Os fatos sobre a Zoom e a criptografia para reuniões/webinars

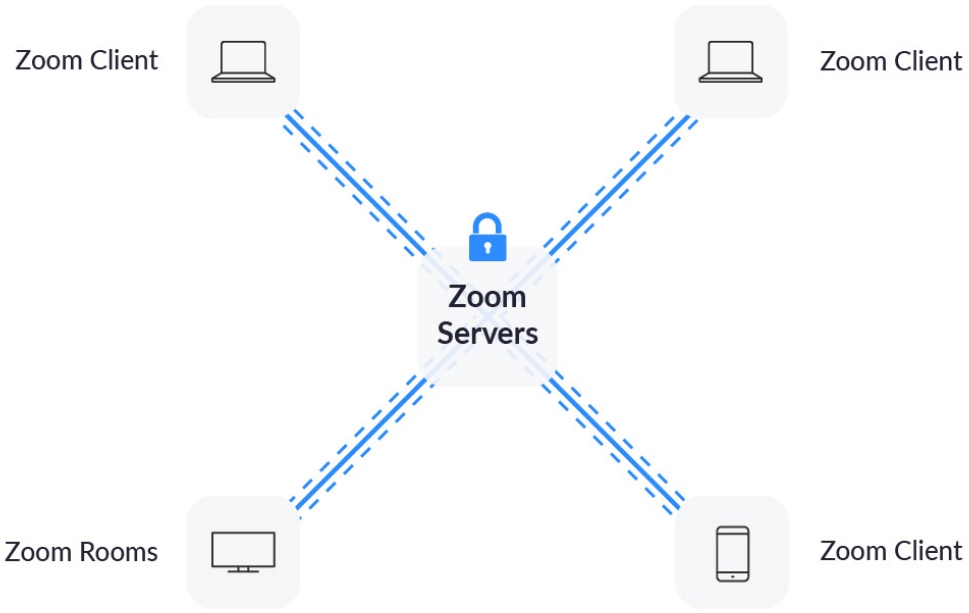
Tendo em vista o interesse recente nas nossas práticas de criptografia, queremos começar pedindo desculpas pela confusão que causamos ao sugerir incorretamente que as reuniões da Zoom podiam usar criptografia de ponta a ponta. O objetivo da Zoom sempre foi utilizar criptografia para proteger o conteúdo no maior número possível de cenários. Foi nesse sentido em que empregamos o termo "criptografia de ponta a ponta". Nunca tivemos a intenção de enganar nossos clientes, mas reconhecemos que há uma discrepância entre a definição comumente aceita para "criptografia de ponta a ponta" e a forma como a usamos. Este blog pretende corrigir essa discrepância e esclarecer exatamente como criptografamos o conteúdo que trafega na nossa rede.

O objetivo do nosso design de criptografia é fornecer a máxima privacidade possível, além de oferecer suporte às diversas necessidades da nossa base de clientes.

Para esclarecer, em uma reunião não gravada em que todos os participantes usam clientes Zoom, criptografamos todo o conteúdo de vídeo, áudio, compartilhamento de tela e chat no cliente emissor, e ele só é descriptografado quando alcança os clientes receptores.

Os clientes Zoom incluem:

- Um laptop ou computador executando o aplicativo Zoom
- Um smartphone usando nosso aplicativo Zoom
- Zoom Room



Nesse cenário, quando todos os participantes estão usando o aplicativo Zoom, nenhum conteúdo do usuário fica disponível para os servidores ou funcionários da Zoom durante o processo de transmissão.

A Zoom oferece suporte a um ecossistema diversificado de canais de comunicação, a fim de permitir que nossos usuários se conectem de várias maneiras. Quando os usuários acessam reuniões na Zoom por meio de dispositivos que não usam o protocolo de comunicação da Zoom de forma nativa, como um telefone (conectado via linha telefônica tradicional em vez do aplicativo) ou sistemas baseados em salas SIP/H.323, a criptografia da Zoom não pode ser aplicada diretamente por esse telefone ou dispositivo. Nosso objetivo é manter os dados criptografados o máximo possível durante todo o processo de transmissão. Para isso, criamos clientes especializados que fazem a conversão entre nossas reuniões criptografadas e os sistemas legados. Eles são chamados de Conectores Zoom e incluem:

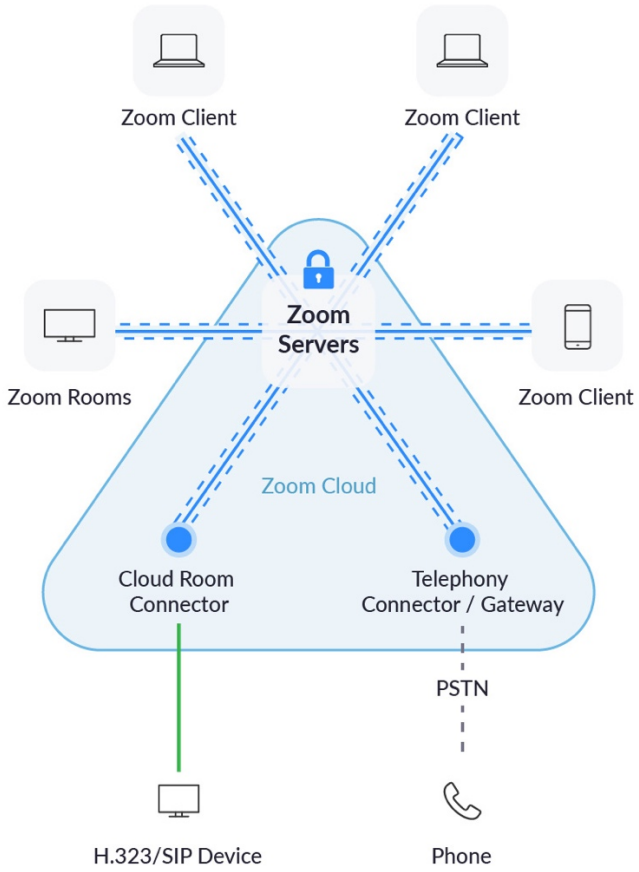
- Conector de telefonia Zoom
- Conector de sala de conferências Zoom
- Conector Skype for Business
- Conector de gravação em nuvem
- Conector de transmissão ao vivo

Esses conectores são clientes Zoom que operam na nuvem da Zoom. O conteúdo permanece criptografado em cada conector, e, quando possível, criptografamos os dados entre cada conector e o destino final (como um sistema de sala que não seja da Zoom).

Os conectores também podem ser convidados para a reunião, mediante solicitação do anfitrião, para ajudar na execução dos serviços. Exemplos disso incluem o Conector de transmissão ao vivo – um cliente Zoom que pode converter o conteúdo da reunião em um formato de transmissão ao vivo e pode ser usado em outros serviços de transmissão na Web.

Acreditamos na importância da criptografia de conteúdo entre clientes, mesmo no cenário em que os Conectores são necessários, pois isso reduz o número de sistemas na Zoom com acesso ao conteúdo do cliente e serve como uma defesa em profundidade.

Para garantir que todo esse processo atenda às necessidades dos nossos clientes o tempo todo e em todo o mundo, a Zoom atualmente mantém o sistema de gerenciamento de chaves para esses sistemas na nuvem. É importante ressaltar que o Zoom implementou controles internos robustos e validados para impedir o acesso não autorizado a qualquer conteúdo que os usuários compartilhem durante as reuniões, incluindo, entre outros, conteúdo de vídeo, áudio e chat. **A Zoom nunca criou um mecanismo para descriptografar reuniões ao vivo para fins de interceptação legal nem temos meios para inserir nossos funcionários ou outras pessoas em reuniões sem que isso seja refletido na lista de participantes.**



Para aqueles que desejam um controle adicional das suas chaves, existe uma solução local para toda a infraestrutura da reunião. Além disso, disponibilizaremos uma solução ainda este ano para permitir que as organizações usem a infraestrutura de nuvem da Zoom, mas hospedem o sistema de gerenciamento de chaves no seu próprio ambiente. Os clientes corporativos também têm a opção de executar determinadas versões dos nossos conectores nos próprios data centers caso desejem gerenciar o processo de descriptografia e conversão.

Estamos comprometidos em fazer o certo pelos usuários quando se trata de segurança e privacidade e entender a importância do momento atual. Com hospitais, universidades, escolas e outras organizações em todo o mundo contando com a Zoom para permanecerem conectados e operacionais, termos orgulho do trabalho que fizemos para proteger os dados dessas instituições essenciais por meio de criptografia e esperamos compartilhar mais informações sobre nossas práticas de segurança em breve.