Global Information Assurance Certification Paper

Securing Online Team Collaboration Environments

Larry Cannell
GIAC Security Essentials Certification (GSEC) 1.4b, Option 1
June 27, 2004

Abstract

The team is at the heart of every creative process in a company or organization. To succeed a team must work to accomplish a given task, must meet the needs of individuals on the team, and do it all securely. "Virtual" teams are using a mixture of computer technologies to speed execution of their work and to provide flexibility in how the work is completed. Securing online team collaboration environments is challenging given the inherent distributed nature of today's virtual team and the diverse set of tools being used. It is essential to understand *what* tools are being used, the *value* they provide to teams and team members, and *how* they are used.

The online team collaboration toolset discussed in this paper includes the following technologies:

- Team Workspaces – used to manage the execution of team projects and the creation of team products
- Web Conferencing – used to facilitate online interactive meetings among distributed team members
- Instant Messaging – provides a collective team "presence" and facilitates quick exchanges of information

This paper will focus on deployment in a private enterprise working with external partners to deliver a product or service. The challenges discussed in securing this diverse set of technologies include common authentication and authorization and securely collaborating among an "extended-enterprise." This paper will also explore future emerging opportunities that will ease some of the burden of virtual team administrators by reusing resources used to secure the environment itself. It also discusses the challenges coming in securing the integration of collaborative applications, or the components that make them up, with business applications.

Table of Contents

Abstract 1
Introduction 3
  Virtual Teams 3
  The Challenges of Virtual Teaming 3
  Virtual Team Tools 4
How Virtual Teams Use Collaboration Tools 5
  Team Workspaces 6
    What is a Team Workspace? 6
    How Workspaces Are Used 6
  Web Conferencing 7
    What is Web Conferencing? 7
    How Web Conferencing is Used 7
  Instant Messaging 8
    What is Instant Messaging? 8
    How Instant Messaging is Used 9
Technical Architecture of Team Collaboration Environments 10
  Requirements Driving the Architecture 10
  Network Diagram 11
Security Challenges in a Team Collaboration Environment 12
  Common Challenges 12
    User Authentication Services 12
    Secure Connectivity to the Client 12
    HTTP Tunneling 13
    Client Software Installation 14
  Team Workspace Challenges 15
    Securing Workspace Files and Information 15
    Workspace Roles and Groups 16
  Web Conferencing Challenges 17
  Instant Messaging Challenges 18
    Securing Presence Information 18
    Securing BuddyLists 18
    Logging of IM Information 18
Future Opportunities 19
  Common Role/Group Management 19
  Federations 19
  Extending Into Other Applications 20
    Contextual Collaboration 20
    Extending Applications into Team Collaboration Environments 20
Summary 21
References 22

Introduction

Virtual Teams

Teams get stuff done. This cannot be stated any clearer or simpler. Regardless of what business processes are mapped out by high-priced consultants, policies or strategies set by management, or how smart a superstar employee may think they are, teams are the heart of every creative process in a company or organization. As James Surowiecki puts it [1]:

> "Instead of looking to a single person for the right answers, companies need to recognize a simple truth: Under the right conditions, groups are smarter than the smartest person within them."

How well your teams function will go a long way to determine the success of your company.

But, team members aren't waiting for their company to tell them how to work together (and, most importantly, how to work together securely). They are "setting standards without you" as Bill Jensen wrote in his 2002 book, "Work 2.0" [2]. Here is some more of what Jensen says:

> "There is only one way you are going to keep succeeding. You need more from all the teamwork within your organization. More innovation. More productivity. More self-direction. Success no longer comes from the top down. It comes from how good you are at finding, funding, focusing, and caring for all the work that bubbles up from below."

The best teams are focused on delivering something as quickly and as effectively as possible. To do this they work closely together and remain in close communication with each other. However, in today's environment there are many challenges to do this securely. In addressing these challenges we are now creating "virtual" teams.

The Challenges of Virtual Teaming

The first challenge today's virtual team faces is in dealing with team members coming from just about anywhere in the world. In a continual effort to streamline operations and improve results companies are focusing on core competencies. This leads to spinning off internal operations they aren't good at doing themselves and relying on others to provide these in their place. In short, companies need to "team" with other companies to get stuff done too. Teams are now made up of members from different companies. These team members may be located just about anywhere in the world.

The next challenge is in meeting the needs of the team members themselves. Particularly after the events on September 11, 2001, even the most die-hard of

corporate workers are starting to re-examine the importance of balancing family and work life. Flexibility is increasingly being demanded by workers. This is leading to an increasing number of companies offering telework and other flexible work arrangements.

Virtual Team Tools

Three primary tools are being used by virtual teams. They are:

- Team Workspaces – used to manage the execution of team projects and the creation of team products
- Web Conferencing – used to facilitate online interactive meetings among distributed team members
- Instant Messaging – provides a collective team "presence" and facilitates quick exchanges of information

Collectively these make up "the new-age collaboration triumvirate," as Matt Cain of the MetaGroup calls it [3]. Although each of these technologies started out independently, and have succeeded in their own right, the combination of these three used together represent the core set of technologies that virtual teams can use to be the most effective in their collaboration.

The first of these tools to become popular was instant messaging (IM), introduced by Internet portals and online services as a free add-on service for their customers. The leading consumer instant messaging services are from America Online, MSN, and Yahoo! Enterprise IM tools were first introduced by Lotus (SameTime) and then later Microsoft (as an add-on to Microsoft Exchange).

Web conferencing has recently become a prominent piece of the Internet with the rising popularity of WebEx and the recent purchase of PlaceWare by Microsoft. Microsoft was a pioneer in this market, releasing (and then bundling with MS-Windows) NetMeeting well before the commercial web conferencing services emerged. Unfortunately the protocols upon which NetMeeting were built are not conducive for use beyond the firewall which was a contributing factor to Microsoft deciding to unbundle NetMeeting from MS-Windows in a future release.

Team workspaces have been around in some form or another for many years. Initially, the need to share documents drove the development of network file systems. Lotus Notes (and then later a web version of Notes called Lotus Domino) showed how this could be enriched in a dedicated application environment that included other features teams need beyond file sharing. Later, eRoom showed how an easy-to-use interface could be delivered within a web browser. In response, IBM/Lotus released QuickPlace a standalone web application built on Domino. Finally, Microsoft came to the market with SharePoint and also co-marketed Groove, which provides a team workspace delivered using peer-to-peer technologies.

The converging markets for these tools reflect how teams are using them. IBM/Lotus' initial release of SameTime showed the synergy between Instant Messaging and Web Conferencing. However, the recently released Lotus Workplace Team Collaboration "integrates on demand capabilities—including instant messaging and presence awareness, Web conferencing and team space capabilities" [4] IBM/Lotus' products are being built as part of the IBM and Lotus Workplace product suites. Microsoft's product strategy is also showing an increasing amount of integration among these tools but coming from a Microsoft Office core. Even Yahoo! is feeling the need to integrate their instant messaging solution and offers a partnered service with WebEx to enable the launching of web conferences from IM sessions.

How Virtual Teams Use Collaboration Tools

Virtual teams work under the following assumptions:

- Team members can be located just about anywhere in the world. Radical time differences can alter the nature of a team but physical distance should have little impact.
- Team members can perform work during any hour of the day or night. However, ad-hoc interaction is important so knowing which team members are available at a given time is critical. Virtual teams prepare for and schedule meetings because synchronous time is the most expensive.

Jaclyn Kostner, and her company "Bridge The Distance," are experts in creating virtual teams. In Kostner's book, "Bionic eTeamwork" she says that physical presence of team members is important for building trust but not for doing the work. She calls it developing "InTouch" [5]

> "In the Bionic Phase, teams know they can collaborate faster, make decisions faster, and participate faster with Web conference, electronic teamroom, and other online collaborative technologies, from afar…Rather than listening to presentations in one room, they can participate in the presentations better through Web conference technology. Rather than carting back heavy paper files on the airplane, they know they can access the latest version of the electronic teamroom."
>
> "Teams that take the Bionic approach have more time to develop InTouch. They don't waste a single minute of rare face-to-face time on anything that they can cover from afar. *Travel to improve rapport, not do the work.*"

The core technologies that virtual teams need are:

- Team Workspaces to create the equivalent of the team war-room.
- Web conferencing to facilitate online meetings for physically separate team members.
- Instant messaging and presence to know who is available at any given time to enable ad-hoc collaboration and interaction.

An underlying assumption here is that team members already have access to email. Also, access to member and team calendars could have a big impact on the team's productivity. Unfortunately, there are insufficient implementations of calendar sharing between enterprises to enable this. However, most team workspaces provide facilities for team calendars.

Team Workspaces

What is a Team Workspace?

Team workspaces provide a place to store all of the team "stuff." This includes documents they are working on together in addition to project plans, team schedules and milestones, issues lists, etc. The simplest of workspaces are shared network drives that enable everyone on the team to access the same set of files. Sometimes this type of space is all a team needs. Often, however, shared network drives do not have the sufficient connectivity to reach all of the team members (shared drives to not traverse firewalls easily, if at all) and simply sharing files is not robust enough.

Lotus Notes was a pioneering technology for workspaces but there have been many alternatives developed since. In the consumer market (soccer teams, bowling leagues, etc.) Yahoo! Groups is a compelling solution providing a place to share files, archive email discussions, etc. Groove also can work well in this consumer environment because a central server is not required (at least, a central server is not required to store team information, central servers are still required to some degree). In the enterprise market Microsoft, IBM (with Lotus), and EMC (with eRoom) all have capable products that provide team workspaces.

How Workspaces Are Used

Teams use their workspace to:

- Work on common documents together. This enables teams to work on the "master" copies of documents together removing the need to constantly email updated files or posting them to a website for distribution. This is particularly important during the creation of a document when changes occur hourly.
- Use online databases to store things like issue lists, task assignments, milestones, meetings, contacts, etc. When the team is done these databases can paint the story of what happened and become the basis of "lessons learned."
- Share a common team calendar.
- Share their work in a context suitable to the team. Workspaces provide a customized web interface tailored to the task. Members are presented with a workspace that reflects what the team is doing. Documents and other pieces of information (like an entry in

an issue database) are linked to provide a holistic view of a project or task.
- Organize other artifacts important to the team like copies of reference documents, links to important resources, team surveys, online discussions, etc.

Web Conferencing

What is Web Conferencing?

Web conferencing provides a way for virtual team members to work together in real-time. Paired with audio conferencing web conferencing provides an environment where people in different locations can work synchronously: viewing and manipulating the same screen, same applications, and the same data, together.

The pioneering technology in this market was Microsoft NetMeeting, a no-charge Windows add-on that enabled online meetings virtually for free (you only pay for the cost of the network bandwidth). However, since virtual teams often have members participating outside of an intranet the use of NetMeeting ran into difficulties due to the nature of the underlying protocols used for the web conference, namely T.120. This is a client/server protocol that does not work through firewalls (without reconfiguration) and does not work through http proxy servers. To meet this growing need services such as WebEx and PlaceWare (later purchased by Microsoft) were created. These solutions use centralized servers to facilitate connectivity to all participants and provide an experience analogous to an audio conference. Clients connect via http (and https) and can easily traverse http proxy servers making them reachable to anywhere on the Internet.

How Web Conferencing is Used

Here is what Jaclyn Kostner says about web conferencing [5]:

> "Without question, Web conference technology is a breakthrough technology that every virtual team needs. Web conferencing doesn't eliminate the need for travel. When used well, however, I dramatically reduces the need to travel"

Wainhouse Research has a similar perspective [6]:

> "Like the other more “traditional” conferencing technologies such as videoconferencing and audio conferencing, web conferencing may or may not replace some of the ordinary in-person business activities an organization normally conducts. It can serve as an alternate solution when time-sensitive information is at play, which can be used to communicate, motivate, educate— - and then to

provide an environment for tracking and creating accountability. Ultimately it can become as much a part of a corporate culture as the lunchroom, the voice mail system, the annual Christmas holiday party, and the monthly or quarterly meeting."

The capabilities a web conference can provide are:

- Sharing applications and computer screens. By sharing my computer screen with you (using web conferencing technology) you can see my screen exactly as I do. So, anything I do on the computer you see as well, within fractions of a second.
- Share keyboard and mouse control. I can also give you control of the computer screen so your keyboard and mouse control my computer.
- Other capabilities such as shared whiteboarding, polling, and text chat.

The obvious benefit for virtual teams is the ability to synchronously collaborate with distributed team members. A clear benefit for any company is the reduced need to travel.

However, teams often find web conferencing more effective for collaborating on a document than physically meeting. If a conference room has a digital projector then you can get close to the dynamics of a web conference where everyone sees a single screen. However, in situations where multiple people contribute to a document web conferencing has a distinct advantage, even over the conference room with digital projector, because keyboard and mouse control is easily passed around. Paper-based meetings, on the other hand, cannot come close to the effectiveness of web conferencing.

Instant Messaging

What is Instant Messaging?

Most people reading this probably already have an idea of what IM is, have used IM at one time, or are using it now. However, what people sometimes miss is an understanding of the true importance of IM. The value of Instant Messaging lies in the "instant" and not the "messaging." What this means is that knowing I can communicate with you (or, rather, knowing that you are available) is more important than what is communicated. As an IM user I already have the message (a question, comment, concern, etc.) what I really need to know now is: who is around that can help me?

This is enabled by a feature found in all IM solutions: presence. Anyone who uses IM on a regular basis will tell you that knowing someone is

online is invaluable. With this presence information you have the choice of sending a text message or simply calling on the telephone.

Sometimes writers or analysts will refer to IM as an alternative to email. Although IM and email share the common trait of exchanging text messages the similarity ends there. IM is a form of real-time collaboration, email is non-real-time. Situations in which IM is used are actually closer to telephone calls than email. In fact, most users of IM in an intranet environment will tell you that their telephone habits are changed when using IM. If I don't see you online why call? I may also send a friendly "have a sec?" IM message before calling to avoid an impolite disruption.

Glover Ferguson of Accenture calls IM "The quiet second channel" [7]

> "Our lives are lived along multiple channels. We sit in a meeting, but are also aware of other forms of communication going on around us. We speak with colleagues, but may be interrupted by other pressing issues. IM, properly used, provides a helpful and welcome sort of "quiet channel" for brief communications that would be disruptive, even rude, using other communications media."

How Instant Messaging is Used

Virtual teams use instant messaging to keep a distributed team close together. A buddylist is the list of people that an IM client will track. This buddylist is often organized by groups of "buddies." When someone on my buddylist comes online (starts their IM client) an icon next to their name changes color or somehow indicates this person's online status. When this person stops using their keyboard or mouse for a few minutes their status is change to reflect this as well. They change to "idle" yet they are still online.

Virtual teams keep track of other team members in their buddylist so they know who is online or available at a given moment. If a team member comes across an issue they can look at their buddylist to see if someone is available to help resolve it. Often this results in a quick exchange of messages that are less disruptive than a telephone conversation and quicker than an email. This type of collaboration helps keep a team's issue list small and meetings focused on solving tough problems.

In a team environment you would expect the buddylist of all team members to be close to the same. Later, we will discuss opportunities to coordinate the content of this buddylist with other security management capabilities needed by the virtual team.

Technical Architecture of Team Collaboration Environments

Requirements Driving the Architecture

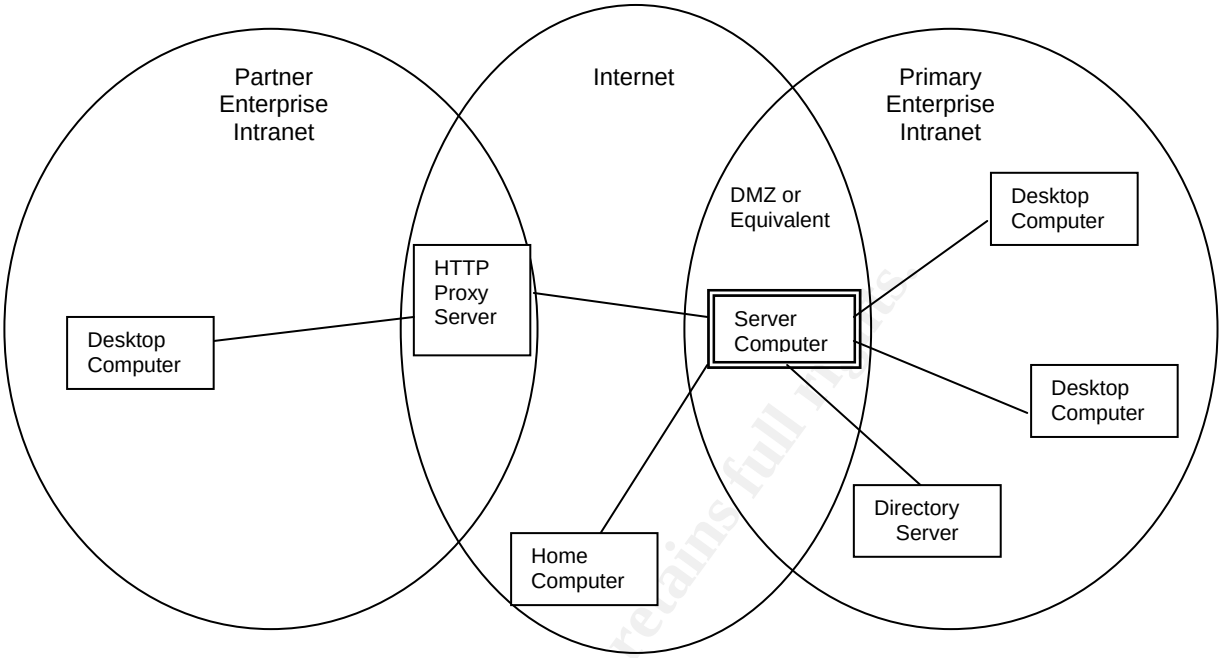
An assumption being made here is that a single primary company is driving the need for any number of virtual teams in support of their products or services. Our primary company's connection to the Internet is isolated with a firewall and access to the web is facilitated with an http proxy server. Furthermore, we will assume that any partner company will have similar firewall and proxy configurations.

Typical firewall policies do not permit IP connections to any address on the Internet without prior approval. And, although web traffic may go mostly unhindered, it must go through the http proxy server. This translates to applications being required to communicate via port 80 (http) or 443 (https) through an http proxy (possibly requiring authentication) to a server (or set of servers). Any IP connections using another port will require firewall modifications that will likely not be enabled in a timely manner (if at all) by other company firewall administrators.

We also have team members working from home during any hour of the day or night. Some may have Virtual Private Network (VPN) connectivity using company-supplied laptop computers. Others may be limited to using a home computer, minimally using a browser.

We also assume our primary company has a single directory containing names of users that can participate in our virtual team environment. These users may be in one directory (as shown in the network diagram below) or possibly two directories with one containing company employees, the other containing IDs of users external to the company Intranet.

Network Diagram



The diagram above shows the following:

- Two Intranets. Our Primary Enterprise Intranet and the Partner Intranet
- The Primary Intranet has a DMZ network holding the server computer hosting the virtual team application. This application could be the Team Workspace server, the web conferencing server, or the IM server. Network connectivity for all of these applications are identical.
- The Primary Intranet has two desktop computers accessing the application
- The Partner Intranet has one desktop computer accessing the application. This is done by going through the Partner HTTP proxy server which then connects to the application server.
- A home computer user connecting to the application server. This is connected to the Internet through an ISP. It may also have a home firewall which is not shown here.
- A Directory Server sitting on the Primary Intranet. This is used by the application server for authentication information.

Other items to note

- Desktop computers do not communicate directly without an intervening server. This is an obvious need for the Team Workspace application since it is a server-based application but may not be the most efficient for IM and Web Conferencing. Given the assumption that firewalls and proxy servers will be involved a server must facilitate all communication. However, there may be times when a peer-to-peer connection is possible and may be desirable for cost reasons. For example, NetMeeting works peer-to-peer without the need for an intervening server. This saves us the cost to use a server. However, NetMeeting only supports online meetings when no

firewalls are involved (when all participants are on an intranet as an example).

Security Challenges in a Team Collaboration Environment

Common Challenges

User Authentication Services

A single source of user authentication should support all three toolsets. Users quickly get tired of tools that have different methods of authentication (different usernames and passwords). Authentication is most important for Team Workspaces and Instant Messaging since user identity is critical in both of these. The team needs to know who created a file or posted a comment in the workspace. The team also needs to know who is online and chatting with them.

However, web conferencing relies less on user identity since it is mostly required when scheduling conferences and less important to participate in a conference itself (other methods are used to secure the conference).

In today's market the only viable option appears to be an LDAP-compliant directory service. Most, if not all, of the popular Team Workspace and IM tools support the use of an LDAP directory as the basis for user authentication.

In the future federations will likely play a large role in providing user authentication services to team collaboration environments. In our assumed scenario federations could greatly simplify authentication for all users, especially for users at partner companies.

Secure Connectivity to the Client

In the network diagram there are three different paths a client computer could take to access our application server. They are:

1. From the Intranet
2. From the Internet
3. From a partner Intranet

Also, the type of applications in our toolset can have an impact on how we secure their connectivity to the server. In the case of team workspaces the most popular products are web-based and run within a standard browser (one notable exception is Groove, based on peer-to-peer protocols) so we will assume the use of a browser. This implies we will be securing this channel with https using a server certificate.

Instant messaging and web conferencing are client/server applications. In the case of IM these clients are either natively coded (for Windows they

are win32 applications) or are Java applications (either running in a browser context or based on a standalone Java Run-Time engine executing on the client computer). There are also situations where an IM client uses a standard browser window but this is generally less than full function since it has to emulate client behavior. (As an aside, this brings up the issue of distributing presence information to web-based applications, something we will cover later.)

Web conferencing clients are always client/server applications (native code or Java). NetMeeting is a native Windows application. WebEx is a combination of native and Java code. PlaceWare, at one time, was written entirely in Java but has since started using win32 code.

How we secure these client/server connections will depend on the path they take. For the intranet clients we could leverage a company's existing single sign-on capability, such as Kerberos for Windows and UNIX desktop computers and then optionally encrypt the channel using SSL.

We do not have as much freedom for securing the Internet and partner intranet clients. In these cases the only access to the server will likely be https. This precludes the use of NetMeeting for these clients since it relies on the T.120 protocol and does not support any type of http transport. Any web conferencing or IM client software supporting clients that are only able to access the server with proxied http connections must use http tunneling.

HTTP Tunneling

Http tunneling (or https tunneling where secure http connectivity is required) is a method of providing client/server connectivity in situations where a standard TCP socket connection is not possible. This is the case for many corporate desktop computers, such as the primary or partner intranets in our scenario, connecting to servers on the Internet.

When an http proxy server is used to facilitate client/server communication the TCP connection from a client is terminated with the proxy server. In turn, the proxy server makes an http request, using a separate TCP connection, with the destination server. There is no single TCP stream between the client and the server.

Specifically in the case of a browser surfing the web from an intranet, the browser acts as the client and the destination server is a web server. The browser passes http packets to the proxy server via a TCP connection. The http proxy server then forwards these packets, using a separate TCP connection, to the web server.

Http tunneling provides a functional equivalent of a TCP socket connection to a non-browser application that must operate where http connectivity via a proxy server is the only path available. IM and web conferencing solutions were one of the first applications to widely use http tunneling.

From a user perspective you could see http tunneling being used by early IM clients. These clients required you to manually enter http proxy server information in a configuration dialog. On intranets requiring username and password authentication to traverse a proxy server these application would store this information along with other configuration information. Recent IM Windows clients leverage functions provided by Internet Explorer for http connectivity. Authenticated proxy servers now result in the standard IE dialog box for entering username and password removing the need to store it locally on the client.

Methods for providing http tunneling have been published by IBM [8], Oracle [9], and many others, but their use has not been without controversy. One of the reasons firewalls and proxy servers are installed is to control the type of Internet connectivity allowed by an intranet client. Http tunneling removes much of this restriction. When deploying IM or web conferencing clients that will be used on partner intranets you should be sensitive to the concerns of the partner's IT staff. Additional information about http tunneling is available in a paper published on the SANS Reading Room written by Daniel Alman called "HTTP Tunnels Through Proxies" [10].

As tempting as it is to simply require all clients (intranet, Internet, and partner intranet) to just use https we should note that tunneling applications this way incurs additional overhead. In the case of https the entire packet is encrypted. This would include the extra packing and transcoding required to tunnel application data. So the overhead is measured in terms of repackaging the data to be transported over https and also the additional overhead in encrypting this larger packet. Since most users are likely coming from the intranet we should support the application's native client/server protocol where possible to reduce cost. We might also consider opening the client/server protocol port to the Internet to support home computers or partner computers allowing unencumbered outbound access to the Internet.

Client Software Installation

Another important consideration is the installation of any client-side software. This will likely require administrator privileges. Many (most) Windows users are running with administrator privileges and will be able to easily install the software. However, this is becoming less likely over time as companies are tightening security policies on desktop computers

and prohibiting users from installing software without assistance from an administrator.

The use of instant messaging almost always requires the installation of client software. Even if the client is based on Java there is at least a need for a Java Run-Time engine (Java VM) to execute this code on the client outside of the browser. If the Java IM client is run inside the browser you are at risk of the user closing the browser window hosting the IM client and, therefore, closing the IM application itself.

The level of administrator involvement for web conferencing depends on the role the user will play in the web conference. Viewers in a web conference usually do not need any native code or privileged Java code to execute.

When a web conference participant shares their desktop or application window, other participants see everything happening in that window or desktop. This includes any text typed, mouse movements, window resizing, etc. Highly privileged access to the windows display subsystem is required to make this happen. To accomplish this WebEx and PlaceWare use native Windows software. A locked-down client will require elevated privileges to install the software. Since NetMeeting is shipped with Windows it will have all of the access it requires to the display to share it in a conference.

Other software required on the web conferencing client are utilities to either prepare a presentation to be uploaded to the web conferencing server or to playback a recorded conference. Check with the individual web conferencing providers for more details on these utilities.

And, lastly, even though team workspaces are generally web-based sometimes client software is required to provide an enhanced user experience. This can be in the form of Active-X controls that enable an easier to use browser interface or a standalone client application to monitor workspaces for changes. These applications may require proxy configuration (including username and passwords, for older versions) to monitor workspaces outside of a corporate intranet.

Team Workspace Challenges

At this point we are assuming users can securely login to the team workspace based on a username and password (that may come from a LDAP-compliant directory source) and their transport to the application server is secure (perhaps using https).

Securing Workspace Files and Information

Securing access to a workspace is handled at two levels:

1. Access to the workspace
2. Access to objects within the workspace

Often users only recognize securing the object themselves (level 2 above) as the only point of control. But, we should not forget that unless users are granted access to the workspace they will not have access to anything there. This is a critical distinction to make for users who are concerned about the maintenance of access control lists for objects within the workspace. If the management of access control lists within a workspace is becoming too complicated then users should consider breaking it into multiple workspaces.

For example, eRooms can be stored in containers called facilities. Facilities are intended to hold multiple eRooms for groups or organizations working on similar tasks. By segregating a facility into multiple eRooms focused on different parts of the organization or different teams then securing the individual eRooms becomes much simpler and more deterministic

For those familiar with UNIX or Windows directory or folder permissions then securing workspace objects should be straightforward. The organization of the workspace is generally hierarchical and folder-based. If a user has access to a particular folder then they can see what is in that folder but may not necessarily have access to objects within the folder (that is determined by access control applied to the object itself).

Workspace Roles and Groups

Managing users who have access to a workspace can take a significant amount of effort depending on the complexity of the workspace, the scope of the team's assignment, and the number of people granted access to the workspace.

Workspaces come with a default set of roles. Administrators (or super-users, coordinators, etc.) generally have full control of the workspace. Other roles determine what type of access the user has. The least privileged role of a user granted access to a workspace can only view objects to which they are granted access. Custom roles could also be granted to help manage the workspace.

Another method for managing the set of users granted access to workspace is to use groups. Now, these may sound the same as roles, and in general they are, but there are some important distinctions, particularly in regards to an enterprise's user management architecture.

One important distinction is in the scope of the role or group. A good workspace product should be able to leverage a central definition of a

group. This definition may come from an LDAP-compliant directory server or some other form of authorization server. We will cover this is more detail later.

Web Conferencing Challenges

At this point we are assuming the transport between a client and the web conferencing server is secured. This is likely done through https or a direct client/server connection. Securing the rest of the web conference involves protecting the scheduling or initiation of a conference, the protection of any presentations that are uploaded to the conference account (if one exists), and the protection of any artifacts created during the conference (marked up files, for example).

User identity isn't as critical for web conferencing as it is for team workspaces and instant messaging. However, if it is possible to configure a web conferencing solution to identify individual users then you should do it. This is where an integrated team collaboration solution can pay off. There are two types of integrations with web conferencing possible in a team collaboration environment.

1. Integration of web conferencing within a team workspace. This allows for the management of the conference on a team calendar, the passing of user identification into the web conference, and the securing of any artifacts created in the conference (like marked-up documents) within the workspace. It also aids in ease-of-use since the team workspace is the place to not only find team information and documents but is also the place where the team holds online meetings.
2. Integration of web conferencing with instant messaging. This facilitates ad-hoc collaboration enabling a chat session to turn into a full conference to make a point or resolve an issue.

A standalone web conferencing solution can still be useful to a team but the ease of transitioning between the tools will be affected. But, also consider that web conferencing will be used outside of a virtual team context and should, therefore, accommodate the participation of users outside of a team.

A standalone web conferencing solution uses passwords to protect a conference. The person who schedules the conference chooses a password and then distributes it to the team members prior to the start of the conference. The only critical function that requires user identification in this case is the scheduling of a conference. Without this identification we wouldn't know who is using the conference (or where to send the bill) and we run the risk of someone using conferencing resources without our knowledge (at least, until the bill arrives).

Some standalone web conferencing solutions also provide methods to upload presentations prior to a meeting. Provisions should be made to ensure these files are deleted immediately after the meeting completes. Also, any artifacts

created during the meeting should not be left on the conference server. One method of doing this is to not use presentation modes that require uploading of slides prior to a conference. Instead, have one of the participants present the slides from their computer and use application sharing for other participants to see. This means the host computer sharing their computer or application screen will have the files located there and not on a conference server.

Instant Messaging Challenges

At this point we are assuming IM clients are connecting to the IM server via https or a direct client/server connection. Securing the rest of the IM environment involves keeping presence information private, securing buddylists of individual users, and securely logging information (if this is desirable).

Securing Presence Information

Although the idea of presence is a valuable capability for IM systems and users who want to chat with you, it is also an extremely private piece of information anyone will want secured. Presence information can contain the following:

- My online status (logged in to the server, busy/idle)
- My IP address (which may imply location)
- My location (depending on the IM service)

It is critical that the IM user be given control over the use of this information or be notified how this information may be used. Most IM systems provide mechanisms for the publishing of presence information. The simplest form of this is to allow anyone on my buddylist to see my presence information. Some IM systems, such as Jabber, provide mechanisms that explicitly asks permission before someone can view your presence.

Securing BuddyLists

Buddylists are usually stored on the IM server. This allows a user to get access to their buddylist from anywhere using an IM client.

My buddylist can tell the world a great deal about me. Depending on how I organize by buddylist (by labeling my groups of buddies) and who is on my buddylist, someone might be able to tell what projects I'm working on or infer other potentially vital pieces of information. Therefore, it is critical that the server protect users' buddylists

Logging of IM Information

This is probably the most sensitive part of running an IM service. The logging of IM information is analogous to tape recording telephone conversations. Also, depending on how much information is logged, it could provide details on where and when a user logged into the system.

Some government regulations require the logging of IM conversations, particularly with customers. This is usually required where the recording of other conversations and exchanges is done. If logging is used then this brings with it a host of other security challenges such as the storage, archival, and retrieval of log information.

Future Opportunities

There are a number of emerging opportunities to improve team collaboration environments.

Common Role/Group Management

Security is not usually the first thing a team thinks about when trying to figure out how to accomplish a task. It is often the one sacrifice made by the team when it comes down to meeting a deadline. "Selling" security is difficult but there are opportunities that vendors and product developers should consider when dealing with team collaboration tools.

Authorization is a key capability with any security solution. Being able to provide a list of people who can perform a particular function or access a piece of information is critical. The key here is that security roles and security groups, at their most fundamental state, are lists of people. Virtual teams also deal with a list of people, the list of people on their team. This is where there is an opportunity to meet the needs of virtual teams while simultaneously making the environment more secure and auditable.

Depending on the scope and size of a team the life of a virtual team administrator can be difficult. Who is on a team and what role they play is something the administrator must constantly track. They do this by updating email distribution lists, permissions in the team workspace, and instant messaging buddylists.

If there were solutions that provided security roles or group definitions that could also be used as email distribution lists, within an IM buddylist, or within the team workspace to define access (and roles within the workspace itself) then team members would whole-heartedly embrace security from the start. This requires the central management of lists (people who play a role or are in a group) that are usable by multiple tools.

LDAP groups seem to be the closest option we have to support this. However, choosing an integrated toolset may be the simplest way to provide this at this time.

Federations

When companies form a trust relationship where one will honor the other's assertion of user identity this is called a federation. This type of capability is being developed by the WS-* consortium as well as the Liberty Group and

others, such as the Internet2 Shibboleth initiative. Team collaboration environments will be one of the first toolsets to benefit when these solutions are realized. The main benefits are in the reduction of team administration, better accountability for user identity and authorization, and quicker deployment of collaboration environments.

Extending Into Other Applications

Contextual Collaboration

A number of years ago analysts predicted the coming of a new capability called "contextual collaboration" [11]. This is based on the assumption that collaboration tools are made from building blocks or components. These components can then be used in the context of a business application. For example, a customer request initiated by a call-center application results in the creation of an online discussion thread, provided by a team workspace product, where the issue is discussed and resolved. The standard team workspace interface is never used. Instead the discussion thread component is called by the call-center application and is used in its context.

One of the best, and most widely used, examples of contextual collaboration is the embedding of presence information in an application. For example, say you are using your company's white pages directory web application to look up someone's telephone number or other piece of information. You enter a name, submit the form, and it returns a list of names that are possible matches for your query. Each match may show a telephone number and email address. In addition it may also show if the person is online with an icon you can click to initiate a chat session.

Imagine this embedded presence icon showing up in the signature of an email or next to the name of the person who approved a part in a manufacturing release system. The possibilities are endless.

The security challenges outlined in this paper would now apply to any application using inline presence or any collaboration component. In addition there is a need to delegate the identity of a user (and, therefore, all of the rights and permissions granted to that user) from one application to another. This is clearly an area where the development of web services standards (particularly in the area of security) will help solve.

Extending Applications into Team Collaboration Environments

An alternative integrated approach is to retain the working context within the team workspace. In this case a team is working to solve a business problem and is using the virtual team tools. To retain this team context we make business application data and functions accessible within the workspace. This enables the team to continue using the workspace as the

place it gets work done. Data comes into it rather than having users leave the workspace to retrieve data from business applications.

The security challenges here are similar to those described above in "contextual collaboration." Specifically, the need to delegate user identify and authority from one application to another.

Summary

Teams are critical to the success of any company or organization. Virtual teams are growing due to the continuing drive for operational efficiencies and due to the desire of individuals for balance between work and home life. Virtual teams use team collaboration environments to accomplish their tasks as efficiently and flexibly as possible. To secure virtual teams it is essential to understand *what* tools are being used, the *value* they provide to teams and team members, and *how* they are used.

Security challenges shared among the virtual team tools are a common source of authentication, securing client connectivity, and client software installation. Additional challenges are posed by each of the applications that make up the environment: team workspace, web conferencing, and instant messaging.

The management of common roles and groups offers an opportunity to "sell" security to virtual teams by providing a capability that eases the administrative burden of team management while simultaneously increasing the level of security and audit-ability of the environment.

The extension of collaborative services into business applications, or the extension of business application data and functionality into collaborative tools, will be challenging to secure given the need to delegate user identity and authority between applications.

References

[1] Surowiecki, James. "Smarter Than the CEO." Wired. Issue 12.06, June 2004. http://www.wired.com/wired/archive/12.06/view.html?pg=2

[2] Jensen, Bill. Work 2.0. Perseus Publishing. 2002. http://www.perseusbooksgroup.com/perseus-cgi-bin/display/0-7382-0804-3

[3] Cain, Matt (MetaGroup). "META Report: Tackling The Instant Messaging Tiger." Datamation Earthweb. September 6, 2001. http://itmanagement.earthweb.com/cio/article.php/879621

[4] Lotus Workplace Team Collaboration 2.0 spec sheet, Accessed: 5-Jun-2004, Copyright 2004. ftp://ftp.lotus.com/pub/lotusweb/workplace/LotusWorkplaceTeamCollaboration20_SpecSheet.pdf

[5] Kostner, Jaclyn. Bionic eTeamwork. Dearborn Trade Publishing. 2001. http://www.bionicteam.com/

[6] Greenberg, Alan D (Wainhouse Research). "Renegades & Rogues: Taming the Chaos of the Unsanctioned Web Conferencing Buy." 2003. http://www.wainhouse.com/files/papers/wr-webrenegades.pdf

[7] Ferguson, Glover (Accenture). "Instant Messaging: Not Just For Kids Anymore" Accessed: 5-Jun-2004, Copyright 2004. http://digitalforum.accenture.com/DigitalForum/Global/ViewByTopic/EmergingTechnologies/0301_IM

[8] Davis, Malcom. “Tunneling through the corporate network.” IBM developerWorks. 1-Jul-2001. http://www-106.ibm.com/developerworks/java/library/j-tunnel/?dwzone=java

[9] “HTTP Tunneling using Servlets Sample.” Oracle Technology Network, 12-Jun-2004. http://otn.oracle.com/sample_code/tech/java/servlets/samples/tunnelClient/Readme.html

[10] Alman, Daniel. “HTTP Tunnels Through Proxies.” SANS Reading Room. 20-Jul-2003. http://www.sans.org/rr/papers/12/1202.pdf

[11] Mahowald, Robert and Levitt, MarK (IDC). "From the ICE Age to contextual collaboration" KMWorld, October 2001. http://www.kmworld.com/publications/magazine/index.cfm?action=readarticle&Article_ID=1107&Publication_ID=56