Zoom Encryption

Introduction

The purpose of this document is to provide information on the encryption methods used for the Zoom platform. The goal of our encryption design is to provide the maximum amount of privacy possible while supporting the diverse needs of our client base.

There are several different use cases and potential ways an individual may connect to Zoom. The following document outlines the encryption methods used by potential interfaces to the platform.

When using the Zoom Client

Zoom offers a feature rich client software package for Mac, Windows,iOS, Android, and Linux that leverages a range of encryption technology to assist with user privacy and security. **All customer data transmitted from the client to the Zoom cloud is encrypted in transit using one of the following methods.**

TLS 1.2

For connections between the Zoom client and Zoom's cloud, HTTPS is the preferred method of communication. These connections leverage TLS 1.2 encryption and PKI Certificates issued by a trusted commercial certificate authority. Some of the common use cases include signing into the client, scheduling a meeting, chatting, polling, sharing files, and in-meeting Q&A. TLS 1.2 also serves as a backup protocol for other communication streams such as meeting real-time content.

AES

For use cases such as meeting real-time content (video, voice, and content share), where data is transmitted over User Datagram Protocol (UDP), we use AES-256 in ECB mode to encrypt these compressed data streams. We expect to upgrade this soon to AES-256 GCM. Additionally, for video, voice, and content share encrypted with AES, once it's encrypted, it remains encrypted as it passes through Zoom's meeting servers until it reaches another Zoom Client or a Zoom Connector, which helps translate the data to another protocol.

SRTP

Our Zoom Phone product uses Secure Real-time Transport Protocol leveraging AES-128-ECB to encrypt and protect phone conversations in transit to and from our data centers. This functionality will soon be upgraded to AES-256 GCM.

When using a Web Browser

Zoom offers a web interface that provides a number of rich features including a complete management console, access to cloud recordings, an extensive set of API endpoints, and a web-based client for meetings. **All customer data transmitted from a web browser to the Zoom Cloud -- including on our website and via our web meeting client -- is encrypted in transit using one of the following methods.**

TLS 1.2

Connections to the Zoom website leverage TLS 1.2 encryption and PKI Certificates issued by a trusted commercial certificate authority. Through this portal, individuals can access a range of features associated with their Zoom account, manage its operations, and integrate with other systems. The strength of encryption and specific ciphers used for connections to the website will depend on the browser used to access the site and the results of the common encryption method negotiated.

AES-256

Beyond the TLS encryption, Zoom's website leverages additional encryption in specific use cases. For example, customer data including cloud recordings, chat history, and meeting metadata are stored at rest using AES-256 GCM with keys managed by a key management system (KMS) in the cloud. When users connect to a meeting using the Zoom web client, leveraging web assembly, Zoom will send and receive meeting real-time content (video, voice, and content share) via User Datagram Protocol (UDP), directly from the meeting server encrypted with AES-256 ECB.

When using a 3rd Party Device / Service

As an open platform, Zoom offers methods for a range of services and devices to connect with our system. This includes support for use cases such as an H323/SIP device connecting to a Zoom meeting, broadcasting over popular streaming services, and calling into a meeting with a standard phone line (i.e., not via our app). As these integrations must leverage communication protocols native to the specific 3rd party device or server, encryption methods will be limited to what's possible on that device. **Therefore, while we encourage the use of encryption with third party devices and services, customer data transmitted via these devices and services may not be encrypted in transit to and from Zoom's system. Regardless, once that data reaches Zoom's system, it is encrypted at that point and remains encrypted the entire time it is transiting our system.** If a third party device does support encryption, it will likely be encrypted using one of the following methods.

TLS 1.2

If supported by the device, Zoom will negotiate over TLS 1.2. For example, if a SIP device has enabled encryption, TLS will be used for signaling.

AES

If supported by the device, Zoom will negotiate encrypting meeting content such as video, audio and screen share using AES on a SIP or H323 endpoint.

Conclusion

In today's world where collaboration takes place across several mediums and communications platforms, Zoom is committed to protecting our customers. When third party devices enter the equation, we offer the ability to extend encryption to a wide range of integrations outside of our platform. Within our platform, we ensure customer content is encrypted.