

BEST PRACTICES IN WEB CONFERENCING SECURITY

A Spire Research Report – April 2003

By Pete Lindstrom, Research Director



Spire Security, LLC
P.O. Box 152, Malvern, PA 19355
www.spiresecurity.com

Executive Summary

Web conferencing is becoming a mainstay for business collaboration. As with any new technology, security risks arise amidst new usage scenarios and architectures. The real-time sharing capabilities that make web conferencing a powerful enterprise application also create a level of risk that must be addressed to ensure the enterprise is protected.

The best way to successfully deploy new applications and platforms in an enterprise is to evaluate all aspects of the initial implementation and follow-on usage for security requirements. This white paper discusses some of the specific risks encountered with web conferencing solutions and best practices for adding appropriate security controls.

About Spire Security

Spire Security, LLC conducts market research and analysis of information security issues and requirements. Spire provides clarity and practical security advice based on its "Four Disciplines of Security Management," an operational security model that encompasses identity management, trust management, threat management, and vulnerability management. Spire's objective is to help define and refine enterprise security strategies by determining the best way to deploy policies, people, process, and platforms in support of an enterprise security management solution.

This white paper was sponsored by Cisco Systems. Spire Security maintains its independence regarding the content and assertions that is the product of years of security audit, design, and consulting work.



Best Practices in Web Conferencing Security

Table of Contents

Introduction	1
Risks of Web Conferencing.....	1
Stolen confidential information.....	1
Compromised and exploited systems	2
Fraudulent use.....	2
Goals for Secure Web Conferencing.....	3
Take ownership	3
Comply with standards.....	3
Secure the environment.....	3
Best Practices for Secure Web Conferencing	4
Deployment and Architecture.....	4
Meeting Access	5
In-Meeting Control	5
Content and Information Protection	6
Administration and Management	6
Supplier Security Policies	7
Spire ViewPoint.....	7



Introduction

Enterprises today are dynamic, worldwide businesses with a “round-the-clock” workforce constantly communicating and conducting business. Project teams often comprise numerous people from many parts of the world and at other companies. Customers, prospects and business partners may just as easily come from next door as another hemisphere. The global economy prospers because of its ability to communicate and participate in activities regardless of geographic location.

Web conferencing is all about sharing information and collaborating in real time with many different groups of people. It provides a flexible, dynamic way to work together without worrying about transportation costs or scheduled itineraries. As is typical with new technology, the capabilities that provide the benefit also create a new set of risks. These risks must be understood, evaluated and eventually managed to ensure the integrity of a web conferencing solution.

Risks of Web Conferencing

The general risks of web conferencing are not so much new as they are existing risks that are updated to match the new architectures and deployments of a solution. Security professionals recognize that new applications have particular risks. And web conferencing introduces vulnerabilities specific to its architecture and usage patterns.

Stolen confidential information

Electronic information used for business decisions abounds. Web conferencing enables people to share this data in ways that make sense. But the logical caveat that is often overlooked by IT organizations is that workers need the tools to share information on a “need-to-know” basis. Computer users work in groups of various sizes and types, each with specific collaboration needs. Projected financials, human resources records, trade secrets and product specs provide a sampling of the information that may be at risk.

Before they can minimize leaks, enterprises must first be keenly aware of what is confidential and what isn’t and set policies about how and with whom users may share information. Also, companies should provide tools that enable people to share and protect confidential information, avoiding solutions that potentially expose



confidential information to “non-need-to-knows” perhaps without the user’s knowledge.

Web conferencing services typically post a company’s data to public web sites and host that content – and the meetings themselves – on shared Internet servers. The general accessibility of the servers increases the risk of information theft, particularly if existing controls are ignored by users or are inadequate for addressing the exposure level of the environment. As a result, unwanted users can access both unprotected content and meetings.

Compromised and exploited systems

Collaboration tools may be deployed as standalone solutions or integrated with other applications. For many companies, this means overlaying or inserting new servers, network devices like caching systems, and applications into the computing environment. Others might reconfigure perimeter security devices or trusted systems to provide user access to the conferencing facility.

Depending on a web conferencing solution’s architecture, unauthorized users or hackers can attack or shut down a company’s web conferencing service resulting in denial-of-service due to system failure. Even more significant, inappropriate designs or configuration decisions can become a springboard into the network, resulting in attacks and exploits against any other system and putting the entire enterprise at risk.

Fraudulent use

Applications are often configured to provide maximum access and allowed to exist in a hostile environment unchecked by system controls. This leads to abuse that can result in fraud, which inevitably creates wasteful costs. Former employees may continue

Web Conferencing: A Risky Business?

One organization’s challenges illustrate the risks related to web conferencing. Attorneys and clients of a global law firm needed to share sensitive materials in confidence. The attorneys had been using hosted services publicly available on the Internet. One time, a lurker stayed in a session and accessed the web conferencing account, holding meetings for days afterwards. That convinced the firm to deploy an in-house solution that runs on its own servers – especially important for a law firm, given the confidentiality of its data.

Other scenarios further demonstrate the power and the need for security in web conferencing:

- A defense contractor discussing product specifications with government agencies.
 - Employees of a pharmaceutical firm planning clinical trials and FDA applications.
 - An advisor at a financial services firm and a client reviewing account information.
 - A company’s marketing director sharing competitive data with the sales force.
-

to use a company's web conferencing account, steal data or commit toll fraud by using web conferencing to access voice conferencing services. Other unauthorized users may break in for non-business, competing or alternative business purposes.

Goals for Secure Web Conferencing

Because web conferencing is still relatively young, IT organizations can help define usage scenarios and corresponding security requirements. When it comes to the project itself, IT organizations can develop a strong foundation from which to build expectations by taking ownership, complying with standards and securing the environment.

Take ownership

Because of its usefulness, web conferencing can infiltrate the enterprise from the "bottom up" through many departments. IT organizations are often left to react to the dictated architectures of solutions chosen by these various groups. By taking ownership of the solution, IT organizations can streamline costs and secure their environments.

Comply with standards

Standards work in two ways. First, external standards such as Transport Layer Security (TLS, commonly known as Secure Socket Layer (SSL)), Hypertext Transport Protocol (HTTP) and T. 120 ensure that a solution is interoperable with applications and platforms used inside and outside an organization. Second, corporate standards create a common architecture and conventions that can, through consistent use, be more effective and secure. Each standards scenario offers an opportunity to gain efficacy over time and contribute to ROI.

Secure the environment

In addition to gaining control over the web conferencing solution selection and ongoing maintenance process, it is crucial for the IT organization to define a process that ensures the security of the overall computing environment. One such process is defined below:

- ▶ Identify usage scenarios

Web conferencing applications can include customer demos, sales forecasts, technical support, staff meetings or other scenarios. An

enterprise's combination of applications and users (e.g. employees, customers, and partners) drives decisions around architecture and security.

- ▶ Identify security needs

The functional use of the application drives security requirements. Typically, it is acceptable for users to have open access to external webinars but strong controls are needed on the server side, including permissions, because of a limited ability to control the listener and audience environment. Budget meetings, conversely, include trusted individuals who should be uniquely identified by user credentials.

- ▶ Build security requirements into request for proposal (RFP)

Once an organization understands its usage and security needs, it is important to build those requirements into the RFP – or risk choosing the wrong solution. Each decision maker should help identify the enterprise's unique security requirements.

- ▶ Include security professionals in the evaluation

Seasoned security professionals bring their background in security principles and controls to any new technology decision or architecture. Given their discrete perspective and the benefits of their security knowledge, the IT organization should include them in any solution decision, including web conferencing.

4-Step Security Process

1. Identify usage scenarios
2. Identify security needs
3. Build security into RFP
4. Include security pros

Best Practices for Secure Web Conferencing

Web conferencing provides excellent opportunities for benefits and savings. Controlled deployment and usage ensure the long-term success of the solution. The following best practices provide insight into secure web conferencing for enterprises.

Deployment and Architecture

The first step in protecting confidential information and networked systems is to control the planning and deployment processes. Key steps include:

- ▶ *Retain control* over the architecture decisions and implementation process.

- ▶ *Isolate confidential meetings* in a trusted environment – ideally, your own network – surrounded by firewalls.
- ▶ *Design a solution* that provides for both internal and external servers, depending on usage scenarios and based on level of security requirements for each meeting.
- ▶ *Integrate with voice conferencing* to secure discussions as well as the shared data.
- ▶ *Integrate with directories* to manage and update web conferencing user accounts according to the same security policies applied to other information assets.

Meeting Access

To protect against information leaks, compromised systems and fraud, an IT organization must consider web conferencing capabilities based on all of its usage scenarios. When evaluating security requirements for setup and configuration of controls for specific meetings, a company should consider the following:

- ▶ *Authorize who can attend.* This ensures pre-validation of users, deterring competitors, undesired employees and hackers from breaking into the system.
- ▶ *Hide meetings.* Sometimes, the simple act of not publishing meeting titles means that a content-oriented attack, such as a competitor monitoring sales prospects by reviewing publicly accessible conference listings, becomes less likely to occur. It's also important that meeting IDs, URLs and passwords are not easily guessed.
- ▶ *Authenticate both web and voice access.* This rapidly reduces the chance of attack and limits the ability to penetrate deeply into the application to access shared data.
- ▶ *Limit authentication attempts.* This protects against dictionary or brute-force guessing of passwords, by limiting authentication attempts and locking accounts after a designated number of failed login attempts.

In-Meeting Control

Hosts or administrators can prevent fraud during a meeting through using controls that:

- ▶ *Identify participants,* approving them for proper levels of control of the meeting.

- ▶ *Control meeting access* by screening new entrants, limiting new access attempts, “locking” meetings from additional participants and ejecting users from sessions.
- ▶ *Control participation*, setting permissions for various roles, including speakers, participants and viewers. Also, the host should be able to control “sharing rules” on the type of data or applications that can be shared or should be protected.

Content and Information Protection

When people share confidential information, that content should be controlled as follows:

- ▶ *Control when content is available*. Manage the ability to access information at different points in time before, during and after meetings.
- ▶ *Control to whom it's made available*. Manage the presentation of the data to specific individuals or groups based on the nature and sensitivity of the content.
- ▶ *Secure the transmission*. A web conferencing solution should be able to prevent the transmission of content from being intercepted or monitored, through SSL encryption or a VPN.

Administration and Management

Compromised systems often can be detected through anomalous behavior and appropriate logging. Behind the scenes, administrators should be able to:

- ▶ *Monitor for security events*. Scrutinize activities during meetings and when the application is otherwise available to identify anomalous behavior.
- ▶ *Create real time reports*. Identify and collect information on meetings, meeting participants and usage patterns.
- ▶ *Receive proactive alerts*. Ensure that meetings that are not actively monitored are not ignored when a security event is identified.
- ▶ *Set system policies*. Configure password minimums, meeting ID restrictions, limits on authentication attempts, dial-out limits, password expiration, etc.
- ▶ *Set user access and controls*. Determine which employees or groups can use the system, and at what levels - some might be allowed to set up meetings, and others to attend only.

Supplier Security Policies

The final set of practices encompasses the supplier itself. Look for web conferencing solution providers that demonstrate:

- ▶ *Organizational focus* as evidenced by a defined position on security.
- ▶ *Secure coding practices* during the development process, to limit the likelihood of finding security-compromising software bugs after deployment.
- ▶ *Operational emphasis* on secure implementation throughout the process.

Spire ViewPoint

Enterprise IT environments are constantly growing in complexity and architecture. New applications provide fresh opportunities for efficiency and effectiveness in company-wide operations. Web conferencing is among the applications that can change communication and work habits across an enterprise. But to succeed, it must be secure. There are many different points to consider when securing web conferencing, not only with the solution itself, but also how it is deployed, configured and managed. Some key points are:

- ▶ Architecture decisions help define the level of risk tolerance. The optimal way to ensure security and minimize risk is through a solution that is demonstrably controlled and secure. The best way to demonstrate this control is through a solution that is deployed in-house on a dedicated server.
- ▶ Security professionals must be involved in the design and deployment of the solution. Security professionals have been applying traditional security principles and techniques to new technology for many years. Their ability to evaluate new solutions and implementation architectures provides the kind of security insight necessary for the success of the application.
- ▶ Security should be designed into the solution - not added on or pieced together after the fact. Well-designed security maintains efficiencies and ensures proper management that is critical to the protection of the web conferencing solution, and most importantly, key enterprise information assets.

Although the benefits of web conferencing are contributing to the effectiveness of various organizations across an enterprise, security

is too important to be ignored. Often, businesses wait until an attack or exploit before fully protecting the information. But by then, it's too late. Proactive security ensures optimal protection of this powerful platform.

Contact Spire Security

To comment about this white paper or contact Spire Security, LLC about other security topics, please visit our website at www.spiresecurity.com.

This white paper was sponsored by Cisco Systems. Spire Security maintains its independence regarding the content and assertions that is the product of years of security audit, design, and consulting work.