Шифрование Zoom

Введение

Цель настоящего документа — предоставить информацию о методах шифрования, которые используются на платформе Zoom. Цель нашей системы шифрования — предоставить максимально возможный уровень конфиденциальности при поддержке разнообразных потребностей нашей клиентской базы.

Существует несколько различных сценариев использования и возможных способов подключения пользователей к платформе Zoom. В этом документе представлены методы шифрования, которые используются в различных способах подключения к платформе.

Работа с клиентом Zoom

Zoom предлагает многофункциональный пакет клиентского программного обеспечения для компьютеров Mac и устройств с операционными системами Windows, iOS, Android и Linux, который использует широкий перечень технологий шифрования для обеспечения конфиденциальности и безопасности пользователей. **Все данные клиентов, передаваемые из клиентского приложения в облако Zoom, шифруются при передаче с помощью одного из следующих методов.**

TLS 1.2

При создании соединений между клиентом Zoom и облаком Zoom предпочтительным способом связи является протокол HTTPS. Эти соединения используют шифрование TLS 1.2 и сертификаты PKI, выданные доверенным коммерческим центром сертификации. Некоторые из распространенных сценариев использования — вход в клиентское приложение, планирование конференции, общение в чате, участие в опросах, предоставление общего доступа к файлам и организация сеансов вопросов и ответов в конференции. TLS 1.2 также выступает в качестве резервного протокола для других коммуникационных потоков, например, для передачи содержимого конференций в реальном времени.

AES

В таких сценариях использования, как передача содержимого конференции в реальном времени (видеоданных, голосовых данных и материалов для совместного использования), где осуществляется передача данных по протоколу передачи датаграмм UDP, мы используем шифрование AES-256 в режиме ECB для защиты этих сжатых потоков данных. В ближайшее время этот метод шифрования будет улучшен до AES-256 GCM. Кроме того, после шифрования видеоданных, голосовых данных и материалов для совместного использования по стандарту AES они остаются зашифрованными при прохождении через серверы конференции Zoom до тех пор, пока не достигнут другого клиента Zoom или коннектора Zoom, осуществляющего трансляцию данных в другой протокол.

SRTP

Наш продукт Zoom Phone работает с защищенным протоколом транспортного уровня в реальном времени (SRTP), который использует шифрование AES-128-ECB для защиты пакетов голосовых данных при обмене с нашими центрами обработки данных. В ближайшее время этот функционал будет улучшен до AES-256 GCM.

Работа в браузере

Сервис Zoom оснащен веб-интерфейсом, который предлагает множество полезных функций, в том числе, полноценную консоль управления, доступ к записям в облаке, широкий набор конечных точек API и веб-клиент для проведения конференций. **Все пользовательские данные, передаваемые из браузера в облако Zoom, — в том числе, на нашем веб-сайте и через веб-клиент для проведения конференций — шифруются при передаче с помощью одного из следующих методов.**

TLS 1.2

Подключения к веб-сайту используют шифрование TLS 1.2 и сертификаты PKI, выданные доверенным коммерческим центром сертификации. Через этот портал пользователи могут получить доступ к различным функциям, связанным с их учетной записью Zoom, управлять операциями и выполнять интеграции с другими системами. Надежность шифрования и определенных ключей, используемых для подключения к веб-сайту, зависит от браузера, который используется для доступа к сайту, и результатов согласования общего метода шифрования.

AES-256

Помимо шифрования TLS, веб-сайт компании Zoom в определенных сценариях может использовать дополнительное шифрование. Например, клиентские данные, в состав которых входят записи в облаке, история чатов и метаданные конференций, шифруются при хранении по стандарту AES-256 GCM с использованием облачной системы управления ключами шифрования (KMS). При подключении пользователя к конференции с помощью веб-клиента Zoom, использующего веб-сборку, платформа Zoom будет отправлять и получать содержимое конференции в реальном времени (видеоданные, голосовые данные и материалы для совместного использования) по протоколу передачи датаграмм UDP непосредственно с сервера конференции, использующего шифрование по стандарту AES-256 ECB.

Работа с устройствами / сервисами сторонних разработчиков

Zoom является открытой платформой и поддерживает другие методы подключения к системе, доступные широкому перечню сервисов и устройств. В число таких сценариев использования входит подключение устройств H323/SIP к конференции Zoom, вещание в популярных сервисах потоковой передачи данных и участие в конференции по обычной телефонной линии (не через приложение). Так как эти интеграции должны использовать «родные» протоколы связи определенных сторонних устройств или серверов, возможности шифрования будут ограничены перечнем методов, поддерживаемых такими устройствами. **Таким образом, хотя мы поощряем использование шифрования с устройствами и сервисами сторонних разработчиков, клиентские данные, передаваемые с помощью таких устройств и сервисов, могут оказаться незашифрованными в ходе обмена с системой Zoom. В любом случае, данные шифруются немедленно при попадании в систему Zoom и остаются зашифрованными на всех этапах передачи в рамках системы.** Если устройство стороннего разработчика поддерживает шифрование, данные, скорее всего, будут зашифрованы с помощью одного из следующих методов.

TLS 1.2

Zoom будет выполнять согласование по протоколу TLS 1.2, если этот протокол поддерживается устройством. Например, если на SIP-устройстве включено шифрование, для передачи сигнала будет использоваться протокол TLS.

AES

Zoom будет выполнять согласование шифрования содержимого конференции, например, видео-, аудиопотоков и демонстрации экрана, с помощью стандарта шифрования AES на конечной точке SIP или H323.

Заключение

В современном мире, где совместная работа ведется сразу на нескольких носителях и коммуникационных платформах, компания Zoom прилагает все возможные усилия для обеспечения безопасности своих клиентов. Когда дело касается устройств сторонних производителей, мы предлагаем возможность расширения шифрования за счет богатого ассортимента интеграций за пределами нашей платформы. В рамках своей платформы мы обеспечиваем шифрование содержимого, предоставляемого нашими клиентами.