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 mee**Wd (omv)11.sraging eb in gs, an ex da dar1s0mcl

When using a 3rd Party Device / Service