Zoom 加密

简介

本文档旨在说明 Zoom 平台所使用的加密方法。我们的加密方式旨在最大程度保护隐私，同时满足用户的多样化需求。

在不同使用案例中，个人可通过许多不同的方法连接至 Zoom。以下文档简要介绍各种平台接口可能使用的加密方法。

使用 Zoom 客户端时

Zoom 为 Mac、Windows、iOS、Android 和 Linux 平台提供功能丰富的客户端软件包，采用多样化加密技术帮助确保用户的隐私性和安全性。**从客户端传输至 Zoom 云的所有客户数据将会在传输过程中使用以下一种方法进行加密。**

TLS 1.2

对于 Zoom 客户端与 Zoom 云之间的连接，HTTPS 是首选的通信方法。这些连接通过 TLS 1.2 加密以及可信商业证书颁发机构颁发的 PKI 证书进行安全保护。其常见使用案例包括：登录客户端、安排会议、聊天、投票、共享文件和会议中问答。TLS 1.2 也作为会议实时内容等其他通信流的备用协议。

AES

对于通过用户数据报协议 (UDP) 传输数据的使用案例，例如会议实时内容（视频、语音和内容共享），我们采用 ECB 模式 AES-256 来加密这些压缩数据流。此方法预计不久将会升级至 AES-256 GCM。此外，对于使用 AES 加密的视频、语音和内容共享，这些数据在启用加密后将会在 Zoom 会议服务器传输期间保持加密状态，直至到达另一个 Zoom 客户端或 Zoom 连接器，从而有助于数据协议转换。

SRTP

我们的 Zoom Phone 产品采用安全实时传输协议，利用 AES-128-ECB 来加密和保护往返于我们数据中心的通话内容。此功能不久将升级至 AES-256 GCM。

使用网络浏览器时

Zoom 提供许多功能丰富的网络接口，包括全面管理控制台、云录制访问接口、多样化 API 端点和基于网络的会议客户端。**从网络浏览器传输至 Zoom 云的所有客户数据（包括网站数据和流经网络会议客户端的数据）将会在传输过程中使用以下一种方法进行加密。**

TLS 1.2

Zoom 网站连接会通过 TLS 1.2 加密以及可信商业证书颁发机构颁发的 PKI 证书进行安全保护。通过此门户，个人可访问各种 Zoom 账户相关功能，管理操作并集成其他系统。网站连接时所使用的加密强度和具体密码将取决于访问站点时所使用的浏览器以及常用加密方法协商结果。

AES-256

除了 TLS 加密，Zoom 网站还在特定使用案例中利用其他加密方法。例如，云录制、聊天历史记录和会议元数据等客户数据会采用 AES-256 GCM 方式进行静态存储，其密钥由云中的密钥管理系统 (KMS) 进行管理。当用户使用 Zoom 网络客户端连接到网络集会会议时，Zoom 将会使用 AES-256 ECB 通过用户数据报协议 (UDP) 直接向/从加密会议服务器发送/接收会议实时内容（视频、语音和内容共享）。

使用第三方设备/服务时

作为开放平台，Zoom 提供许多将各种服务和设备连接到我们系统的方法。所支持的使用案例包括：将 H323/SIP 设备连接到 Zoom 会议，通过流行的流媒体服务进行广播，以及使用标准电话线呼叫会议（即，不是通过我们的应用）。由于这些集成必须采用特定于第三方设备或服务器的本地通信协议，加密方法将受限于该设备可用的协议。**因此，尽管我们鼓励采用第三方设备和服务进行加密，但是通过这些设备和服务传输的客户数据在往返于 Zoom 系统期间将不会进行动态加密。然而，这些数据在到达 Zoom 系统之后，将会立即进行加密，并在整个系统数据传输期间保持加密状态。**如果第三方设备不支持加密，可能会采用以下一种方法进行加密。

TLS 1.2

如果设备支持，Zoom 将通过 TLS 1.2 进行协商。例如，如果 SIP 设备已启用加密，则将会使用 TLS 进行信号发送。

AES

如果设备支持，Zoom 将在 SIP 或 H323 端点上使用 AES 协商视频、音频和屏幕共享等加密会议内容。

总结

在如今需要满足各种媒介和通信平台协作需求的环境下，Zoom 致力于为客户保驾护航。在涉及第三方设备的情况下，我们还可以将加密功能扩展到平台外的多样化集成模块之中。我们将竭力确保平台中客户内容的私密性。