Zoom Security White Paper

May 2013

Zoom offers the first Unified Meeting Experience (UMX), a cloud service that provides a 3-in-1 meeting platform with HD video conferencing, mobility and web meetings. UMX also offers the first available mobile-screen sharing, an innovative hybrid cloud service and works across desktop, tablet, mobile and room systems.

A growing number of businesses, small and large, use Zoom for a variety of use cases – team meetings, sales interactions, marketing events, group mediation, product training and customer support.

Zoom places security as the highest priority in the lifecycle operations of its public and hybrid cloud networks. Zoom strives to continually provide a robust set of security features to meet the requirements of businesses for safe and secure HD meetings.

The purpose of this document is to provide information on the security features and functions that are available with Zoom.

The reader of this document is assumed to be familiar with Zoom functionalities related to video conferencing, web meetings and video chats.

INFRASTRUCTURE

Zoom's communications infrastructure for real-time video, audio and data communications leverages Amazon Web Services. Amazon Web Services provides a highly reliable, scalable, secure infrastructure platform in the cloud that powers hundreds of thousands of businesses in 190 countries around the world.

For information on Amazon EC2, please see http://aws.amazon.com/what-is-aws/
For information on AWS Security, please see http://aws.amazon.com/security/

MULTIMEDIA ROUTERS IN THE CLOUD

A distributed network of low-latency multimedia routers (software) resides on Zoom's communications infrastructure. With these low-latency multimedia routers, all session data originating from the host'sdevice and arriving at the participants' devices is dynamically switched — never stored persistently through the Zoom communications infrastructure.

Zoom sessions are completely temporary and operate analogously to the popularmobile conversation over the public mobile network.

In addition to unique security benefits, Zoom's communications infrastructure also enables an extremely scalable and highly available meeting infrastructure unrestricted by the physical limitations of physical data centers.

THE UNIFIED MEETING EXPERIENCE SECUIRTY

Zoom's security design focuses on five key elements:

1. Role-based user security
2. Meetings security
3. Communicationssecurity
4. Meeting connector security
5. Single sign-on security

1. Role-based user security

The following security capabilities are available to the meeting host:

- Secure log-in
- Start a meeting (with password)
- Schedule meetings (with password)
- Enable wait-for-host to join
- End a meeting
- Lock a meeting
- Chat with an participant or all participants
- Mute/un-mute an participant or all participants
- Expel an participant or all participants
- Enable/disable an participant or all participants to record
- Temporarily pause screen-sharing when a new window is opened

The following security capabilities are available to the administrator:

- Secure login
- Add user and admin to account
- Delete user from account
- Upgrade or downgrade user subscription level
- Review billing and reports

The following security capabilities are available to the meeting participants:

- Secure login
- Mute/unmute audio
- Mute/unmute video

2. Meetings Security

Host authenticated meeting: A host is required to authenticate (via https) to the Zoom site with their user credentials (ID and password) to start a meeting. This ensures access control and audit trails.

Client authenticated meeting: Client authentication process uses a unique per-client, per-session token to confirm the identity of each participant attempting to join a meeting. Each session has a unique set of session parameters that are generated by Zoom. Each authenticated participant must have access to these session parameters in conjunction with the unique session token in order to successfully join the meeting. This ensures session control and security.

Open or password protected meeting: The host can require the participants to enter a password before joining the meeting. This provides greater access control.

Edit or delete meeting: The host can edit or delete an upcoming or previous meeting. This provides greater control over availability of meetings.

Join after host meeting: The host can require the participants to enter the meeting only after the host has started and joined the meeting. This provides greater control of the meeting.

Join before host meeting: The host can allow participants to join before the host. When joining before host, participants are restricted to a 30-minute meeting. This provides greater control of the meeting.

Selective meeting invitation: The host can selectively invite participants via email, IM or SMS. This provides greater control over the distribution of the meeting access information.

In-meeting security: During the meeting, Zoom delivers real-time, rich-media content securely to each participant within a Zoom meeting. All content is shared with the participants in a meeting is only a representation of the original data. This content is encoded and optimized for sharing using a secured implementation as follows:

- Is the only means possible to join a Zoom meeting
- Is entirely dependent upon connections established on a session-by-session basis
- Performs a proprietary encoding process that encodes all shared data
- Can encrypt all screen sharing content using the AES 128 encryption standard
- Can encrypt the network connection to Zoom using 128-bit TLS encryption standard
- Provides a visual identification of every participant in the meeting

Post Meeting Security: Once the meeting is over, no session information is retained on the Zoom multimedia routers or on any participant's devices. If a meeting is recorded, the recording is located on a client machine. Zoom communications infrastructure does not store any recording content.

Meeting Details Security: Zoom retainsevent details pertaining to a session for billing and reporting purposes. The event details are stored at the Zoom secured database and are available to customers for review on theZoom site once they have securely logged-on.

API Security: A set of APIs is available for admins that are approved for use by Zoom. Each customer account managed by the admin will be given a pair of API key and passcode. The API calls are transmitted securely over secure web services and API authentication is required.

3. Communications Security

Communications security: Zoom can secure all session content by encrypting the communications channel between the Zoomclient and the multimedia router using a 128-bit Transport Layer Security (TLS) encryption tunnel.

Connection security: Zoom meeting participants connect to the Zoom communications network via a dedicated logical connection. This connection is strictly controlled by the Zoom client and is dedicated exclusively to session communications – no other tasks outside of what the meeting client allows.

Firewall compatibility: The Zoom client communicates with the multimedia router to establish a reliable and secure connection. At the time of instantiation, the Zoom client will determine the best method for communication. It attempts to connect automatically using udp and tcp port 8801, 8802 and 8804 or HTTPS (port 443/TLS).

Application security: Zoom can encrypt all presentation content at the application layer using the Advanced Encryption Standard (AES) 128-bit algorithm.

4. Meeting Connector Security

Zoom Meeting Connector is a hybrid cloud deployment method which allows a customer to deploy Zoom multimedia router (software) within the company's internal network.

User and meeting metadata are managed in Zoom communications infrastructure, but the meeting itself is hosted in customer's internal network. All real-time meeting traffic including audio, video and data sharing go through the company's internal network. This leverages your existing network security setup to protect your meeting traffic.

5. Single Sign-On (SSO) Security

With SSO, a user logs-in once and gains access to multiple applications without being prompted to log-in again at each of them.

Zoom supports SAML 2.0 which enables web-based authentication and authorization including single sign-on (SSO).SAML 2.0 is an XML-based protocol that uses security tokens containing assertions to pass information about a user between a SAML authority (an identity provider) and a web service (Zoom).

CONCLUSION

A growing number of businesses, small and large, use Zoom meeting services everyday. It is a high quality service for team meetings, sales interactions, marketing events, group mediation, product training and customer support.

Zoom places privacy and security as the highest priority in the lifecycle operations of its communications infrastructure and meeting connector networks.

In addition, Zoom strives to continually providea robust set of security features to achieve its goal of providing the most efficient and secure real-time HD meeting service.