Improving Usability by Adding Security to Video Conferencing Systems

April Slayden Mitchell, Alan H. Karp
HP Laboratories Palo Alto
HPL-2006-26(R.1)
January 10, 2007*

security, user interface design, usability

Business travel is at an all-time high despite the plethora of video conferencing applications available in the world today. One major drawback in many of these applications is a confusing interface which may require a large amount of setup time and training. The second major drawback is lack of security which can lead to less use of the system due to lack of trust regarding private interactions. In this paper, we propose the "One Space" video conferencing user interface. Through the One Space interface, all persons in every connected room have the same view of and control over the user interface. The view is spatial in orientation, contains no nested menus, and information which is private cannot be accessed by those who lack permission. All icons are pictorial and represent common objects found in and around the room. A One Space interface overcomes many of the drawbacks of current video conferencing applications. Utilizing the One Space guidelines when designing video conferencing interfaces will provide more visible security assurances and support repetitive use, all while enabling even a novice to use the system to its fullest extent.

* Internal Accession Date Only
An abstract of this paper to be published in the proceedings of Usable Security 2007 (USEC'07), a workshop organized in cooperation with the International Financial Cryptography Association
http://www.springer.de/comp/lncs/index.html.

Approved for External Publication

Improving Usability by Adding Security to Video Conferencing Systems

April Slayden Mitchell, Alan H. Karp

Hewlett-Packard Laboratories. 1501 Page Mill Rd, Palo Alto, California, USA
{april.mitchell, alan.karp}@hp.com

Abstract. Many video conferencing solutions exist in the market today and many new ones are being introduced. In striving to provide an experience to users as close to "being there" as possible, two major design issues must be considered: security and ease of use. In this paper, we describe a method for designing a "One Space" video conferencing user interface that reveals security information to the users while reducing the complexity of the user experience. [1]

Keywords: Usability, Security, User Interface Design

1 Introduction

Given the global economy, and the number of geographically dispersed offices of many large companies, the need to travel is still at an all-time high. The plan to use video conferencing as a means of reducing the frequency of such trips and bringing down travel costs is by no means a new concept. There are currently a plethora of desktop video conferencing applications and video conferencing equipment available in the market. However, no single solution has accomplished the task of providing such a successful alternative that it is "as good as being there". Why is this so?

Several reasons are apparent to many consumers, and we'll focus on two of the main ones here. The first drawback is a confusing interface that makes many conferencing applications too complicated to use. Some systems require massive amounts of time to setup. Other systems require an engineer to figure out how to run them once they are set up. Training before use is often needed, and last-minute meetings are commonly held over the phone due to difficulty and unreliability of the setup process. If there is no guarantee of a successful connection every time, why bother?

Another issue is security. Private discussions between CEOs and customers or internal strategy planning sessions cannot be shared via the public internet for fear of leaks and vulnerability. Encrypting the transmission can protect this information, but providing confidentiality to the users of the systems remains crucial. Many systems do not present via the video transmission complete revelation of who is in attendance

[1] The ideas contain herein are not details of any video conferencing product by HP or any other company. They are proposals for designing a more secure video conferencing interface.

due to off-camera "watchers" and over the phone "listeners". Often in these cases, the rewards of the personal connection and enhanced confidentiality of a face-to-face meeting outweigh the costs involved in flying a large group to another continent for a meeting of top executives. In this paper, we outline some key concerns by current video conferencing system users, and we describe a solution for designing a video conferencing user interface which is both secure and easy to use.

2 Motivation

Recently, two Fortune 100 companies announced new video conferencing solutions. Both HP's Halo[2] and Cisco's TelePresence[3] offer integrated video and audio room solutions for remote collaboration. In comprehensive solutions such as these, it is important that users are able to operate comfortably while in the room and are able to make the same assumptions about security as they are in a standard conference room.

In order to get to the root of security concerns, we conducted an interview study of users of video conferencing solutions. Table 1 shows a typical list of user questions and their associations with key security concerns. In regards to the security of video conferences, users had many questions such as "Who is listening to my conversation", and "How can I tell who is connected over the phone?" *etc*. The majority of the questions brought up by video conferencing solution users centered on privacy. It was apparent that with the introduction of cameras and microphones into a space, the "assumption" of private communication is no longer valid. We took privacy strongly into consideration in developing our model for a secure video conferencing solution interface. The theme of our solution can be summarized by the term "Revelation", revealing the presence of "watchers" and "listeners" as well as making any action taken visible to all participants.

Table 1. Eleven Meanings of Security.

Security Concern	User Question
Authentication	Who am I talking to?
Authorization	What should I be able to do?
Audit	Who did that?
Access control	Should this request be honored?
Non-repudiation	Can I pretend I never said that?
Confidentiality	Can others see what I'm seeing?
Integrity	Can this data be changed?
Privacy	Can others see that I'm seeing it?
Anonymity	Can others find out who I am?
Denial of service	Can I be assured of access?
Physical security	Who can touch it?

[2] HP Halo: http://www.hp.com/halo/index.html
[3] Cisco Telepresence:
http://www.cisco.com/en/US/netsol/ns669/networking_solutions_solution_segment_home.html

Also at the center of the complexity and confusion for users of standard video conferencing applications and conferencing equipment is the user interface. Too often the interface consists of menus within menus. While this pattern is familiar from desktop computing, it is nevertheless confusing for occasional users, leading them to ask questions such as: "Which menu do I look in to find the phone?" and "Where's the option for sharing my display?" The nested menu metaphor can also be detrimental to security. Without extensive customization, users are often presented with many options that the security policy prevents them from using, thus revealing protected information and introducing confusion (see principle of expected ability in [2]). In order for a video conferencing application to be a success, the user interface must be understandable by a novice, warrant repetitive use, and reveal the aspects of security relevant to the participants.

3 The "One Space" Metaphor

In this paper, we describe an interface to a video conferencing system that achieves each of these goals. A video conferencing system consists of one or more physical locations (rooms containing the video conferencing equipment) connected over a network. In a "One Space" video conferencing system, both the interface and room design encourage people to act as if the physical room is a single location in which all participants are present. All rooms consist of the same equipment and physical layout, including a center table, chairs, lighting, and color scheme. The rooms are not customized based on company or location, thus adding to the illusion of a shared environment.

3.1 User Interface Design

In addition to various microphones and speakers, each room contains video display screens for showing other attendees and an additional display for showing the shared interface (see Figure 1 for an example from HP Halo). When two or more rooms are connected, the shared interface appears in each room. This display contains means for controlling all of the physical devices available in each room, including the cameras, PCs, etc. This shared display is considered an extension of the table desktop and is visible to all attendees in every room. Each room contains a device for controlling the interface (such as a mouse), thus enabling not only shared viewing but also shared control by all parties.

The One Space interface, which is visible on the shared display in each room, shows a schematic representation of the space including the tables/chairs/doors in both rooms as well as other physical devices, such as cameras and PCs that are available for use. The interface also reveals virtual devices which are available such as phone lines and access to help features. Dial-in participants can access this view via a web browser. This interface uniquely uses a spatial metaphor to connect disjoint but real physical locations as opposed to other interfaces which use spatial modeling to represent a shared virtual space.

Fig. 1. Video conferencing room layout for HP Halo.

In the One Space metaphor, it is very important that all rooms always view the same user interface. Attendees in any room can control the interface by using a device such as a mouse, which allows full control of the interface and its actions are visible to everyone, regardless of room. The spatial view of the One Space interface, in which all equipment, devices, *etc*. are represented as icons, removes the need for traditional nested menus, thus preventing the common user error of selecting the wrong menu when trying to perform some task. All icons are pictorial and represent common objects such as a table, a phone, or a camera. Mouse tips can provide alternative denotations. The shared control of the space is an essential element in making the interface more secure and easier to use because there are no hidden actions by any connected parties, and there is no need to worry about the learning curve due to using a room in a different location.

3.2 Human Assistance

Help is provided by a human contact person(s), who is available 24-hours a day. The help-assistant is represented on the user interface by a representation of an unoccupied desk with a bell. When the user clicks in this area (which is always viewable on the interface) a bell will ring in all rooms and the phone connection to the help-assistant will be initiated. The icon representing the help-assistant's presence in the room will change to show the desk as occupied once the help-assistant has answered the phone call. Once the attendee's have finished communicating with the help-assistant, the help-assistant will end the call. Once the audio connection has been terminated, the icon of the help-assistant's desk icon will change back to show it as unoccupied, giving all attendees a visual indication that the call has ended.

3.3 Security Revealed

In any application which consists of transmitting audio or video between multiple locations, security will be an issue. Some high-end conference rooms use private networks to guarantee the video link meets strict latency guarantees. A side benefit of

the use of a private network is that it eliminates many of the most immediate security concerns in that it is much more difficult for an external malicious attacker to do traffic analysis or disrupt communications. But, private networks do not protect against internal threats such as eavesdropping or watching a video connection from another room on the network. While adding encryption for internal communication is an option, answers to questions such as: "Who is on the phone?", "Is there a meeting help-assistant and is he/she listening?", "Is the door to the room open?", and "Are there people in the room who are off-camera?" must be readily apparent to all attendees at all times during the conference.

Our One Space user interface reveals these security features to all attendees. In our video conferencing system, there is no way through the interface to connect to and "listen in" to a conference uninvited or unannounced. All video links must be explicitly accepted or declined. All attendees who dial in to a conference line are represented by a uniquely identified icon and mouse tip on the user interface. Similarly, the audio connection with the help-assistant is always represented on the user interface by a representation of an occupied or unoccupied desk, thus allowing the attendees to know when the connection with the help-assistant is active. The lack of physical customization of the rooms enhances security since people will rely on who they see in the video display instead of easily spoofed differences among rooms such as flowers on a table or pictures on the wall.

3.4 Room Reservations

While operating over a private network protects the data being transmitted from external threats, it is still important to also protect the knowledge of room usage and connections. For example, internal knowledge that the video conferencing rooms of two CEO's are being used frequently to connect with one another may be interpreted as evidence of an upcoming merger. This information, while independent of the actual video and audio data being transmitted during these meetings, should also be kept private. Therefore, access to the scheduling system is controlled by personal login. Each person's permissions are tied to the login session. Room owners can designate which people or groups of people can access the calendar of their room for booking, thus eliminating the possibility of an un-trusted source gaining access to a room's calendar or booking that room for a meeting. This feature is particularly important for competing companies, which may both have rooms operating on the same network. By allowing these permissions to be configured and reconfigured, group policy declaration becomes easier and removes the need for a central administrator to maintain multiple permission policies. Scheduling control also improves usability. Since users only see rooms that they are allowed to reserve, there is no chance of limited access due to security contributing to confusion about why a reservation attempt is failing.

The convenience of personalized booking also lets meeting organizers configure the connected room for their events. They can pre-set wired/wireless LAN connections for access to their company's local network or the public internet at the time of booking. Similarly, they can designate a conference line to be initiated for tracking remote attendees who may join during the meeting. They may also configure

the amount of information about their meeting that can be seen publicly, thus protecting any information they do not want to share. Physical security can also be tied to the room booking. For example, the door can be unlocked by the ID badge of the person designated in the reservation or by a lock combination assigned per individual per meeting. Invitees can delegate others to attend the room meeting in their stead by giving them this number, yet the responsible party can be identified by which code was used. The same concept applies to those phoning in from other locations. Each invitee is given a per person, per event code number. This code makes it possible for all attendees in the meeting to know who the responsible party is even when a delegate is attending instead.

4 Implementation

Here, we describe one instantiation of a secure user interface designed using the "One Space" user interface guidelines as shown in Figure 2. We'll use the numbered callouts in the figure to guide our description. The numbered callouts in the figure do not appear on the actual interface; they appear only to facilitate the description.

4.1 Revelation Icons

All video conference rooms which are currently connected will be represented on the One Space user interface. Figure 2 represents a 2-room event in which two rooms are connected; however, the table as indicated by callout 1 can be expanded to show a 3 or more room event, or reduced to show only one side of the table when the room is being used locally. As shown in callout 6, the location and company information for each room is displayed on the interface. The name of the room (or other public information about the location) appearing on the interface can be configured during booking as well as the attendee list, the telephone number for a conference line to dial at start-up, and the preference for whether wired LAN access is internal or external. If there are wired/wireless LAN connections and/or phone connections in either room then their existence and activity are viewable via the user interface. For example, in Figure 2 three laptops (callout 10) are shown, which represents that three devices have been connected (perhaps to the local LAN) within the room.

In callout 2, remote attendees who are not physically located in one of the rooms (in this case, those who are dialed in over the phone) are recognized on the user interface. This information is tracked through a per-meeting/per-person pass code which each invited member receives. An invitee can delegate this code to another person to attend on their behalf.

In callout 3, a remote delegate is identified by name as well as the responsible party's name according to the distinct pin number the remote caller used to join the meeting. Callers enter their names via keypad or using speech recognition software. Each name is compared with the name of the responsible party. If the name is different from the name associated with the pin used, the system recognizes that this person is a delegate of the responsible party and lists the joining party's name as well as the term delegated and the responsible party's name.

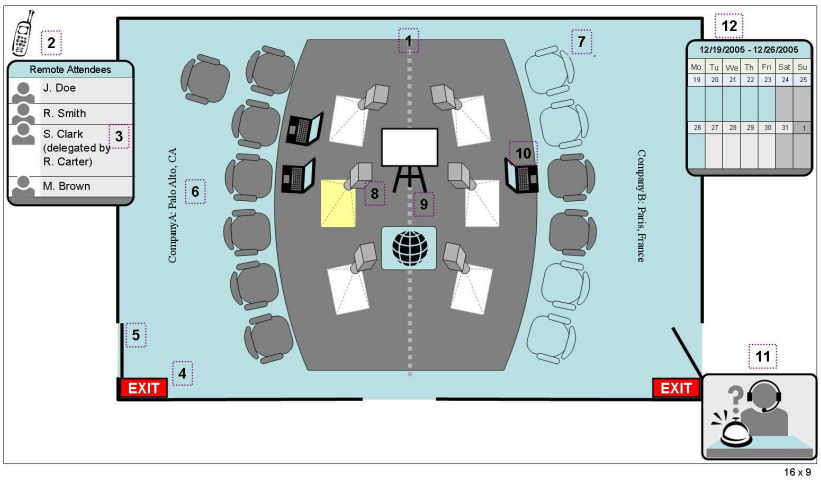

Fig. 2. Example of One Space user interface for a video conference connection between two physical locations with remote participants dialed in via a conference line.

Every physical seat in each room should be represented on the user interface by a chair icon. Each chair icon should be colored based on whether or not the seat is actually occupied, which is important when not all seats are viewable on camera. Additionally, on-camera seats should be colored (or highlighted) as well to distinguish them from off-camera seats. If the chair icons are gray, then they are occupied. If they are outlined with a solid black line, then they are on camera. If they are outlined in a dashed black line, then they are off camera (see callout 7 for an off-camera, unoccupied seat). This detection can be done by weight sensors placed on the chair to determine occupancy as well as by camera tracking tools which could identify extra chairs brought into the room as well as extra people standing off-camera [1].

In addition to seats in the room, an icon representing the door to the room will also appear on the user interface, as shown in callout 5. This icon indicates whether or not the actual physical door is open or closed in order to reveal if persons located outside of the room can easily hear or see participants in the video conference.

4.2 Interaction Icons

In addition to icons on the user interface which reveal attendance and connection information, etc., there are other icons which allow users in either room to control conference actions. For example, callout 4 indicates an Exit sign. When an attendee in either room clicks on the exit sign, the room associated with that sign can choose to leave the conference. The attendee will be asked if they definitely want to leave, and if they click yes they will exit the event. All other rooms will still stay connected in the current event and the table arrangement will adjust to reflect that one room has left the event.

Several icons representing overhead cameras are shown on the user interface. The interface also reveals the area on the table that will be illuminated if it a particular camera is activated. Video conference rooms may have zero, one, or more cameras or other similar physical devices and each should be revealed and be controllable via the user interface. Once a camera or device is activated, the icon should change to reflect that it is in an active state. In this case, the area on one table as denoted in callout 8 is shaded a different color to reflect the portion of the table that is on camera .

Icons that appear in the center of the table (as denoted by callout 9) represent virtual devices which can be accessed. These include a shared web browser or whiteboard.

The icon denoted by callout 11 represents the help desk. It should only show the desk as occupied when the help-assistant is online (connected to the video conference via audio, video or both) and can interact with the meeting attendees. When the help help-assistant is not connected, the icon should appear as an unoccupied desk with a bell. Any user may click on the bell to contact the help-assistant.

A calendar, as indicated by callout 12, should be accessible when in a video conference. This calendar shows the availability of all rooms currently connected. Through this interface, attendees are able to schedule a follow-up event with the same rooms and the same attendees, but not access any other room's calendars or change the attendee list.

5 Best Practices

The following implementations should be considered best practices when designing secure collaborative environments. Once a meeting is successfully scheduled and before the connection can be made between any rooms, all rooms must first agree to begin that connection. This eliminates the possibility of "peeking" in on rooms uninvited or surprising others when they are not expecting it. Similarly, video should always be connected shortly before or at the same time as the audio. This eliminates the ability to "eavesdrop" on conversations by listening to one side before they can see you. All attendees in each room are represented by an occupied chair on the user interface, even in the case where there are off-camera attendees, which may happen in situations when more than two rooms connect, so their presence is still known by all attendees. Any changes in meeting involvement, such as the help-assistant joining/leaving or a remote attendee dialing in/hanging up, are represented by a graphical change on the interface which is accompanied by a unique sound. This practice of dual audio/video alerts is important as users tend to selectively ignore audio-only alerts and users may fail to see visual-only alerts if concentrating on something else.

Adhering to the mantra of WYCSIWYCU, "What You Can See Is What You Can Use," is always a best practice in user interface design. Presenting users with an abundance of information or choices that they can not use is overburdening. Such displays also compromise security by introducing a point of attack. Instead, revealing only control points which users may access minimizes the training required to use a system while enhancing its security.

6 Conclusion

Utilizing the One Space metaphor for the user interface both enhances meeting attendees' feelings of occupying a shared physical space and provides confidentiality assurances, such as knowing at all times who else is present in the connected rooms. The schematic of the One Space shared interface makes using the various devices in the room intuitive while enhancing security by revealing physically absent listeners at all times. Similarly, the pictorial representation of all devices, attendees, *etc*. and the consistency of the interface regardless of room locale makes repetitive use simple and success of interaction guaranteed. Hiding booking options from people who lack access to view various rooms simplifies their experience while providing privacy for hidden rooms. HP has utilized portions of the One Space interface guidelines in designing the interface for Halo, and internal studies have shown successful use by novices and overall improved user experience. Utilizing the One Space metaphor when designing video conferencing interfaces will provide more visible security assurances and support repetitive use, all while enabling even a novice to use the system to its fullest extent.

References

1. Harville, Michael; Li, Dalong.: Fast, Integrated Tracking and Activ ity Recognition with Plan-View Templates from a Single Stereo Camera. Proceedings of the IEEE Computer Vision and Pattern Recognition Conference. Washington, DC (2004).
2. Yee, K.: User Interaction Design for Secure Systems. Proceedings of the Fourth Inter national Conference on Information and Communications Security. Si ngapore (2002).