WebEx Security Overview
Security Documentation

WebEx Security Overview

Introduction

WebEx™ Communications, Inc. provides real-time communication services to a large and growing number of corporations. These corporations use WebEx services for diverse purposes ranging from sales, marketing, project management and support. These corporations represent a variety of market sectors including technology, finance, manufacturing and healthcare. WebEx endeavors that its service offerings meet the most stringent security requirements of corporations so they can use WebEx services effectively and routinely, secure in the knowledge that their sessions are safe and private. It's no surprise then that WebEx assigns data security the highest priority in the design, deployment and maintenance of its network, platform and services.

The purpose of this document is to provide information on the data security features and functions that are available in the various WebEx services and inherent in the underlying WebEx communication infrastructure. We discuss the following items in this document:

- Application
- User Interface
- Architecture
- SSL Encryption
- Facilities Security
- WebTrust Accommodation

The reader is assumed to have knowledge of core WebEx capabilities and services, including an understanding of the WebEx MediaTone Network. The WebEx services include:

- Meeting Center, for highly interactive sessions
- Training Center, to deliver the most effective training via the Web
- Event Center, for large Web-based seminars
- Support Center, optimized for helpdesk and support sessions

The reader should also be aware of the roles available in the various services, like Host, Presenter, Panelist, etc.

Unless otherwise specified, the topics described in this document pertain equally to all WebEx services.

Application

WebEx implements security at the application layer primarily via the WebEx Service Manager software. This is comprised of several local machine software components that make data collaboration possible by coordinating with WebEx Services clusters located across the WebEx MediaTone Network. The WebEx Service Manager has many features that make it a safe and secure method for data collaboration.

It is impossible to participate in a WebEx session without the close coordination between the Service Manager and the WebEx Services cluster. Since the data in a WebEx session is shared using the Service Manager software, which must establish a connection with a WebEx Service cluster, these security features are inherent throughout the session. In short, each session is dynamic and involves a handshake between the client and the WebEx Service cluster, and the communication between these components is by default encoded and optionally SSL encrypted.

Firewall Compatibility

The WebEx Service Manager communicates with the WebEx Services cluster to establish a reliable and secure connection. At the time of client instantiation, the WebEx Service Manager will attempt to determine the best method for communication. In the process of establishing this connection, the WebEx Service Manager attempts to connect using TCP (port 1270) or HTTP/HTTPS (port 80/443). Quite often port 1270 is blocked by a firewall and when this is the case the WebEx Service Manager will tunnel all WebEx communications using HTTP/HTTPS. In the case that a WebEx site incorporates an SSL connection, all the traffic is carried over HTTPS (port 443). Regardless of the connection that is established at the time of client instantiation, by establishing this communication between the Service Manager and the WebEx Cluster, firewalls do not have to be specially configured to enable WebEx sessions.

Content Security

WebEx provides several controls to prevent unwittingly sharing data. Unlike other Web conferencing solutions, WebEx restricts application sharing to specified applications. With WebEx, when a Presenter shares a web page or a specified application, other applications running on the Presenter's desktop will never appear on Participants' machines (other vendors display everything within a predefined "frame"). Further, a Presenter can use the Pause Sharing feature at any time to restrict the Participants' view of sensitive data within a shared application. Finally, WebEx is the only provider of 128-bit SSL encryption that encompasses all session data, from the session creation and join pages, to the actual session itself, to the Web pages that follow an interactive session.

WebEx provides a highly secure environment for data collaboration. The WebEx Service Manager is designed to deliver in real time, rich-media content securely to each Participant within a WebEx session. All content that a Presenter shares with the Participants in a WebEx session is only a representation of the original data. In addition, all content that is shared with the Participants in the session is encoded with a proprietary encoding process.

To gain a better understanding of this process, it is useful to compare the WebEx proprietary encoding process to the PDF encoding process. The PDF format is a proprietary encoded representation of the original object. This encoded content contains no executable data but only inert data, which can be interpreted only by the appropriate content viewer. The WebEx Service Manager functions similarly. The WebEx Service Manager encodes a representation of the original object and delivers that representation

to the other Participants within the session. The encoded content contains no executable code and it is viewable only by the WebEx Service Manager.

However, the way in which this encoded content is delivered is entirely different. As discussed previously, WebEx Services never sends session content in clear text. Prior to sending information from a Participant's Service Manager to the WebEx Service Cluster, the WebEx Service Manager encodes all data in a proprietary format. Moreover, WebEx uniquely identifies session Participants with individual session IDs that WebEx uses to thwart hackers from reassembling session content. These techniques provide safeguards to prevent reconstruction of the data conferencing portion of the WebEx session.

Session Security

In every WebEx session there is only a logical connection between each local machine via the WebEx MediaTone Network; there is no direct network connection between the local machines. The logical connection is fixed and only application functions can be performed. There is no way to perform general-purpose tasks outside of what the WebEx Service allows.

A WebEx session connection is composed of several layers superimposed on one another. The lowest layer is TCP/IP that allows for general data communication and underlies all communications. Above this is the application (web) layer that provides for logical connection of a web browser to a web server. The WebEx Service Manager software, which establishes an end-to-end connection between the Service Manager software and the WebEx Cluster, also communicates at the same application layer as the web browser.

Each layer serves a different purpose and has different capabilities. While the lowest level provides arbitrary data communications, higher layers are more specific and less flexible in what can be done. As each layer is established, the network connection is further constrained by the limitations of each layer.

The end result being that the total connection is limited to what can be done at the WebEx layer.

The layers can be characterized by connection flexibility, protocols used and capabilities allowed. The following table summarizes each layer.

Layer	Connection Flexibility	Protocols Used	Capabilities Allowed	Scope and Security
TCP/IP	Can be used to create connections between network components.	TCP/IP	Capabilities allowed subject to limits imposed by network security (e.g. firewalls).	Although TCP/IP underlies all communications, it is only directly used by the web browser to initiate a connection to a web server. In many cases, this will be a connection to a proxy server that is internal to the respective company. There are no other connections being initiated outside of the web connection.
Web	Can only be used to establish a connection between a web browser and a web server. Connection must be initiated by the web browser and made OUTBOUND to the web server.	HTTP, SSL	HTTP allows a rich data stream that can implement a wide variety of application-specific capabilities.	The Web layer provides a secure connection between the web browser and the web server. No other use of the connection is allowed. Once established the endpoints are fixed.
WebEx	No flexibility at all. Endpoints are fixed between the WebEx Server and the Web browser plug-in.	Proprietary protocols specific to WebEx services	Capabilities are defined explicitly by the WebEx server and the Service Manager software running in the web browser. No other capabilities allowed.	Provides collaborative capabilities and functionality. Only of the applications that are specified by the Presenter from presenting machine. The application-specific functions are possible since WebEx components are running on each end of the connection.

Client Connection Security

Every WebEx Service Manager connection must authenticate properly prior to establishing a connection with the WebEx cluster to join a WebEx session. The client authentication process uses a unique, per client, per session cookie to confirm the identity of each Participant attempting to join a WebEx session. Each WebEx session has a unique set of session parameters that are generated by the WebEx Service cluster. Each authenticated Participant must have access to these session parameters in conjunction with the unique session cookie in order to successfully join the WebEx session.

User Interface

WebEx security is also enforced through a variety of mechanisms exposed through the WebEx user interface which include web pages devoted to site maintenance, Host profiles, and creating sessions, as well as the session interface itself (denoted by the "Welcome Screen"). The available options depend on the role a WebEx session Participant assumes.

Roles and Responsibilities

There are several roles in a WebEx session – Host, Presenter and Participant. (Training Center has the notion of a Panelist, which in the context of privileges, is treated similarly to a Presenter in Meeting Center.)

A Host can create, schedule and maintain WebEx sessions, including session parameters that the Host defines (see below). Only the Host can view and edit these session parameters. The Host is the only user who can start a WebEx session.

Hosts are identified and created either by self-registration, a site administrator or via WebEx on behalf of our customer. (Self-registration can be disabled.)

Meeting Parameters

Hosts can specify the following meeting parameters relating to security:

- Unlisted meetings
- Meeting passwords
- Participants must have a Host ID for the site

When a meeting is created, WebEx assigns a randomly generated, non-sequential meeting number to uniquely identify the meeting. Unlisted meetings never appear on the user interface. They are accessible only through a link sent via the email invitation process or by a Participant explicitly providing the meeting number on the WebEx join page. In either case, the Host must explicitly inform the Participant of the existence of the meeting.

Meeting passwords can be forced at either the site or the meeting level. If the site requires meeting passwords, all meetings on that site will require passwords. In addition, the notion of strong passwords can be specified on the WebEx site as a requirement if the site has been configured to require meeting passwords. The strong password feature will apply to Host ID passwords as well.

The WebEx site can also be configured to disable email invitations. This allows the Host greater control over the distribution of the meeting access information.

Host, Presenter and Participant Privileges

Only a Host can start a WebEx meeting. Each Host is required to log on to the WebEx site with a Host ID and password. Once the Host is authenticated on the site, the Host can start a WebEx meeting. The Host has the first level of control in the meeting and is made the initial Presenter. He or she can grant or revoke Host or Presenter permissions at any time to any Participant in the meeting. The Host can also terminate the session for all Participants at any time.

Additionally, the Host can expel any meeting Participant for any reason and can prevent subsequent meeting access from any potential Participant by "locking down" the meeting.

The Presenter is the WebEx session Participant who has the capability to share data. The Presenter determines what is shared in a WebEx session and the level of access that the Participants will have during a WebEx session by setting Participant privileges.

A special case is where the Presenter may also grant permissions for individual Participants while an Application/Desktop sharing session is under way. One such permission is the ability for a Presenter to grant a Participant the ability to remotely control the Presenter's shared application or desktop. This is the WebEx remote control capability. At any point during such a session the Presenter can immediately revoke the Participant's remote control privileges. This allows granular control over what can occur during a remote control session. The key point here is that the Presenter must specifically identify a Participant, allow that Participant to remote control his or her application or desktop, and is able to immediately relinquish this capability if required.

A Participant within the WebEx session can view the data that is being shared by the Presenter and, using remote control with the Presenter's permission, manipulate a shared application. The Presenter controls the permission levels that Participants have when interacting with the shared data.

Site Administration Configuration

WebEx Site Administration permits customization of the configuration of a WebEx site to disable some of the core functions available within a session. For example, the Presenter's ability to Share Desktop can be disabled on a per site basis. The Share Desktop feature in the WebEx Service Manager software user interface would be disabled for any sessions that are started from that site and the Presenter would be unable to share their desktop with other Participants in the session. Other related features of Site Administration Configuration include:

• Require login before site access
• Require approval of "Forgot Password?" request
• All meetings must be unlisted
• Require participant email address
• Require strict password for new user accounts
• All meetings must have a password

Summary of Host responsibilities:

- Start/Schedule WebEx meetings
- Grant/Revoke Presenter privileges
- Grant/Revoke Host privileges
- Terminate application sharing session for all Participants in the meeting
- Expel Participants
- Restrict access to the meeting
- Terminate WebEx meetings
- Mute/Un-Mute individuals using the integrated teleconference

The following security capabilities are available to the Presenter:

- View the list of Participants in the session
- Enable Participants to save or print presentations or documents shared in the session
- Enable Participants to switch pages in a presentation or document share
- Enable Participants to annotate on session content
- Enable Participants to send text messages to other Participants, the Presenter (or both)
- Enable Participants to record the session
- Ability to grant temporary control of a shared application to specific Participants
- Temporarily freeze an application share, preventing the Participants from viewing the shared content, in order to allow the Presenter private and secure access to sensitive portions of the application

Architecture

WebEx uniquely deploys a globally distributed network of high-speed switches. With this architecture, session data originating from the Presenter's machine and arriving at the Participants' machines is switched – never stored -- through the WebEx MediaTone Network. No session data is stored on the WebEx cluster; WebEx sessions are completely transient.

It is useful to compare the WebEx switching network with the telephone system, where voice is carried across the PSTN in a sophisticated, switched manner. From a security standpoint, this architecture has an advantage in that there is no persistent storage of any session data within the WebEx infrastructure. There is no need to upload content to the WebEx Services cluster; dynamic session content displayed during a WebEx session originates only from the Presenter's machine; Participants see only representations of this data. At the conclusion of a session, all such representations dissipate – similar to what happens when a voice telephone call terminates. Like the phone system all that remains of a WebEx "data call" is ancillary information like billing records, not a record of the conversation itself.

WebEx has invested much time and energy into developing and deploying a secure environment for our services. WebEx employs state of the art firewalls, network monitoring, and intrusion detection tools. Production servers undergo a hardening process prior to deployment. Strict change management is employed and additional policies and procedures are enforced. To further ensure adherence to best practices with respect to data security, WebEx retains third parties to regularly perform security audits and conduct vulnerability threat assessments.

SSL Encryption

In addition to all the safeguards discussed herein, for utmost security, WebEx provides the option of securing all session content with 128-bit encryption using Secure Sockets Layer (SSL), which is the most widely used Internet standard for securing sensitive data communications. With SSL, WebEx encrypts all data within a WebEx Service cluster, including the WebEx session data. This will prevent third parties from accessing any data in transit.

Facilities Security

WebEx session services are provided through points of presence (POPs) in various geographic locations, including the San Jose and Denver-based Data Centers. The facilities have on duty personnel, 24 hours a day and seven days a week. To gain access to any facility, one must first be on the approved access list and then be authenticated by additional security controls.

Security Personnel

WebEx has a dedicated security department. Security personnel receive regular training in all aspects of enterprise security. WebEx spends a significant amount of time receiving training from vendors and industry experts to keep current in this rapidly changing environment.

WebTrust Accreditation

WebEx has been awarded a WebTrust seal of accreditation. Here is a brief excerpt that describes the value of this accreditation.

WebTrust is a seal awarded to web sites that consistently adhere to certain business standards established by the Canadian Institute of Chartered Accountants (CICA.ca) and the American Institute of Chartered Public Accountants (AICPA). Now globally recognized, these standards can be in the areas of privacy, security, business practices/transaction integrity, availability, confidentiality or non-repudiation.

The WebTrust Security Principle sets out an overall objective for the security of data transmitted over the Internet and stored on an e-commerce system. In the course of a WebTrust audit, the practitioner uses the WebTrust Criteria as the basis for assessing whether the Principle has been achieved.

Backed by the CICA and AICPA, WebTrust is the only Internet seal that can give web-goers true confidence that certain businesses can be trusted with consumers' (and business') most important asset and prized possession: their private information. What makes WebTrust different from all other Internet seals? Independent verification is the key to WebTrust.

Unlike any other Internet seal that claims to protect consumer or business privacy, WebTrust is the only seal administered by a third-party. That means when you see a WebTrust Seal on a web site, the owners did not get a seal simply by paying for the privilege. They had to meet standards set by the professional accounting bodies of Canada and the United States (CICA & AICPA). And the site is audited for WebTrust compliancy at least every 6 mo.

Conclusion

WebEx services have undergone exceptional increases in usage. This would not be possible without careful attention to the incorporation of security principles and standards in the design and operation of the WebEx infrastructure and services. Data security will remain the highest priority at WebEx, enabling WebEx to continue achieving the goal of providing the most efficient and secure online real-time communication service.

WebEx's Commitment

WebEx believes that privacy and security are of the highest importance to our clients and business partners. WebEx's commitment includes:

- Consult with specially trained and licensed WebTrust auditors to review our security policies and procedures
- Maintain the highest business standards found on the Internet
- Have our production environment regularly audited to make sure the standards are maintained

For more information on WebTrust please visit: http://www.webtrust.net/