# TANDBERG and Security

TANDBERG

D50172, Rev 3.1

# Table of Contents

# 1. Introduction

This document is intended to be used as a resource for video conferencing security in general, as well as how TANDBERG addresses security specifically. There are many aspects of video conferencing that must be identified and addressed, so that participants may confidently use video as a communication tool when sensitive information is involved. Also, there are several degrees of security, which need to be understood, so that the correct methods are implemented for each environment.

# 2. Audience

This document was written for public distribution. Please distribute accordingly.

# 3. Installation Recommendations

The following section addresses some of the basics of installing video conferencing units into common network environments.

## 3.1 ISDN Only Rollout

ISDN video conferencing is a fairly secure environment by nature, in comparison with the IP world. Intercepting an ISDN video call is very challenging. A hacker would first need access to at least one of the ISDN switches while it is trafficking the call. Secondly, the hacker would need to deal with the challenges of multiple B-channels and the chance that the channels travel through multiple switches. Once all of the B-channels have been identified, they would need to be bonded together to make sense of the proceeding call.

In the unlikely event that the above scenario is possible, the best protection is to encrypt the call. Refer to section 4 of this document for more details regarding encryption and the several levels of security it can offer.

## 3.2 IP Only Rollout

Using video over IP can be a security problem, but if the correct steps are taken, H.323 video conferencing can be a very secure environment.

The first concern is to allow the video equipment to function correctly on the given IP network without compromising the existing devices on the network. In most corporate LANs there is already an existing firewall which will need to be adjusted to accommodate the video systems. There are several firewall solutions available and are discussed in section 5.

The second concern is protecting the equipment from unauthorized users and malicious attacks from internal and external users. Section 7 has more details about disabling management services and applying passwords for access.

## 3.3 Mixed ISDN/IP Rollout

The above two sections will obviously apply. In addition refer to section 6 regarding any concerns about LAN intrusion from the ISDN world.

# 4. Encryption

## 4.1 What is Encryption?

The goal of encryption is to allow the passing of data without interception as well as preventing impersonation. Encryption has been implemented historically by transposing or replacing text characters in order to send information that was unreadable unless the decoding "key" was known. With the advent of the modern computer, encryption and cryptography have become much more complex, and as a result, very secure.

## 4.2 Methods Currently Used Today in Video Conferencing

### 4.2.1 DES

Adopted by the National Institute of Standards and Technology (NIST) in 1972, the **D**ata **E**ncryption **S**tandard is a symmetric block cipher encryption method using a 56-bit key. It was developed for use as a government standard for non-classified data until 1997. It is still used today in many applications, but NIST required a new standard that would withstand the power and speed of today's computers when used as brute force attacks[1].

### 4.2.2 AES

The **A**dvanced **E**ncryption **St**andard was adopted in May of 2002 as an official government standard. It is also a block cipher encryption like DES but is many orders of magnitude more secure. Compared to DES; if a brute force attack[1] was able to crack a single 56-bit DES key in 1 second, the same technology would take 149 trillion years to crack a single 128-bit AES key. AES is able to be implemented with a 128, 192, or 256-bit key.

### 4.2.3 Triple-DES (DES3)

This is a minor modification of the DES standard which is three times slower but billions of times as secure. Using the same comparison as in the above section; if an attack could crack a single 56-bit DES key in 1 second, the same attack would take 4.6 billion years to crack a 168-bit triple-DES key. It's not quite as secure or portable as AES, but it provides an excellent solution for some applications. Triple-DES is also an approved standard.

### 4.2.4 Custom

There are many custom boxes that provide different levels of encryption and are often used in military applications. These can be very expensive and some are even illegal to be owned by civilians. Some examples are the KIV7 and KG194.

[1] A brute force attack is a semi-automated attempt to crack a code by using computers simultaneously, and repeatedly to "guess" codes or passwords.

## 4.3 How Does TANDBERG Use Encryption?

### 4.3.1 Overview

TANDBERG supports 128bit AES and 56bit DES encryption in the entire product line as an embedded feature. These two methods of encryption may be used in H.320 and H.323 environments simultaneously. A mix of AES and DES is also permitted if configured to do so.

### 4.3.2 Certification

TANDBERG's encryption has been tested by a National Institute of Standards and Technology (NIST) approved laboratory and validated as conforming to the Data Encryption Standard (DES) as specified in Federal Information Processing Standard Publication 46-3, Data Encryption Standard (DES) and as specified in Federal Processing Standard Publication 197, Advanced Encryption Standard (AES).

For a listing of TANDBERG’s certificates, please see:

DES Certificate: http://csrc.nist.gov/cryptval/des/desval.html
AES Certificate: http://csrc.nist.gov/cryptval/aes/aesval.html

### 4.3.3 Key Exchange

TANDBERG implements the Diffie Hellman method for encrypted key exchange. Below is a generalized example of how this key exchange takes place.

To generate a key, Joe selects a public generator (3 in this example), a public prime modulus (10001 hexadecimal), and a secret exponent (9A2E hex). Joe then calculates the following:

```
joe% dh 3 9A2E 10001
C366
```

This is his public key. Joe sends these three numbers (3,10001,C366) to Alice.

To encrypt a message to Joe, Alice picks a secret random number (4C20 in this example) and using Joe's generator and modulus, calculates:

```
alice% dh 3 4C20 10001
6246
```

She sends this result to Joe. Alice then takes Joe's public key and her secret random number and calculates:

```
alice% dh C366 4C20 10001
DED4
```

She uses this result as a session key to encrypt her message to Joe.

To decrypt the message, Joe uses the number Alice sent him, and his secret key to calculate:

```
joe% dh 6246 9A2E 10001
DED4
```

Joe now has the session key and can decrypt Alice's message.

An eavesdropper sees Joe send Alice three numbers (3,10001,C366), and sees Alice send Joe '6246'. But the eavesdropper can not use these numbers to calculate the secret session key (DED4), and thus can not decrypt the message.

# 5. Firewalls

Firewalls are an integral part of securing a corporate LAN, so in most real-world scenarios, they cannot be avoided when implementing H.323 video conferencing. This next section will outline some of the challenges brought about by firewalls, and discuss how to work through the issues.

## 5.1 Categorizing Firewalls

There are three major types of firewalls implementations. Some firewalls have attributes of more than one of these categories, but for the sake of generalization, these three will be discussed independently of each other.

### 5.1.1 Type 1 – Packet Filtering

This is probably the most common variety of firewall. The packet filtering model gains information from the IP header of each packet and makes its filtering decisions based off of that information. Since H.323 dynamically allocates ports the only sure way to allow packets to pass freely is to open all TCP and UDP ports above 1024.

Since this type of Firewall is so common, TANDBERG has restricted the range of ports in which it uses for H.323. This allows for smaller holes in the firewall, and then becomes a more acceptable solution. At a minimum the TANDBERG will require a packet filtering firewall to allow TCP ports 1720, 2326-2373 and UDP ports 5555-55XX (see section 7 for more details on TANDBERG’s port usage).

### 5.1.2 Type 2 – Connection Gateways

Also known as a circuit gateway, it is very similar to a packet filtering gateway, but it allows for some dynamic port opening based on limited application level knowledge. This limited knowledge is often referred to as being H.323 aware. This is a better solution than a packet filtering firewall, but it is not without its own challenges.

The connection gateway must disassemble the control packets to understand which UDP ports to open dynamically. So in short, the firewall must disassemble the control packets, interpret them correctly, and implement the port openings as needed. This is not as easy as it sounds, and can lead to interoperability issues. For instance; a firewall supports only H.323 version 1 and 2, but the endpoint uses H.323 version 3.

### 5.1.3 Type 3 – Application Proxies

Unlike the other two examples of firewalls, a proxy is visible to the applications. The codec acts like a client and treats the proxy as a server; on the other side of the network the proxy appears as the client and the remote location appears as the server.

Because of the nature of this client-server relationship, there inevitably is some address translation that must take place. Because of this close relationship with the actual application, it is possible that a proxy would use portions of the H.323 stack to maintain both sides of the network connections.

Since this relationship requires that the endpoint calls the proxy (not the callee), the codec must make use of other H.323 fields to relay the callee's information so that the proxy knows where to forward the call. This being the case, the endpoint must be proxy aware in some capacity. In the video conferencing world, gatekeepers are used to relieve the endpoints from being proxy aware.

## 5.2 NAT

A Network Address Translation (NAT) device is often used in conjunction with (or is already an imbedded part of) the above types of firewalls. The NAT gives the ability to use a range of private IP addresses internally, while sharing a single or small pool of public IP addresses. In effect internal users can see the public internet, but the public internet cannot see the individual devices on the private side of the NAT.

This is a very common implementation, and can cause a problem with H.323. The NAT adjusts the IP headers of the packets traversing the firewall but does not change any of the information in the payload of the packets. In H.323, IP information also resides in the payload of some of the packets. As a result a device outside of the NAT may try to send information to a private IP address from the public world where it is an invalid address. To resolve this, the endpoint must know about the NAT and make provisions for it. TANDBERG has included a NAT feature which a user can make the endpoint aware that there is a NAT in the network by entering the "public" IP address into a field in the codec menu. This adjustment causes the codec to alter the payload of each packet to reflect the public return address of the NAT.

## 5.3 DMZ

A Demilitarized Zone is another segment of a LAN that has a general set of rules associated with it that allow less restrictions to the outside world, while retaining full functionality to the private segments. This segment also lies behind the firewall and is often used for mail and web servers that require public access. It can be a good solution for video systems as well, provided that the access is set correctly. It can offer the benefit of a protected environment while still retaining a public IP addressing scheme while at the same time allowing for management from the private segments exclusively.

# 6. ISDN and IP

TANDBERG video conferencing systems are capable of using ISDN and IP networks simultaneously. With this in mind, there is concern regarding the feasibility of malicious acts to a user's IP network via the ISDN interface of the TANDBERG codec. Addressed in the next few sub-sections are explanations of how this type of malicious activity is not possible.

## 6.1 Using Codec as a Modem

The possibility of using a TANDBERG codec as an ISDN modem to gain access to a LAN is impossible. To achieve this goal, the codec software would need to have been written to support an access protocol such as PPP or SLIP. The TANDBERG ISDN interfaces are designed to use H.320 only.

## 6.2 Remote Controlling Codec

The TANDBERG codec does not support any control features to be given to a remotely connected codec, thereby allowing a remote user to manipulate a local codec to commit malicious acts. To allow this type of use, the codec software would need to have been written explicitly to use an inband data channel. TANDBERG has not implemented this type of data channel.

## 6.3 Identity Masking

The concern with identity masking is that a trusted user could use a TANDBERG codec to conduct malicious acts which would appear to originate from the codec. TANDBERG codecs do not support outbound telnet or FTP sessions, so using a codec as a mask or an outbound point of attack is therefore impossible.

# 7. TANDBERG Specific Features / Implementations

The following section details specifically the methods in which TANDBERG addresses certain security issues.

## 7.1 Ports Usage

The following TCP and UDP ports are relevant for TANDBERG systems.

| Port Number | Service | Protocol |
|---|---|---|
| 21 | FTP/control | *TCP |
| 23 | Telnet | *TCP |
| 80 | HTTPd | *TCP |
| 123 | NTP | *UDP (Codec Only) |
| 161 | SNMP/queries | *UDP |
| 162 | SNMP/traps | UDP |
| 443 | HTTPs | TCP |
| 963 | Netlog | TCP |
| 970 | Streaming/RTP | UDP |
| 971 | Streaming/RTP | UDP |
| 972 | Streaming/RTP | UDP |
| 973 | Streaming/RTP | UDP |
| 1026 | FTP/data | TCP |
| 1027 | VNC | TCP |
| 1719 | H323/RAS | UDP |
| 1720 | H323/Q931 | *TCP |
| 2326-2373 (2837)** | H323/RTP | UDP |
| 5555-55xx (5587)** | H323/H.245/Q.931 | TCP |

The first outgoing call uses 5555 for outgoing Q.931 and 5556 for H.245, next uses 5557 for Q.931 and 5558 for H.245, etc. Each incoming H.323 call uses the next available port for H.245. Disconnecting a site in a call will not free up available 55XX ports until the whole conference is down.

(** Listening Sockets*)

(** Values in parenthesis indicate additional ports needed for TANBDERG MCU)

## 7.2 Disabling Management Services

The entire TANDBERG product line is equipped with the ability to disable IP management services as well as H.323 video. Please keep in mind that if the telnet service is disabled, you will need to connect to the codec locally (data port 1) to enable these features again. The following chart outlines the proper terminal commands for disabling each service.

| | |
|---|---|
| Telnet | services telnet <disable/enable> |
| FTP | services ftp <disable/enable> |
| HTTP | services http <disable/enable> |
| H.323 | services h323 <disable/enable> |
| rinfo command set | services remote-parameter <disable/enable> |
| Remote Software Upgrades | services remote-software <disable/enable> |

There are also terminal commands to restrict the SNMP traffic to and from the TANDBERG codecs. Remember, if the SNMP service is disabled, there will be only limited functionality if TMS is also being used.

| | |
|---|---|
| Disable SNP | services SNMP disable |
| Enable SNMP | services SNMP enable |
| Restrict SNMP to read only | services SNMP read-only |

Note: *These commands take effect only after a reboot.*

## 7.3 Security Regarding Wireless Usage

TANDBERG has included a PCMCIA slot in select models to allow for a wireless Ethernet solution. In addition to using 802.11b, TANDBERG has included support for WEP (Wired Equivalent Privacy) with a choice of 64-bit, 128-bit or no encryption.

The Following TANDBERG models support wireless Ethernet connections (802.11b).

TANDBERG 550
TANDBERG 880
TANDBERG 1000

The following is a list of recommended wireless PCMCIA cards.

- Cisco Aironet 350 Wireless LAN adapter (AIR-PCM 352)
- Compaq WL110 11Mbps Wireless LAN
- Lucent Orinoco PC24E-H-(ET/FC/FR/JP) 11Mbps
- Enterasys Networks RoamAbout 802.11 DS High Rate (P/N: CSIBD-AA-128)
- Melco Buffalo WLI-PCM-L11G

### 7.3.1 Managed

A managed wireless connection requires the use of an access point. This connection uses an SSID (Service Set Identification) code, which acts as the network name or ID that the system will operate on. This SSID is alphanumeric and case sensitive, and the codecs will not work if this SSID does not match the entry in the access point.

Even though a system will not work without the correct SSID it is recommended to make use of the MAC address filtering functionality of most access points. This will ensure that ONLY approved wireless systems are permitted on the network.

### 7.3.2 Adhoc

This is also known as a peer-to-peer connection. This can be used to establish a call between two systems when there is no access point. Since there is no access point, there is no SSID relationship and the only security offered for this type of connection is the automatic DES encryption over H.323 that the TANDBERG offers.

## 7.4 Passwords

The entire TANDBERG product line supports password protection on the IP network.

To set the password which blocks telnet, HTTP, and FTP use, enter the dataport command:

*ippassword <password>*

The dataport command for protect mode is:

*protect on <password>*

To password protect the streaming functionality of the codec enter:

*streaming password <password>*

With the exception of the protect mode password, these passwords can also be entered from the codec webpage.

## 7.5 Protected Mode

Protect mode is a dataport command that protects certain configuration portions of the Menu from being edited. The protected menus are:

*Network* menu, and all submenus
*LAN* menu, and all submenus
*Call Settings* menu, and all submenus

This prevents unauthorized users from making configuration changes in the menu.

This command can also be password protected to avoid a user from turning protect mode off. See the above section for usage.

## 7.6 Access Codes

TANDBERG codecs have an access code feature which prompts the user for an alphanumeric password each time the user attempts to dial out. This access code can be used for accounting purposes but can also be used as a security feature to restrict unauthorized users from operating the system.

It is recommended that “Protected Mode” is turned on so that users cannot disable the access code feature from the user menu.

## 7.7 HTTPS

The TANDBERG MCU has provisions for HTTPS to allow web control to be more secure.

HTTPS (Secure Hypertext Transfer Protocol) is similar to HTTP but is transmitted over Secure Sockets Layer (SSL). SSL is a method of sending packets as encrypted data.

## 7.8 HTTP Digest

The TANDBERG product line uses HTTP Digest to protect the webpage password login. HTTP Digest is a standard method of indirectly transmitting the login password without using “clear text”.

HTTP Digest Authentication allows the client (your PC) to prove to the server (Endpoint/MCU in this case) that it knows the correct password without having to send the password itself to the server. The client does an irreversible computation, using the password and a random value supplied by the server as input values. The result is transmitted to the server who does the same computation and authenticates the client if he arrives at the same value. Since the computation is irreversible, an eavesdropper can't obtain the password.

## 7.9 NTLM Authentication Scheme for HTTP

NTLM is used by TMS to authenticate users as they log in to TMS.

NTLM stands for NT Lan Manager; it is sometimes referred to as NTCR (NT Challenge/Response.) Similar to HTTP Digest, NTLM does not actually transmit any passwords, but rather communicates to the server that it "knows" the password through a "Challenge/Response" process as follows:

1. Client makes HTTP request.
2. Server sends "401 Access Denied", presents NTLM as authentication method
3. Client requests again
4. Server sends "401 Access Denied" again, with a random value (the Challenge)
5. Client generates a Hash [1] value based on the random number and the password (the Response)
6. Server sends the User Name, the Hash [1] and the random value to the Domain Controller
7. If the Domain Controller computes the same value based on the stored Hash [1], the Domain Controller authenticates the user.
8. Page appears in browser

Through this process the password acts as a Private Key and the random value acts as a constantly changing Public Key.

[1] A Hash is a 128bit value generated form the password by the Internet Standard MD4 Hashing Algorithm. It is theoretically impossible to use this algorithm and the Hash in a reverse process to retrieve the password. Domain Controllers may store Hash values rather than clear text passwords.

## 7.10 SNMP "Incorrect Password" Trap

TANDBERG codecs provide an SNMP trap which TMS uses to warn administrators that someone has entered an incorrect password during an attempt to login to the codec. The trap sends details on the type of network the attempt was made (HTTP, Telnet, or FTP) and also shows the IP address of the user attempting the login.