Seguridad en servicios de mensajería instantánea

Unas de las herramientas más utilizadas por organizaciones para realizar su labor política son los servicios de mensajería instantánea. A diferencia de otros tipos de mensajería cuyas vías recorren el ciberespacio, la mensajería instantánea permite comunicarse de forma rápida, ágil y segura… o al menos esto último se cumpliría si supiéramos elegir bien estas herramientas.

Probablemente nada haya sido más útil para las fuerzas del orden a la hora de detener a militantes y desbaratar manifestaciones u otro tipo de actividades que el mal uso de los servicios de mensajería instantánea o el uso de servicios inseguros para comunicarse y organizar dichas actividades.

En el artículo de hoy, por tanto, pretendemos dar una respuesta a esta problemática que por ser atajada de manera insuficiente, le ha costado muy cara a los movimientos revolucionarios en los últimos años.

Para ello, hemos organizado esta guía de tal forma que sea didáctica, no requiera conocimientos avanzados para ser

comprendida y transmita de manera clara cuáles son las ventajas de cada servicio de mensajería y en qué contexto es mejor utilizar cada uno de ellos. Empezaremos, pues, con la explicación de unos conceptos fundamentales para comprender el funcionamiento de la mensajería instantánea y sus tipologías. Después, haremos un repaso por las mejores alternativas que hemos considerado, explicando las ventajas y desventajas de cada una, así como sus características y los ámbitos y casos de uso a los que mejor se ajustan. También problematizaremos sobre los límites inherentes a los medios de mensajería instantánea, ya que no son medios infalibles, por lo que hay que usarlos con respeto y responsabilidad a la hora de compartir contenido sensible a través de ellos.

Topologías

Cliente-Servidor

El diseño Cliente-Servidor es el método más sencillo y usado en la comunicación entre dispositivos. Por un lado, existe un servidor, que no es otra cosa que una computadora preparada específicamente para gestionar peticiones de

otras máquinas y darles respuesta. Por otro lado, existirían los clientes, que serían máquinas (habitualmente computadoras personales, smartphones, etc.) que se dirigen al servidor para hacer peticiones o solicitar servicios.

Pongamos un ejemplo. Cuando se usan Whatsapp o Telegram, se escriben mensajes en el smartphone y cuando se pulsa el botón de envíar, el smartphone traslada el mensaje al servidor de Whatsapp o Telegram y este envía dicho mensaje al usuario que corresponda. Así, el servidor actúa como intermediario entre los usuarios finales.

Otra característica muy a tener en cuenta sobre esta topología y que nos parece fundamental para comprender algunos servicios de mensajería de los que hablaremos más abajo, es que cliente y servidor pueden ser totalmente independientes. Por ejemplo, Whatsapp es una aplicación monolítica, fuertemente dependiente de su servidor: para usar el servidor de Whatsapp solo puedes usar la aplicación oficial de Whatsapp. En el lado contrario, estaría Matrix, donde el servidor y la aplicación son totalmente independientes. Esto significa que para chatear en un servidor Matrix puedes escoger entre varias aplicaciones creadas por la comunidad, del mismo modo que puedes elegir entre varios servidores gestionados por empresas, fundaciones, gobiernos o personas independientes; cada uno

con sus propios intereses y objetivos.

Ventajas:

- Es el diseño más simple y fácil de desarrollar y desplegar.

- Al tener un servidor central al que dirigirse, los datos se transmiten más rápido sin tener que andar dando vueltas entre varios nodos.

- No es necesario que los clientes (usuarios) estén conectados al mismo tiempo. El servidor almacena los mensajes y los envía a los usuarios cuando están conectados a la red.

Desventajas:

- Centralización: Si cae el servidor, no hay manera de continuar con la comunicación entre los clientes. Esto implica que el servidor es un punto de fallo crítico, pues toda la comunicación no puede realizarse sin su concurso. Además, si el servidor es comprometido por

un atacante, puede tener acceso a toda la información de los usuarios y a los mensajes (aunque pueden estar cifrados).

- Es necesario confiar en el servidor central, ya que, al pasar toda la información por él, se le está dando poder absoluto sobre la información misma.

Peer-to-Peer

El diseño Punto-a-Punto o Peer-to-Peer (P2P a partir de ahora) es un tipo de topología que, a deferencia de la topología Cliente-Servidor, no dispone de un servidor entre los clientes, realizándose la comuncación directamente entre ellos. Es cierto que a veces se necesita de un servidor central para que gestione las conexiones entre los clientes, pero una vez gestionada dicha conexión, el servidor ya no actúa más como intermediario entre la comunicación.

Ventajas:

- No se depende de un servidor central y, por tanto, no existe un único punto de fallo que pueda interrumpir la

comunicación entre los nodos.

- En general, cualquiera puede unirse a una red y convertirse en un elemento más de ésta.

- Permite una mayor soberanía en la gestión de la información de cada cliente (o nodo), ya que no se depende de la gestión por un servidor central.

Desventajas:

- La comunicación es más compleja, problemática y requiere que ambos nodos estén conectados a la red al mismo tiempo. Esto suele resultar en un peor servicio a la hora de intercambiar mensajes, retrasando su entrega o perdiéndose mensajes durante el tránsito. Además expone nuevos retos de diseño más complejos que llevan a haber tardado más en publicar este modelo como válido.

Malla

La topología en malla no es más que una topología P2P, pero en la que los nodos o clientes de la red pueden reenviar mensajes a otros nodos de la red. De nuevo, no existe un servidor central y toda la gestión del reenvío de mensajes recae sobre los clientes de la red. Sus ventajas y desventajas son prácticamente las mismas que en una topología P2P.

Ventajas:

- Los nodos de la red se apoyan unos en otros para hacer llegar los mensajes a los demás (algo muy útil cuando la distancia es un obstáculo).

Desventajas:

- Acrecenta la complejidad del servicio y, por tanto, acrecenta los problemas en la robustez de la red.

Otras cuestiones técnicas

Autoalojar un servidor

Autoalojar o autohostear un servidor significa que cualquiera con los conocimientos suficientes puede levantar un servidor propio y gestionarlo a su manera. Esta es una capacidad muy positiva cuando se trata de preservar la soberanía sobre la información, ya que el servidor es propio y, por tanto, no hace falta confiar en un tercero. Por poner un par de ejemplos, un servidor **no autoalojable** sería el servidor de Whatsapp, ya que es de código cerrado y propiedad de Facebook Inc., mientras que un servidor **autoalojable** sería cualquiera de código abierto, como Prosody (un software de servidor para el protocolo XMPP).

Para autoalojar un servidor, hay dos opciones. Por un lado, se puede utilizar una máquina propia, abriendo los correspondientes puertos del router doméstico o pasando el tráfico, por ejemplo, a través de Tor. Por otro lado, se puede contratar un VPS (Virtual Private Server) de algun proveedor (Amazon AWS, OVH, etc.) y desplegar ahí el servidor. Sin embargo, contratar un VPS implica tener que proveer una serie de datos personales (cuenta bancaria, a veces documentación legal, nombres, etc.) que podrían ser

reclamados por las autoridades llegado el caso y ser cedidos por el proveedor del VPS (Amazon, OVH o quien sea). Ante esto, hay que saber bien cuándo conviene contratar un VPS y cuándo es mejor alojar el servicio sobre una infraestructura propia.

Cifrado punto a punto

El cifrado punto a punto (End-to-End-Encription o E2EE) es un tipo de cifrado que, tal y como dice su nombre, cifra los mensajes a nivel de cliente. Es decir, que el mensaje se cifra en la aplicación cliente y luego se envía al servidor central o al otro cliente, según la topología. Este tipo de cifrado es realmente importante cuando en el servicio de mensajería interviene un servidor central, porque no permite al servidor conocer el contenido del mensaje. Existen otros tipos de cifrado que sí permiten al servidor conocer el contenido del mensaje y esto, obviamente, es problemático. También queremos remarcar que el cifrado E2EE **no asegura una completa privacidad o anonimato**. Aunque esto depende de cada protocolo de comunicación, cifrar el contenido del mensaje no protege frente a otros datos que se pueden extraer como pueden ser: hora de envío del mensaje, localización GPS de una foto, identificador del usuario, identidad del servidor, etc.; éstos son los llamados

metadatos y hay que tener en cuenta su existencia.

Seguridad de la información

Cuando se trata de mantener la seguridad de la información, hay tres dimensiones que son fundamentales. Aplicadas a los servicios de mensajería, corresponderían a:

- **Confidencialidad:** los mensajes solo pueden ser leídos por sus destinatarios legítimos. Para preservar esta dimensión, se utilizan técnicas de cifrado.

- **Integridad:** los mensajes no deberían poder ser alterados y deberían llegar al destinatario en las mismas condiciones en las que fueron enviados. Hay varias formas de preservar esta dimensión, pero las más usadas son las firmas digitales y los hashes (o resúmenes).

- **Disponibilidad:** es la dimensión que trata de que el servicio esté disponible y no se interrumpa la mayor parte posible del tiempo. Existen una infinidad de técnicas para ello y quedan bastante alejadas del campo

de los servicios de mensajería, por lo que no serán tratadas aquí.

Centralización y descentralización

La centralización, cuando se habla en lenguaje telemático, significa, *grosso modo*, que solo existe un servidor (o grupo de servidores que actúan como uno solo) al que las aplicaciones clientes deben dirigirse. Un servicio descentralizado, por el contrario, es aquel en el que participan más de un servidor, pudiendo federarse entre sí. Un servicio descentralizado también puede existir cuando no hay servidores de por medio y la conexión es directa entre los nodos, aunque a este tipo de situación se le conoce mejor como un servicio *serverless* o sin-servidor.

Un servicio centralizado tiene como ventaja principal la mejor gestión de la información del servicio, porque al estar centralizado, no se depende de otras partes que puedan retrasar o obstaculizar dicha gestión. Sin embargo, un servicio descentralizado es más resiliente, porque no depende de un único servidor que, de fallar, dejaría a los usuarios sin servicio.

Servidor, término problemático en la guía

Tras revisar la guía, hemos comprendido que a la hora de usar la palabra servidor, pueden resultar confusiones. Hay que diferenciar entre, por un lado, el servidor como software y, por otro lado, el servidor como dominio. Diferenciarlo es fácil:

- Un servidor como software es, por ejemplo, Synapse para el protocolo Matrix. Es un software o programa que puede desplagarse en una máquina para implementar todas las funciones del servidor y dar servicio a usuarios.

- Un servidor como dominio, en cambio, es el servidor concreto (físico, una máquina) y su nombre. Por ejemplo, *matrix.org* sería un dominio que corre un servidor Synapse y *feneas.org* sería otro dominio corriendo Synapse.

En general, cuando hablemos de que una aplicación de mensajería **dispone de varias implementaciones** de servidores, nos referiremos a que hay varios software de

servidor que pueden utilizarse para desplegar un servicio. Va de la mano que, si existen varias implementaciones de servidor como software, entonces también existirán muchos dominios que los implementen.

Sistemas de mensajería a evitar

Whatsapp y Telegram

WhatsApp y Telegram son dos de las aplicaciones más usadas por todo tipo de usuarios y, por desgracia, muy usados en las organizaciones políticas del proletariado. Ambas son propiedad de empresas que atienden a sus intereses privados lucrativos, donde es precisamente la información lo primordial dentro de su modelo de negocio.

En el caso de WhatsApp, el código del cliente y el servidor son cerrados, para Telegram en cambio, sólo el código del servidor está cerrado. Al no saber cómo funcionan internamente estos servicios, pero sabiendo claramente que lo que les interesa a estar corporaciones es la información, no hay razón alguna para confiar en estos medios de

comunicación, más aún si se trata de organizar y hablar sobre cuestiones sensibles, en términos políticos. Añadido a ésto, en ambos casos la ausencia del código del servidor imposibilita el autoalojamiento del servicio, por lo que al ser una red centralizada, cuando el servidor esté caído la comunicación queda interrumpida; WhatsApp ya es famoso por tener repetidas caídas de su servicio.

En cuanto a la privacidad, es bien sabido que el cifrado de estas aplicaciones tiene fallas intencionadas, pues varias han sido las veces que se ha reconocido poder acceder a los mensajes en caso de que las autoridades lo requieran.

Resumiendo, es altamente recomendable no utilizar o minimizar el uso de estos servicios, sobre todo para actividades de organizaciones revolucionarias. Es más, el objetivo de esta guía es proveer alternativas e información para poder prescindir de servicios como Whatsapp o Telegram.

En cualquier caso, como entendemos que a veces hay razones de otros tipos para utilizar estas aplicaciones, queremos recomendar para el caso de Telegram, la aplicación Partisan Telegram que dispone de varias funcionalidades útiles para militantes políticos.

Sistemas de mensajería seguros

Signal

Topología: Cliente-Servidor

Signal es una conocida aplicación de mensajería instantánea, centrada en la privacidad y la seguridad. Los mensajes, archivos y llamadas de Signal están cifrados punto a punto, por lo que el servidor central no puede acceder al contenido de los mensajes enviados.

El servidor y el cliente son independientes, por lo que pueden utilizarse diferentes clientes para usar Signal. Sin embargo, existen muy pocos de estos clientes alternativos a la aplicación oficial de Signal. Uno de ellos es Molly, el cuál recomendamos utilizar en su versión FOSS, porque tiene seguridad añadida y se está planeando introducir características que podrían ser de utilidad para la militancia como, por ejemplo, el borrado remoto de mensajes (en caso de que el dispositivo móvil acabe en manos de la policía). Por tanto, recomendamos utilizar Molly FOSS, en lugar de la aplicación oficial de Signal.

Plataformas:

- Android
- iOS
- Microsoft Windows, Linux y MacOS

¿Se puede autoalojar?

Sí, pero no a efectos prácticos. El código del servidor de Signal es abierto (aunque el código fue cerrado durante un año por razones comerciales) y puede ser desplegado por cualquiera… con los correspondientes recursos. Por la cantidad de recursos necesarios y la complejidad en el despliegue, nadie suele desplegar un servidor de Signal y es por ello que decimos que a efectos prácticos no se puede autoalojar.

Mejores aplicaciones cliente:

Molly

Signal (oficial)

Ventajas:

- Cifrado robusto.
- El código y el protocolo de Signal dispone de una buena reputación y ha sido auditado para comprobar su seguridad.
- La experiencia de usuario es muy amigable. Dispone de todas las características existentes en aplicaciones de mensajería comerciales como Whatsapp.

Desventajas:

- Se necesita proveer el número de teléfono móvil para registrarse.
- A efectos prácticos es complicado autoalojarlo.
- La oferta de aplicaciones cliente es extremadamente reducida.

Casos de uso:

- Uso diario con familia y amigos.
- Para comunicaciones relativas a la actividad política, es recomendable utilizar Signal solo con gente conocida y de confianza, debido a que el número de teléfono móvil es un identificador personal bastante claro.

Matrix

Topología: Cliente-Servidor

Matrix es un protocolo de comunicación de código abierto que ha adquirido mucha popularidad en entornos de organización de software libre y público, gracias a su diseño seguro y una gran comunidad de desarrolladores. Hoy por hoy, es **una de las mejores alternativas** en cuanto a servicios de mensajería se refiere, hasta el punto que está siendo adoptada incluso por las administraciones de diferentes gobiernos. Soporta cifrado P2P, tanto en conversaciones uno a uno, como en salas de varios usuarios, canales de comunicación públicos y privados como el modelo de Telegram, etc.

Lo más fundamental que hay que comprender de Matrix es que no constituye un servicio de mensajería, sino un protocolo. Dicho de otra manera, Matrix define una serie de reglas, requisitos y detalles técnicos para implementar dicho protocolo. Al ser así, existen muchas implementaciones de servidores y clientes para Matrix. Esto da al usuario la oportunidad de escoger entre una amplia gama de implementaciones de servidores y de clientes. ¿Qué quiere decir esto? Que puedes conectarte al servidor que quieras utilizando el cliente (aplicación) que quieras, eligiéndola en

base a las características que más se ajusten a tus necesidades: apariencia, facilidad de uso, seguridad, capacidad de enviar archivos multimedia, integraciones añadidas, etc.

Del mismo modo que se puede escoger entre varios clientes, se puede escoger entre varios servidores. Ya sea en cuanto a la implementación del servidor como tal o sea en cuanto a un servidor ya desplegado, el usuario dispone de libertad para elegir si conectarse a un servidor existente o a uno alojado por cuenta propia. Esto último nos interesa porque al poder autoalojarse por cuenta propia, nos dota de cierta autonomía respecto de los servicios comerciales y de la infraestructuras del capital.

Otra característica interesante de Matrix es su interoperabilidad con otros servicios de mensajería a través de puentes o bridges. Por ejemplo, es posible que, una sala en Matrix se asocie con un grupo de Telegram a través de un puente, de tal modo que se cree una única sala, manteniéndose cada uno de los usuarios en el servidor y plataforma que prefieran. Sin embargo, esto es problemático porque, entre otras cosas, obliga a desactivar algunas características de seguridad que nos habría interesado mantener (por ejemplo, el cifrado) o elementos de nuestra organización que nos habría gustado mantener ocultos.

Plataformas:

- Android
- iOS
- Microsoft Windows, Linux y MacOS
- Web

¿Se puede autoalojar?:

Sí y es recomendable para la actividad política. Para ello, la mejor opción es utilizar la implementación Synapse, ya que es la implementación de referencia y la que más soporte lleva detrás. Como es habitual, **autoalojar un servidor es fácil si se tienen los conocimientos necesarios para hacerlo**. Entendemos que si alguien tiene dichos conocimientos, también tiene los conocimientos necesarios para consultar la documentación de Synapse o encontrar guías útiles por Internet.

Sin embargo, como uno de los principales objetivos de nuestro colectivo es facilitar el uso de las tecnologías de la información y la comunicación para el proletariado, tenemos planeado subir guías detalladas y recursos automatizados para el despliegue de servidores de mensajería y de otros tipos.

Mejores aplicaciones cliente:

Element

FluffyChat

Existe una gran variedad de clientes, pero muchos de ellos están en fases de desarrollo tempranas, por lo que es arriesgado utilizarlos para actividades sensibles.

Ventajas:

- Cifrado robusto.
- Gran comunidad detrás, lo que supone una mayor

implicación tanto cuantitativa como cualitativa en el desarrollo de clientes, servidores, puentes y bots.

- No requiere de número de teléfono móvil para el registro y no siempre es obligatorio introducir un correo electrónico para registrarse (esto depende de cada proveedor de servicio).

- Es autoalojable y los servidores pueden comunicarse entre sí.

- El servidor y el cliente son totalmente independientes, por lo que cada cual puede utilizar el cliente que le plazca y el servidor que le parezca más fiable.

Desventajas:

- Es conocido que el protocolo Matrix filtra metadatos. Esto quiere decir que el servidor puede conocer quién habla con quién, aunque no sepa qué se está hablando. Es una desventaja a valorar si lo que se pretende es que no se conozca con quién se está hablando. No obstante, esto puede solucionarse de dos formas. La primera es

anonimizar totalmente las cuentas, creándolas y usándolas siempre desde Tor. La segunda es autoalojando un servidor y usándo únicamente ese mismo servidor. Evidentemente, el servidor sigue conociendo quién habla con quién, pero al ser un servidor propio no supone un problema.

- De vez en cuando se descubren vulnerabilidades en la implementación de servidores y clientes de Matrix. Una cosa es que el protocolo Matrix sea seguro (cosa que está generalmente aceptada) y otra cosa muy diferente es que los desarrolladores de clientes o servidores cometan errores a la hora de programarlos y hacerlos compatibles con el protocolo. Esto último es lo que suele fallar más a menudo, aunque no es un problema específico de Matrix, ni algo ausente en el resto de sistemas de mensajería que compartimos aquí.

Casos de uso:

- Puede utilizarse para uso diario con amigos, familia o conocidos.

- Para contextos de actividad política, es una buena

alternativa a Telegram para crear grupos y comunidades, con el añadido de que es mucho más confiable que Telegram o Signal, ya que en Matrix los servidores son de código abierto, autoalojables y descentralizados. Además, a diferencia de Telegram y Signal, **los usuarios no se identifican por algo tan problemático como los números de teléfono móvil**, dificultando, así, la labor a la investigación policial.

XMPP

Topología: Cliente-Servidor

Al igual que Matrix, XMPP es un protocolo de comunicación extensible de propósito general en el mundo del intercambio de mensajes.

En el aspecto técnico, funciona de forma muy diferente a Matrix, pero hemos dicho que no nos interesa explicar los aspectos técnicos en una guía como ésta. Lo que hay que entender es que supone una topología Cliente-Servidor, descentralizada y federable. Una vez más, cliente y servidor son independientes y existen múltiples implementaciones de clientes y servidores para elegir.

El protocolo no está cifrado de base, por lo que son los clientes los que pueden o no implementar el cifrado de mensajes, mediante tecnologías que se han añadiendo con el tiempo como diferentes capas superpuestas. Hoy por hoy, la mejor alternativa de cifrado para XMPP es OMEMO. Por tanto, es importante buscar clientes que lo implementen.

Plataformas:

- Android
- Linux
- Web

¿Se puede autoalojar?:

Sí, y además es de los servicios de mensajería más fáciles desplegar. De toda la gama de implementaciones de servidores XMPP que existe, la opción más sencilla y robusta nos parece la de Prosody. Tenemos planeado desarrollar una guía de despliegue de Prosody en un futuro no muy lejano.

Mejores aplicaciones cliente:

Conversations (Android)

Monal (iOS)

Gajim (Linux, Windows)

Ventajas:

- Cifrados robustos, como OMEMO, OTR y PGP.
- Fácil y liviano en consumo de recursos de sistema para autoalojar.
- Amplia gama de clientes y servidores.
- No requiere identificadores como correo electrónico o número de teléfono para registrar cuentas.

Desventajas:

- Dispone de pocas funcionalidades, aparte de las tradicionales: envío de texto, imágenes, vídeos, documentos, audios y llamadas.

Casos de uso:

- Es un buen sustitutivo de Signal o Matrix, para usarlo para la comunicación en y entre organizaciones, sin necesidad de revelar la identidad de los participantes.

- Podría usarse en el día a día con familia y amigos, pero hay aplicaciones más amigables, como Signal.

Briar

Topología: Malla

Briar es una aplicación de mensajería para Android (aunque actualmente se está haciendo una versión para Linux) cuyo

objetivo principal es poder permitir una comunicación segura y anónima incluso en situaciones en las que la red de Internet no se encuentra disponible. Es esto último lo que la hace una aplicación única entre las comentadas en este artículo.

Las cuentas en Briar no requieren de ningún tipo de identificador. Basta con instalarse la aplicación e introducir una clave para cifrar la base de datos local (para almacenar la información de la aplicación). Al usuario se le asigna un identificador único dentro de la red y a través de ese identificador puede ser agregado por otros usuarios.

Todo el tráfico de Briar pasa por la red Tor, de tal modo que se preserve el anonimato de los usuarios, frente a posibles identificaciones por parte de las fuerzas represivas del Estado. Es más, aunque interviniesen uno de los dispositivos con Briar instalado, no serían capaces (en teoría) de identificar a las personas con las que dicho dispositivo se comunica.

La topología es en malla, es decir, que cada nodo (dispositivo) se apoya en los demás para hacer llegar los mensajes. Esto es especialmente útil para Briar, porque dispone de la funcionalidad para poder comunicarse por WiFi o por Bluetooth, en caso de que la red de Internet se

encuentre caída o censurada.

Dispone, además, de la posibilidad de crear grupos, foros y blogs, lo que es realmente útil para organizar acciones y flujos de información. No obstante, la experiencia de usuario es bastante mala. Por un lado, la interfaz es poco amigable y con mucho que mejorar en el aspecto estético. Por otro lado, a veces hay problemas para recibir las notificaciones en tiempo real, debido a las limitaciones de Android con la batería y, como en cualquier aplicación que funcione sin servidor, debido a que ambos interlocutores deben estar conectados a la red al mismo tiempo.

Plataformas:

- Android

¿Se puede autoalojar?:

No. Es serverless.

Ventajas:

- Anonimato a través de Tor. Sin identificadores personales.

- Comunicación cifrada.

- Funcionalidades varias como grupos, foros y blogs.

- Puede funcionar sin Internet y gracias a la topología en malla puede generar una red autónoma.

Desventajas

- Mala experiencia de usuario, sobre todo en cuanto a estética.

- No dispone de un desarrollo avanzado, por lo que pese a que sea muy interesante su capacidad, no existe un avance tan rápido en su desarrollo como para usarlo de manera normal.

Casos de uso:

- Situaciones en las que es muy probable que se materialice o que ya se haya materializado una posible censura de Internet. Por ejemplo, una manifestación en la que se corten las vías de comunicación habituales y sea necesario intercambiar mensajes a través de redes WiFi y Bluetooth improvisadas.

- Briar es muy útil para crear comunidades mediante foros y grupos, fáciles de disolverse y de tal forma que sea muy difícil tanto descubrir la existencia de dichos puntos de encuentro, como de identificar a sus participantes.

Session

Topología: Descentralizada

Session es una aplicación disponible para varias plataformas, cuyas principales características son la

descentralización, el anonimato y que no filtra metadatos. Se apoya sobre una red de nodos que funcionan parecido a la red Tor, pero la red es propia de Oxen. Esto significa que los mensajes rebotan en varios nodos antes de llegar al destinatario, haciendo anónimas a las dos partes. Aparte de cifrar los mensajes punto a punto, cada nodo en el que rebotan los mensajes añade una capa de cifrado adicional, como si de una cebolla se tratase (de ahí el concepto de "onion routing"). Estos nodos descentralizados son los que almacenan la información necesaria para la comunicación.

La aplicación está basada en Signal, algo que se ve claramente en la interfaz de usuario. La funcionalidad es parecida, solo que en Session no se depende de un servidor central.

En resumen, Session viene a ser un Signal sin números de teléfono en el registro, sin filtrar metadatos y que se apoya en una red parecida a la red Tor para anonimizar a los usuarios y almacenar la información de forma descentralizada.

Por último, si bien Session parece una buena apuesta para ser usada en ámbitos de militancia política, últimamente han surgido dudas sobre su fiabilidad. Aparte de que se ha encontrado alguna que otra vulnerabilidad, Session es una

aplicación con sede en Australia, donde recientemente se han promulgado leyes que permiten intervención y vigilancia en servicios digitales (aunque en sí, la red Oxen es una red descentralizada). Además, Session está vinculada a Oxen, una organización que provee servicios de criptomonedas, aparte de una red propia que funciona igual que la red Tor. En la comunidad preocupada por la privacidad es un servicio que causa muchas dudas y nosotros no hemos ahondado profundamente en investigarla como para poder recomendarla o prevenir de su uso.

Plataformas:

- Android
- iOS
- Microsoft Windows, Linux y MacOS

¿Se puede autoalojar?

Sí y no. El diseño de esta aplicación está hecha para que solo se pueda usar a través de la red Oxen, la cual está compuesta de nodos. Por lo tanto realmente no se gestiona un servidor, sino un nodo de esta red que sirve como un

punto más en una red. Aunque es cierto que la manera de obtener o conseguir levantar un nodo de esta red es complejo.

Ventajas

- Comunicación cifrada.
- No se filtran metadatos.
- Anonimato a través de una red descentralizada de nodos.
- No requiere de identificativos personales.
- Buena experiencia de usuario en lo que se refiere a apariencia.

Desventajas

- Mala experiencia a la hora de recibir mensajes: a veces

llegan tarde, se pierden…

- Está asociada a una organización que promueve el uso de criptomonedas y dispone de la suya propia. Por lo que entendemos que puede llegar a ir en su propio interés del valor la misma red de comunicación.

- Crea dudas en la comunidad hacker.

Casos de uso:

- Pese a que el modelo que ofrece Session es interesante y trae consigo una serie de características que en otras redes no se presentan, **no podemos recomendar** Session para comunicaciones sensibles y para actividades clandestinas. Sin embargo, su diseño trae consigo una serie de propuestas interesantes que otros servicios de mensajería deberían tener en cuenta.

Conclusiones

Tras este repaso por esta selección de aplicaciones de mensajería segura, queremos poner sobre la mesa varias advertencias.

Siempre y cuando sea posible, es preferible no tratar cuestiones sensibles por medios digitales. De hecho, en la actividad militante, es importante minimizar el uso de estas vías de comunicación, ya que siempre existen posibilidades de fallos o vulnerabilidades desconocidas por los desarrolladores, pero conocidas por las fuerzas del orden. Además, hay que tener muy claro que la comunicación puede ser segura, pero los dispositivos pueden estar comprometidos (“pinchados”) y, por tanto, se lean todos los mensajes antes de ser enviados y cuando se reciben. Ahora bien, si es necesario utilizar medios de comunicación como estos, hay que ser serios y utilizar los medios más seguros posibles.

Estos medios de comunicación además, suponen una gran oportunidad de crear nuevos, o al menos sustituir los anteriores medios de comunicación de organizaciones. El sistema clásico del correo electrónico está obsoleto desde hace años y debe ir siendo desplazado poco a poco como

todas aquellas tecnologías que fueron innovadoras en la comunicación, pero que tienen que ir quedando atrás al no poder enfrentar correctamente los nuevos retos que requiere la coyuntura actual en materia de ciberseguridad.

Estas herramientas también ofrecen oportunidades para organizar comunidades y actividades militantes. Por ejemplo, grupos en los que se pase información pública de organizaciones (los típicos canales) o grupos/foros en los que se realicen debates sobre cuestiones estratégicas, tácticas, de teoría, de práctica, etc. Lo importante es saber determinar si es un lugar adecuado para reunir y conectar a personas u organizaciones y contemplar bien los riesgos asociados a cada uso.

Finalmente, nuestras recomendaciones:

- **Uso diario:** Signal, a través de la app Molly. Es una aplicación conocida por su seguridad, su usabilidad, su carácter intuitivo y su robustez. Es el sustitutivo perfecto a aplicaciones como Whatsapp o Telegram, perfecto para comunicarse con amigos y familia.

- **Uso militante:** ésta es una decisión difícil, porque depende de la casuística. En nuestra opinión, Matrix es

el mejor servicio, porque permite no solo una mensajería segura, sino que permite unir a grandes comunidades e interconectar grupos. Por ejemplo, una organización debería crear un canal en Matrix, en vez de crearlo en Telegram, como suele ser habitual. A eso nos referimos. Tanto para conversaciones 1 a 1, como para grupos, Matrix es un servicio que permite una experiencia excepcional, con muchas funcionalidades y muchas implementaciones de clientes y de servidores. Además, permite ser autoalojada y es descentralizada, por lo que no se depende exclusivamente de un servidor central gestionado por terceros. Por último, permite cierto anonimato, ya que las cuentas no requieren de identificadores personales (número de teléfono o correo electrónico, aunque hay servidores que piden este último) para registrarse lo que, sumado al uso de Tor, puede hacer su uso teóricamente anónimo.

Colectivo 406