted data flows between itself and other video endpoints / infrastructure devices

The recently ratified H.460 recommendation provides a structure for H.323 videoconferencing traffic to securely traverse enterprise firewalls and Internet security systems through the use of external session border controllers (SBCs). Note that H.460 is not the only way to allow videoconferencing traffic to flow between internal and external devices. But the H.460 method offers several key advantages as follows:

- 1) Typically no firewall hardware or software upgrades are required
- 2) No custom firewall configurations (port forwarding, rule sets, signal routing, etc.) are required
- 3) Additional firewalls, proxies, or application layer gateways¹ are not required
- 4) External users and systems can authenticate with the session border controller and be given specific permissions to communicate with internal videoconferencing systems / devices

Following both the H.235 and H.460 recommendations, which requires the use of H.235- and H.460-capable video systems and devices, is an important part of creating a secure enterprise videoconferencing environment.

¹ An application layer gateway (or ALG) is a proxy designed to provide access control for specific types of traffic. Deploying an ALG for H.323 traffic is one method for allowing H.323 traffic to flow between public and private networks.

Conferencing-Specific Security Concepts

In addition to the IT security concepts that apply to conferencing, certain conferencing-specific aspects of security, such as device management and control, are worthy of consideration.

Device and Environment Management

Over time, videoconferencing has become a mission-critical business tool for many enterprises. As usage and deployments expand, the need for an effective means of managing the videoconferencing environment becomes increasingly vital. Videoconferencing management systems, available from a number of leading vendors, provide a variety of valuable features including endpoint and device monitoring, system management, centralized scheduling, and more. These management systems have the potential to impact the security of the videoconferencing environment.

User Access

The first area of concern regarding management systems is the level of access provided to system users. Some rudimentary management systems provide only front-end security (anyone who goes to the proper URL gains immediate access to all information). Others provide only basic password protection, without user-based permissioning, meaning that all users with the proper password gain access to all management system data and functions. This raises both general security and data confidentiality issues.

Superior management systems interface with enterprise directory systems, such as Active Directory, and provide user-based “tiered” or “hierarchical” permissioning to features, functions, and information based on the individual user’s log in.

System Functionality

In order to function properly, these management systems must have *administrator-level* access to all devices (endpoints, bridges, gateways gatekeepers, etc.) within the global videoconferencing environment.

Superior management systems enforce proper enterprise security including authentication, user permissioning, and message encryption.

In addition, the management system may need access to the enterprise directory systems (such as Active Directory) for permission, policy, and scheduling purposes. Due to its need to communicate with so many different devices and systems, the videoconferencing management system – if not properly controlled – can introduce a significant security risk.

To maintain the security of the environment, management systems should comply with the same security measures previously discussed including proper authentication, policy, and data privacy. Some management systems, for example, send clear-text (non-encrypted) messages between devices within the environment. In order to minimize exposure, all such messages should be encrypted – end to end – and browser-based interfaces should utilize SSL security. This is even more important if the management system is located outside the enterprise firewall, a common scenario for many managed service provider (MSP) offerings.

Attendee Control

Security must also be a consideration during the meeting itself. Specifically, it should be easy to password-protect meetings and deny access to those without appropriate login information. Some organizations may wish to combine this with the organization's authentication and policy process. For example, meeting access could be limited to authenticated endpoints, from specific locations, whose users know the appropriate meeting password.

It should also be possible to create a list of participants permitted to attend the meeting, and to lock out additional attendees (a function available on many video bridges) once all invited and authorized attendees have joined the session. Furthermore, meeting hosts and coordinators should have access to an up-to-date list of all participating locations.

Content Security

It is also important to secure the meeting content. Specific items of concern include any meeting-related files or documents including presentations, associated attachments (Word documents, Excel files), meeting agendas, invitee lists, and more. Many organizations post this type of information in centralized scheduling systems or within enterprise groupware applications. Whenever possible, these items should be password protected, and stored in non-publicly-accessible locations.

Furthermore, it should be difficult for remote users to capture the on-screen content. For example, control rooms should be locked and recording functions should be password protected, making it difficult for attendees to make unauthorized recordings.

In addition, it should not be possible for users to log into the participating endpoints directly to monitor the discussion. If the meeting is to be streamed using either the streaming capabilities within the endpoint or a streaming server / service, attendees should recognize that unless content rights management systems are used, unauthorized people may gain access to the stream. In other words, if streaming is enabled, one should assume that the meeting content is available to the general public.²

Meeting security involves securing meeting files, limiting meeting attendees (video, audio, and streaming), and controlling content capturing.

Overall, meeting content security involves controlling and limiting meeting attendees (either in the video meeting, associated audio add-ons, or viewing via streaming), securing meeting files, and discouraging content capturing.

² In many enterprises, streaming content and the login credentials to streaming servers are not encrypted. This means that, in theory, anyone with access to the network could intercept the login credentials and gain unauthorized access to the streaming media content. Proper network security is a key part of minimizing this risk.

A Typical Secure Videoconferencing Environment

The diagram below highlights a typical secure enterprise videoconferencing deployment including several basic enterprise security systems (active directory server, login server, file server), and numerous secure videoconferencing elements including centrally located infrastructure devices (MCU / gateway, gatekeeper), a secure management system, H.460- / H.235-capable video endpoints, and an H.460-compliant firewall traversal solution.

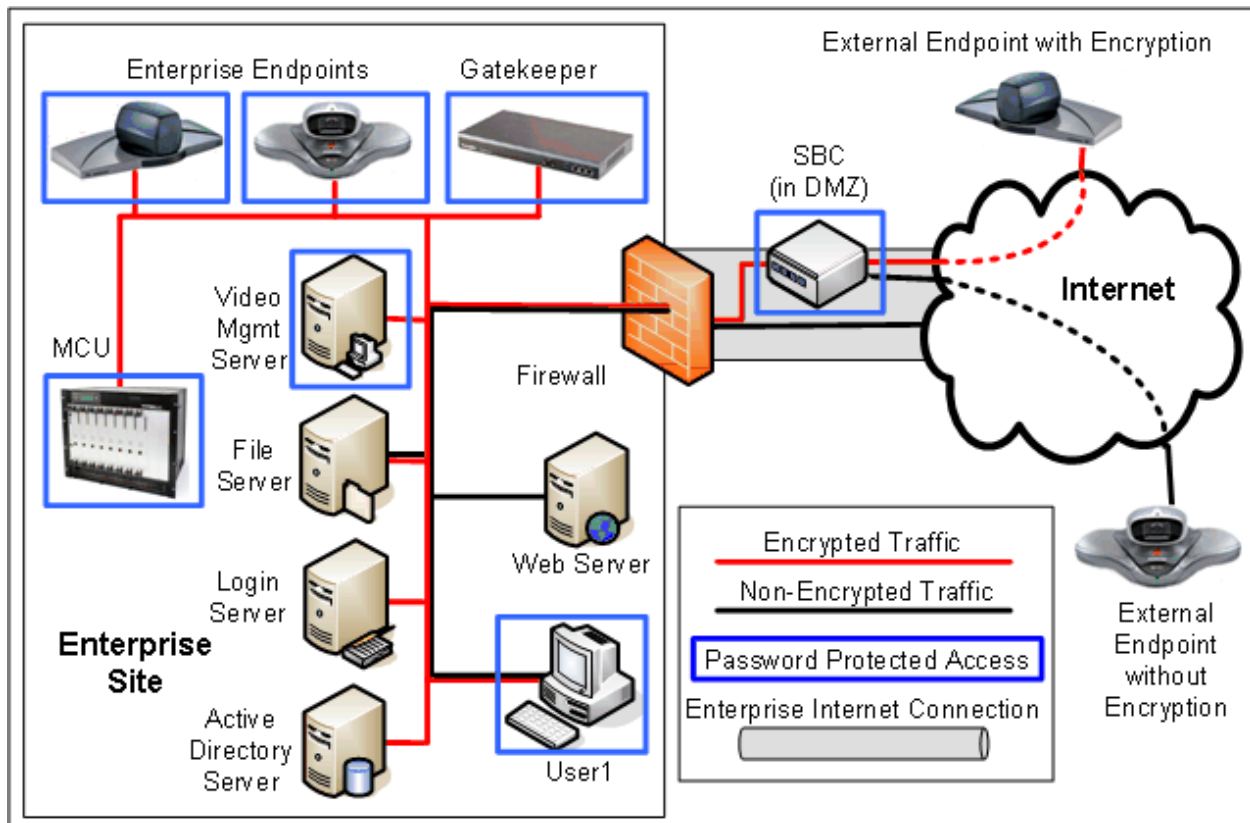


Figure 2: Typical Enterprise Security Implementation

The key to the above drawing is that *all* communications throughout the environment are secure. For example, the data flows between all internal endpoints and the MCU are encrypted, as are the connections between the external endpoints and the session border controller. Similarly, before gaining access to enterprise resources, the user must log into the management system and provide a password – which is then sent in a secure manner to the management system for authentication.

It is also worth noting that even if the external endpoints, which are not under the control of the enterprise, do not support encryption, the area of exposure (during which the data flows are not encrypted) is limited to the data path between the session border controller and the external endpoint as shown above. While not ideal, encryption on 90% of the data path is better than no encryption at all.

Real World Examples

The following examples highlight the benefits afforded by a secure video environment.

Guest Endpoint Access

In this example, a non-authorized endpoint has been connected to the enterprise LAN. This may be the result of a new installation, system upgrade, or deployment of a video system for temporary use (perhaps for a specific event).

Non-Secure Environment - In a non-secure environment, this endpoint would immediately have access to all enterprise resources including MCU, ISDN gateways, and more. In addition, this system would be able to dial and connect to any endpoint within the environment.

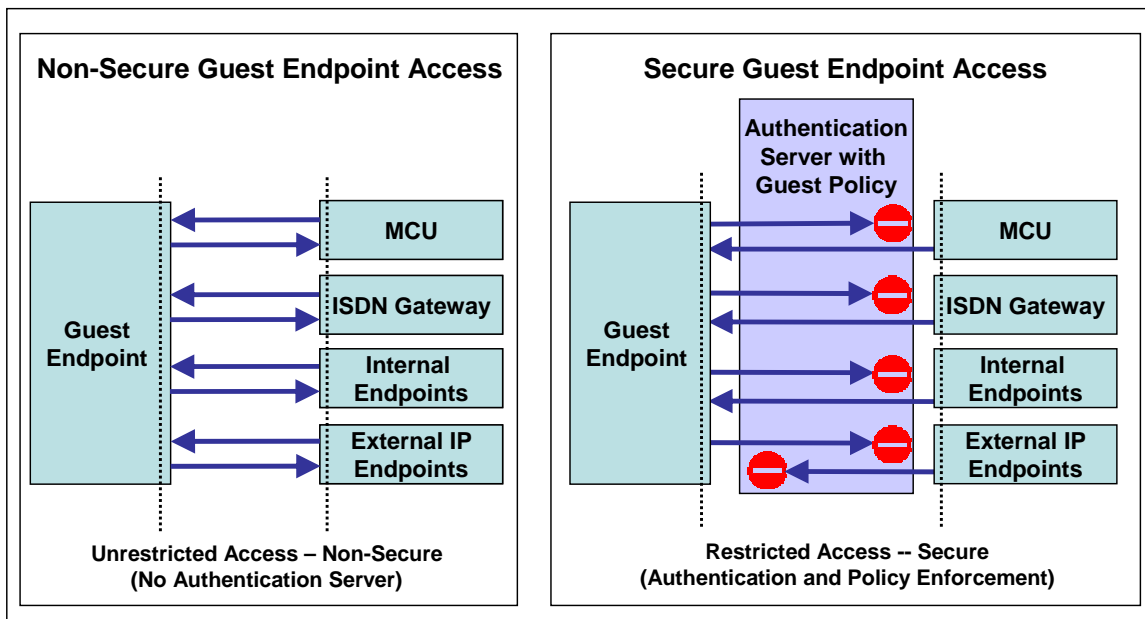


Figure 3: Non-Secure vs. Secure Guest Endpoint Access

Secure Environment – In a secure environment, this endpoint would be unable to utilize enterprise video resources or connect to other endpoints until it has contacted the authentication server. If this endpoint is able to authenticate (i.e. it is an approved endpoint that has been given specific rights by enterprise administrators), it is immediately granted the appropriate rights and privileges. If the endpoint is unable to authenticate, it will receive “guest” privileges only, which depending upon the environment might range from no access to any resources or systems through to full access to the entire environment.

Participant Control

In this example, a technician in one location is seeking to place a series of test calls to remote endpoints. Unfortunately, he has selected the CEO Executive Boardroom, which is currently in use hosting a quarterly shareholder meeting, as one of his test rooms.

Non-Secure Environment - In a non-secure environment, this technician would be able to call any endpoint within the enterprise environment from any location. Thus, when the technician places his test call to the CEO's Boardroom, the video system may – depending upon the system settings – answer the call automatically, or perhaps even add the technician to the video meeting already in progress. In other words, the technician's testing could interrupt the CEO's presentation and perhaps give the technician unauthorized access to confidential information.

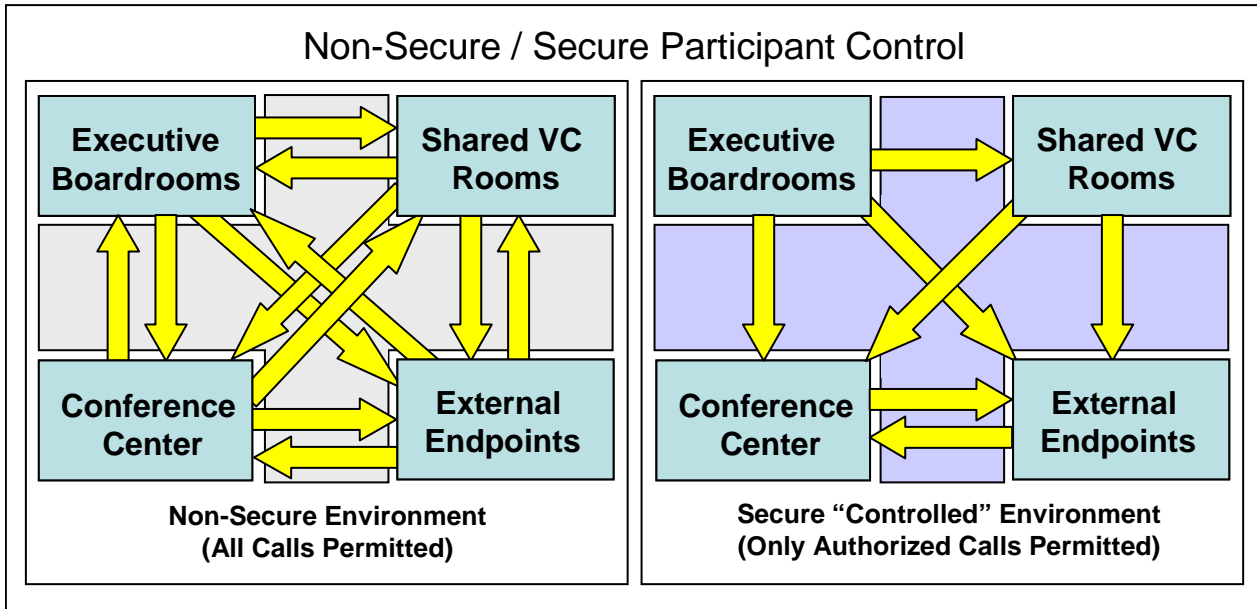


Figure 4: Non-Secure vs. Secure Participant Control

Secure Environment – In a secure environment, enterprise administrators can set policy regarding which systems are able to call which other systems. In this case, a policy could be established that allows only a handful of rooms (those typically used by upper-level executives) to dial into the CEO's Boardroom. Alternatively, policy could dictate that in order to avoid unauthorized connections and eavesdropping, the CEO's Boardroom will not accept any incoming connections.

The graphic below highlights the differences between an uncontrolled and controlled call environment.

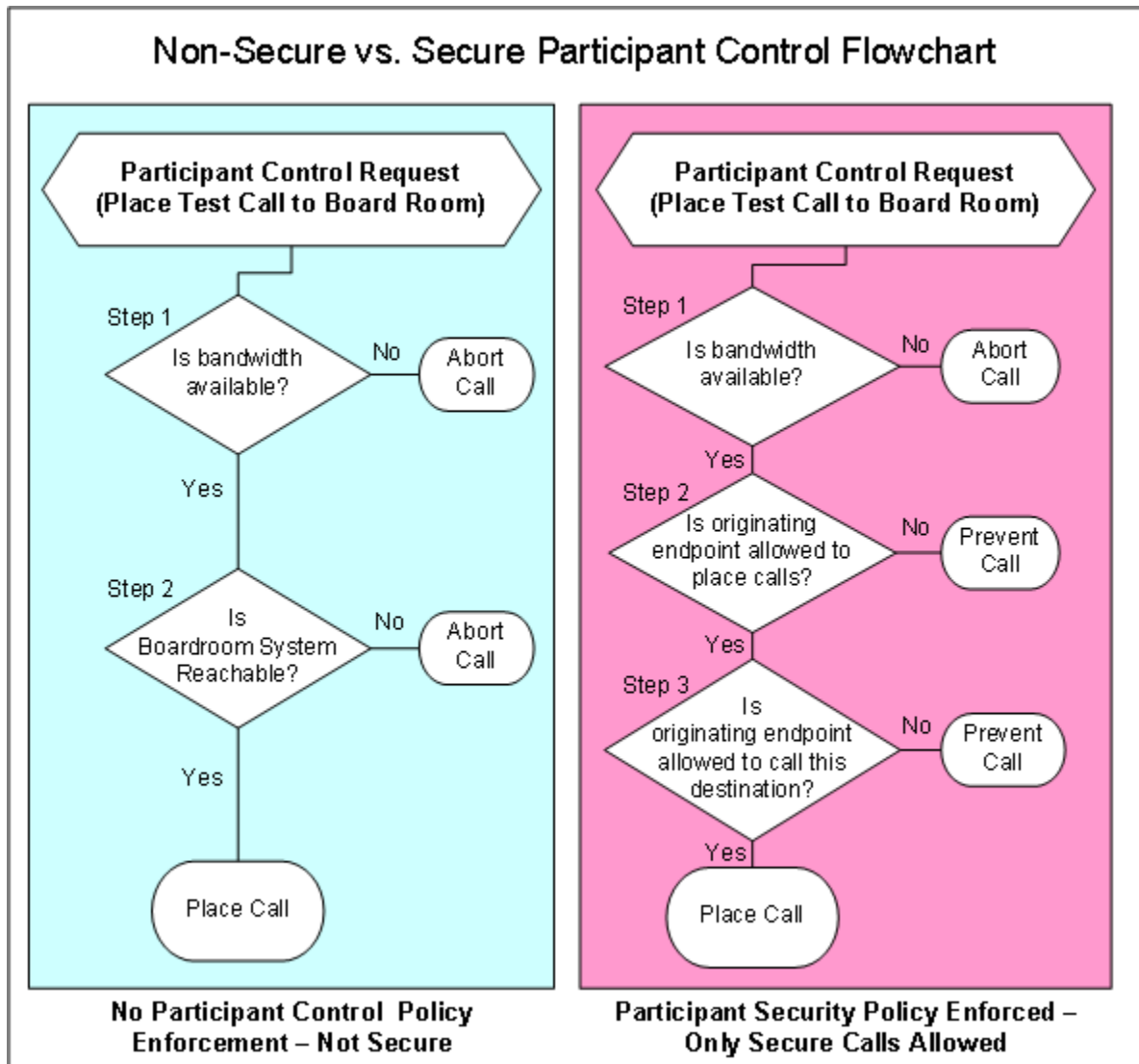


Figure 5: Non-Secure vs. Secure Participant Control Flowchart

As shown above in the uncontrolled environment on the left, assuming bandwidth is available and the systems are reachable (turned on), any system can call any other system. The environment on the right includes both endpoint capability permissioning (i.e. is this endpoint permitted to place any calls?) and access permissioning (i.e. is this endpoint permitted to call this particular endpoint?).

Videoconferencing Security Futures

Wainhouse Research foresees a day when end user authentication, within the meeting room itself, will play a major role in videoconferencing security strategies. Today's security solutions primarily consider the endpoints and devices used within the enterprise. The assumptions are that the meeting participants themselves are authorized to participate in these meetings, and that the locations from which they will attend are known in advance by system administrators and conferencing support staff.

User-based meeting security would require a user to log into the video system in order to participate in the meeting. Depending upon the organizational policies and management systems in place, the call may be connected in advance of the authentication process, but the audio and video signals will not be accessible until authentication is complete.

This concept affords a number of security and functionality benefits including:

- Participant-based identify verification – ensures that only authorized participants are able to participate in video meetings
- Participant-based permissioning – allows administrators to grant users rights and capabilities that apply to video rooms throughout the environment. For example, if an executive logs into a video system on the conference room floor, he gains access to the enterprise ISDN gateway, but if a visiting client logs into the system with a guest password, he can only place calls to a specific list of approved endpoints.
- Free seating capabilities – once a user logs into a video system, the management system can automatically direct this user's meetings to the proper room. This is often called "free seating" or "find-me seating" because the user's permissions and meetings follow him wherever he goes within the environment.
- Enhanced user convenience and confidentiality – once a user logs into a system, the user can immediately access his buddy list, user directory, log of recently dialed numbers, and more. In addition, since directories and call logs are user specific, users are not able to review the call records of prior users.
- Improved resource utilization – the ability to dynamically route calls based on which users have logged into each video system allows organizations to change meeting room assignments simply by directing the user to a different room.

User-based permissioning is already in use throughout most enterprises on an operating system and application level. For example, enterprise Windows users can log into any PC and gain access to their personal network drives and email. Considering the significant security and convenience benefits highlighted above, WR anticipates that user-based permissioning will enter the videoconference room in the near future.

Conclusion

This white paper describes key security concepts that IT, network, and conferencing managers must consider as they deploy and manage videoconferencing over their corporate data network.

In recent years several standards have emerged, including H.235 for user and device authentication and policy, and H.460 for secure firewall traversal, to enable enterprise-grade IT security within videoconferencing environments. Depending upon the vendors and products selected, currently available videoconferencing endpoints and infrastructure devices provide varying degrees of security awareness and support for key security capabilities, such as user-based permissioning end to end encryption, is often lacking. In addition, new IT protocols, such as the IEEE802.1x standard for authentication over wireless LANs, represent new challenges for both IT managers and equipment vendors alike.

For enterprises seeking to securely deploy videoconferencing over their production LAN or WAN, Wainhouse Research recommends the use of standards-compliant videoconferencing devices (endpoints, bridges, gateways, gatekeepers, scheduling and management systems, etc.) from vendors whose core architecture revolves around maintaining data security.

Videoconferencing security does not just happen ... it is the result of proper planning, careful product selection, and adherence to key security concepts.

Although basic security capabilities like password protection offer at least some protection, this is not sufficient in today's business climate where even a small breach of security could cost a firm its competitive edge or impact its ability to meet Sarbanes Oxley requirements³.

Today's videoconferencing environment *is an IT environment*, so conferencing managers and IT managers alike must be familiar with IT security concepts and how they apply to conferencing. As with other areas of IT security, videoconferencing security does not just happen, and should *never* be considered an afterthought. It is the result of proper planning, careful product selection, and a consistent adherence to key security concepts throughout the enterprise.

³ Source: Edward Hurley, SearchSecurity.com News Writer, "[Security and Sarbanes-Oxley](#)"

"Sarbanes-Oxley doesn't mandate specific internal controls such as strong authentication or the use of encryption." It does, however, mandate that CEOs and CFOs confirm that their company maintains strong 'internal controls,' which would certainly include an appropriate level of IP network security.

About Wainhouse Research

Wainhouse Research (<http://www.wainhouse.com>) is an independent market research firm that focuses on critical issues in rich media communications, videoconferencing, teleconferencing, and streaming media. The company conducts multi-client and custom research studies, consults with end users on key implementation issues, publishes white papers and market statistics, and delivers public and private seminars as well as speaker presentations at industry group meetings. Wainhouse Research publishes Conferencing Markets & Strategies, a three-volume study that details the current market trends and major vendor strategies in the multimedia networking infrastructure, endpoints, and services markets, as well as a variety of segment reports, the free newsletter, The Wainhouse Research Bulletin, and the PLATINUM (www.wrplatinum.com) content website.

About the Author

Ira M. Weinstein is a Senior Analyst and Consultant at Wainhouse Research, and a 14-year veteran of the conferencing, collaboration and audio-visual industries. Prior to joining Wainhouse Research, Ira was the VP of Marketing and Business Development at IVCi, managed a technology consulting company, and ran the global conferencing department for a Fortune 50 investment bank. Ira's current focus includes IP video conferencing, network service providers, global management systems, scheduling and automation platforms, ROI and technology justification programs, and audio-visual integration. Mr. Weinstein holds a B.S. in Engineering from Lehigh University and is currently pursuing an MBA in Management and Marketing. He can be reached at jweinstein@wainhouse.com.

About TANDBERG

TANDBERG is a leading global provider of visual communication products and services. The Company has dual headquarters in New York and Oslo, Norway. TANDBERG designs, develops and markets systems and software for video, voice and data. The Company provides sales, support and value-added services in more than 90 countries worldwide. TANDBERG is publicly traded on the Oslo Stock Exchange under the ticker TAA.OL. Please visit www.tandberg.net for more information.