La popular plataforma de mensajería social Discord ha informado que está lanzando un nuevo protocolo personalizado de cifrado de extremo a extremo (E2EE) para proteger las llamadas de audio y video.

Este protocolo ha sido denominado DAVE, que significa *«Cifrado de extremo a extremo de audio y video de Discord»* («E2EE A/V» en inglés).

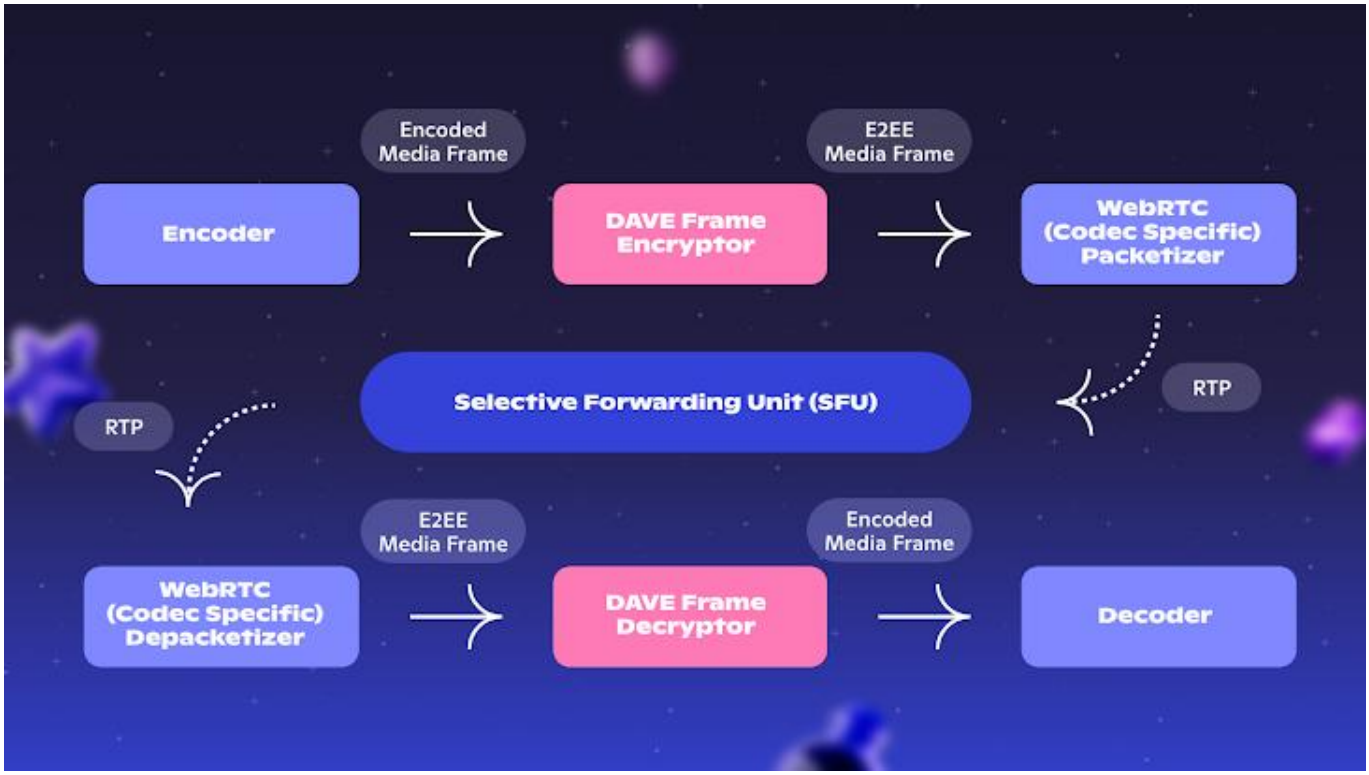
Como parte de la actualización introducida la semana pasada, se espera que las comunicaciones de voz y video en mensajes directos (DMs), DMs grupales, canales de voz y transmisiones en vivo (Go Live) migren al uso del protocolo DAVE.

Sin embargo, es importante mencionar que los mensajes escritos en Discord no estarán cifrados y seguirán sujetos a las políticas de moderación de contenido de la plataforma.

> *«Cuando consideramos implementar nuevas funciones de privacidad como el cifrado E2EE para audio y video, lo hacemos teniendo en cuenta la seguridad. Por eso la seguridad está integrada en nuestro producto y nuestras políticas, y por esa razón los mensajes de texto en Discord no están cifrados»*, explicó Discord.
>
> *«Los mensajes seguirán sujetos a nuestro enfoque de moderación de contenido, lo que nos permitirá continuar brindando protecciones de seguridad adicionales».*

El protocolo DAVE es auditado públicamente y ha sido evaluado por Trail of Bits. Utiliza WebRTC con transformaciones codificadas y Seguridad de Capa de Mensajes (MLS) para cifrado y el intercambio de claves en grupos (GKE).

Esto permite que los fotogramas de medios, excluyendo los metadatos del códec, se cifren una vez codificados y se descifren antes de ser decodificados por el receptor.



> *«Cada fotograma se cifra o descifra utilizando una clave simétrica específica para cada remitente. Esta clave es compartida por todos los participantes de la sesión de audio y video, pero es desconocida para cualquier persona ajena a la llamada, incluido Discord»,* indicó Discord.

El uso de MLS, además, permite que los usuarios se unan o salgan de una sesión de audio o video en Discord sin que los nuevos participantes puedan descifrar los medios enviados antes de unirse, ni que los usuarios que se van puedan acceder a los medios futuros.

> *«El cifrado de transporte de Discord para audio y video entre el cliente y nuestra unidad de reenvío selectivo (SFU) se mantiene, lo que garantiza que solo se retransmitan los datos de audio y video de los participantes autenticados»*, señaló Discord.

> *«Aunque la SFU continúa procesando todos los paquetes de la llamada, los datos de audio y video dentro de cada paquete están cifrados de extremo a extremo, por lo que la SFU no puede descifrarlos».*

Este avance se produce pocos días después de que la Asociación GSM (GSMA), el organismo que regula el desarrollo del protocolo de Servicios de Comunicaciones Enriquecidas (RCS), anunciara que está trabajando para implementar el cifrado de extremo a extremo para proteger los mensajes entre dispositivos Android y iOS.