

The growth of Web conferencing software has inspired concerns about the security of the data, audio, and video information that may be stored and/or transmitted across public and/or private networks during live online sessions or during the administration of such services.

Security concerns can be broken into two general categories – that of potentially sensitive information which may be stored in data warehouses on servers used to act as “front-ends” to Web conferencing solutions, and the actual data that may be transmitted once a live event has been joined (audio, video, real-time content, live chat, etc). Both areas are of significant concern to Web conferencing customers today, particularly those in corporate environments where financial data, corporate strategies, human resource information, and other sensitive data may be stored and/or used.

In response to these security concerns, the Web conferencing industry has typically reacted with standard encryption technologies, commonly available on many e-commerce Web sites today: Secure Socket Layer (SSL) or Hypertext Transfer Protocol over Secure Socket Layer (HTTPS). These technologies work with accepted standards: public/private key encryption, relying on trusted third party providers to ensure the security of the keys. Client software programs (typically Web browsers) negotiate encrypted channels with a server based on secure “keys.” Public keys and private keys are generated using algorithms considered to be unbreakable with today’s technologies. 128-bit or even higher levels of encryption are supported. This technology relies on encryption and decryption of the secured communications at both the client machine and at the server. Each connection to the server therefore requires that a secure channel be negotiated.

In most cases, these technologies work well; Web browsers, the universal end-user access tool for Web conferencing front ends, support such technologies transparently, and make the encryption and security invisible to end users. Browsers handle the client negotiation and encryption/decryption fairly seamlessly. And most Web servers today provide easy implementation steps to enable SSL. While the impact of these additional communication and transactions on network traffic is not insignificant (encryption typically adds overhead to the size and speed of transactions), it is typically not an issue for end users. A slight delay may be noticed by end users as the encryption and decryption transactions at both the client and server take place. But in most cases the data exchanges between client and server are small, brief and “transactional” as opposed to “persistent.” Thus any delays in Web browser to server transactions are barely perceptible, assuming adequate bandwidth is available.

Most Web conferencing providers today rely on SSL and HTTPS for the encryption of “front-end” transactions, such as user logins and management functions, content downloads and uploads, registrations, scheduling, and the like. The iLinc product suite indeed conforms to such standards. The iLinc Communications Center, as an Internet Server Application Program Interface (ISAPI) extension of the popular Microsoft Web server software Internet Information Server (IIS), can be fully secured using server certificates and SSL. With this, by all accepted standards, “front-end” iLinc Communications Center Web conferencing data is entirely secure.

The extension of SSL and/or HTTPS to the second general area of concern with Web conferencing security, however, is not quite as simple. Real-time communications such as audio, video, and synchronous content (such as PowerPoint presentations, Whiteboards, tests or surveys, polling information, text chat, user feedback,

etc.) frequently contain secure information, and thus must also be encrypted. But applying the classic SSL solution to this type of real-time information is more problematic due to the nature of conferencing software: it is real-time information and connections between the client and server are “persistent”. So, the added overhead of negotiating an encrypted channel between every client and the central server for every transaction, can introduce latency, increase packet sizes, increase bandwidth requirements, significantly increase central processing unit (CPU) and processing time required at the server, and essentially inhibit the efficient exchange of real-time data.

As an example, real-time audio communications in Web conferencing products have several characteristics that make them different from standard Web browser type transactions, and as a result, make them inappropriate candidates for classic SSL encryption technologies. First, real-time audio needs to be very low latency in order to enable effective interaction among participants. Typically, delays of more than a second or two, while not an issue for transactions such as logging into a secure server, make real-time communications with audio cumbersome and awkward. For example CNN video interview with an overseas correspondent on a satellite connection, where delays can exceed 5 seconds. Thus, the added overhead of encrypting real-time audio, as well as video and content, poses a different challenge; the encryption must be fast and efficient and additional packet and bandwidth overhead must be kept to a minimum so that latency is kept to an absolute minimum.

Real-time audio connections are not typically one-time transactions (such as a simple get/post transaction as a user logs into a secure site). Instead, real-time audio is a persistent stream of data from one or more Web conferences to the others. Any added overhead or delay or CPU requirements is multiplied by the volume of data

Key Facts:

The iLinc product suite implements AES in a unique fashion that leads the industry in security and efficiency. All real-time communications data is encrypted with a key at the client side prior to being placed on the network. The key for use in this encryption is downloaded from the server using SSL and is thus secured in itself.

The key is then used to encrypt all live session data, which is then passed through the server without decryption, to other clients in live sessions, where it is decrypted and played or displayed.

Where most SSL transactions require the negotiation of a secure channel with the server, iLinc encrypted data is simply passed through the server to the receiving clients. Communications require less overhead, server performance is not affected, and because of the distributed nature of client/server computing, even client side CPU overhead is only modestly affected.

The Bottom Line:

AES represents the latest standard in encryption technology. When combined with SSL for “front-end” communications, the two solutions combine to provide an entirely secure and yet still very efficient method for encrypting all data and transactions in a real-time Web conferencing solution.

and by the number of participants involved. Again, this simply means that efficiency of encryption becomes a critical point for real-time audio, and indeed, for all Web conferencing real-time data. A more efficient method for encryption is in order.

That method is the Advanced Encryption Standard, or AES. The National Security Agency reviewed and approved the current AES encryption standard, and in 2003 the US Government approved the use of AES encryption for classified information. AES has been scrutinized ever since, and is still considered unbreakable today.

The iLinc Hosting Network

The iLinc hosting network provides iLinc partners and customers with a reliable and secure infrastructure for the delivery of Web conferencing services. The iLinc® hosting network is fully redundant and monitored 24 hours a day, 7 days a week, 365 days a year. The network is managed by a team of highly trained and experienced technicians located in Salt Lake City, Utah; Phoenix, Arizona; and Albany, New York.

To assure reliability, scalability, security, and performance, the iLinc hosting network utilizes:

- Multiple private-line, high bandwidth Internet connections
- High-speed SSL-capable load balancing
- Redundant peering arrangements
- Traffic routing
- Network management
- Regularly-scheduled penetration tests and remediation cycles
- Sophisticated diagnostics
- Intrusion prevention
- Host-based intrusion detection
- Firewall separation between hosting network and office network

The primary hosting infrastructure is housed within a 175,000 square-foot datacenter in Arizona. The facility is completely 2N for power and cooling (meaning that it has twice as many uninterruptible power supplies, generators, and air conditioning units as are required for normal operation), and can provide five days of independent power (fuel is maintained onsite, with contracts in place for continual replenishment). It also includes redundant and diverse fiber vaults, power feeds, and carrier connectivity. The facility boasts 24-hour onsite security, badge and fingerprint readers for datacenter access, and video cameras throughout the building.

The hardware and network infrastructure includes:

- Multiple clusters of Intel Xeon-based servers running Linux and Windows
- An Oracle database Real Application Cluster (RAC) implementation
- A cluster of servers providing customer in-session content
- Redundant and Gigabit-capable switches, firewalls, and load balancers, able to push a full 1Gbps of data
- Intrusion-Prevention System (IPS) in front of the infrastructure

Each server is configured in either an active-active cluster or with a failover standby server for full redundancy, and data is mirrored across facilities for optimization and disaster recovery. Network services provided within the infrastructure include authoritative DNS servers, redundant e-mail relays, system administration servers, firewalls, and monitoring servers. All networking hardware is best-of-breed. Connectivity to the application is managed using BigIP Load Balancers also configured for redundant fail-over, providing superior traffic routing capabilities. iLinc conferencing services are delivered on clusters of Intel Xeon-based servers, while the front-end applications are delivered separately by an additional Xeon-based server cluster running Apache on Linux. The systems are continuously monitored for Internet and server availability every 60 seconds on a 24x7 basis, and administrative access is provided through dedicated private connections.

The iLinc ASP delivery solution also implements security at the network and software layers. 128-bit or higher SSL and AES encryption are available for complete end-to-end data encryption services on 100% of conferencing data. The integrity of customers' data is secured using the latest US government standards for data security making iLinc the most complete and secure conferencing application available on the market today.

If you'd like to learn more about about AES, visit this website:

<http://csrc.nist.gov/CryptoToolkit/aes/index.html>

Flexible Options:

iLinc customers may choose to install iLinc software behind their own firewall or to utilize the hosted environment (ASP), which does provide some additional benefits:

- Eliminates the need to purchase hardware or add to infrastructure
- Eliminates the need for an IT department or IT expense
- Provides additional branding features
- Adds conference management system functionality to the iLinc system
- Adds the ability to host off-the-shelf content and custom content providing a blended delivery solution

For More Information:

Demo:

www.ilinc.com/dailydemo

Email:

followup@ilinc.com

Call:

1-800-767-9054