پیام رسانی امن در اینترنت؛ توهم یا افسانه؟ - دیجیاتو

سامه گل زاده | پنجشنبه، ۲۵ دی ۱۳۹۳

این روزها کمتر کسی پیدا می شود که از سیستم های پیام رسانی اینترنتی استفاده نکند. اپلیکیشن واتس‌اپ به تنهایی بر روی صدها میلیون دستگاه در سراسر دنیا نصب شده و ده ها میلیارد پیام را روزانه انتقال می دهد. البته اسکایپ، وایبر، ICQ، ده ها مسنجر معروف و غیر معروف دیگر مانند قابلیت های انتقال داخلی پیام فیسبوک، لینکدین و مشابه های آنها هم هستند که نباید نادیده گرفته شوند.

در حالی که این سیستم ها از محبوبیت خودشان سودهای کلانی می برند، مساله حریم شخصی کاربران نیز نباید نادیده گرفته شود. هر چند با توجه به حجم عظیمی از اطلاعات که روزانه بر روی اینترنت به اشتراک گذاشته می شوند احتیاط بیش از حد بی معنی به نظر می رسد، اما مواردی هست که ارتباط باید کاملا محرمانه باشد و هیچ شخص ثالثی امکان نفوذ به آن را نداشته باشد. آیا امکان برقراری چنین ارتباطی وجود دارد؟

در ادامه این موضوع را دقیق تر مورد بررسی قرار می دهیم.

پیش درآمد

پیش از شروع این بررسی لازم است بدانیم که یک پیام متنی یا صوتی از چه راه هایی ممکن است در اختیار شخص ثالث قرار گیرد. گزینه های اندکی وجود دارند. هر پیامی اعم از متنی، ویدئویی، صوتی یا تصویری بر روی فضای حافظه وسیله فرستنده و گیرنده ذخیره می شود؛ سپس از طریق شبکه بی سیم یا با سیم انتقال داده شده و در بسیاری اوقات بر روی سرور پردازش می شود.

اگر شخصی به هر طریقی به تاریخچه پیام رسانی دسترسی پیدا کند، باقی مسیری که پیام طی می کند از کنترل خارج می شود. البته رمزگذاری به حفظ امنیت کمک می کند اما نه به طور کامل. چه کسی تضمین می کند که یک پروتکل -مخصوصا آنهایی که از الگوریتم های مشترک رمزگذاری استفاده می کنند- از آسیب به دور است؟

اسکایپ را در نظر بگیرید؛ تا چندی پیش به عنوان یک ابزار خوب برای مکالمات خصوصی به شمار می رفت، یک قلعه نفوذناپذیر که هیچ هکر و سازمان قدرتمندی امکان یورش به آن را نداشت. اما مایکروسافت اسکایپ را خرید و پس از آن که شرکت اسکایپ استقلال خود را از دست داد. همه چیز عوض شد. حالا نمی توان با اطمینان گفت که پیام رسانی از طریق اسکایپ ۱۰۰٪ امن است.

سرویس واتس‌اپ روزانه صدها میلیون پیام را پردازش می کند. به سختی می توان آن را امن در نظر گرفت. اخبار درباره آسیب پذیری (حتی اگر تنها در مورد نسخه های اندرویدی باشد) هر ماه به گوش می رسد. به عنوان مثال یک تحقیق تازه درباره اپلیکیشن نشان داد که با کمک یک کد ساده، فایل رمزگذاری شدهٔ تاریخچه پیام ها در وسیله شما، قابل هک شدن است. لازم به اشاره است که خریداری شدن واتس‌اپ توسط فیسبوک هیچ تاثیری بر امنیت آن نداشته است.

بد نیست بدانید این مشکلات محدود به اسکایپ و واتز اپ نیستند. سایر پلتفرم ها از وایبر تا آی‌مسج همگی دارای ضعف های امنیتی مشابهی هستند. در همه آنها به سادگی امکان دسترسی به ارتباطات وجود دارد. بنابراین، شاید تا حدی بد نباشد که چنین سرویس هایی بخشی از اموال موسسه های بزرگ باشند که عدم دسترسی دولت ها به اطلاعاتشان را تضمین می کنند. خوشبختانه راه کارهای امن تری توسط اپلیکشن های دیگری معرفی شده اند. آیا آنها واقعا قادر به حفظ حریم افراد هستند؟ باید دید. اما پیش از آن لازم است که در نظر بگیریم چه سطحی از امنیت مورد نیاز شماست.

اگر دقت کرده باشید در سیستم های حمل و نقل عمومی امکانات ضد تروریست وجود دارد. به عنوان مثال در فرودگاه ها وسایل و چمدان های مشکوک در ایستگاه های خاصی بررسی می شوند. از سیستم هایی با ویژگی های مشابه نیز می توان برای انتقال پیام استفاده کرد. البته این بدان معنا نیست که برخی از برنامه های انتقال پیام کاملا بلا استفاده هستند چرا که کاربران زیادی هستند که امنیت پیام برایشان اهمیت ویژه ای ندارد.

کافی است بدانید در برابر چه کسی می خواهید از پیام هایتان حفاظت شود: یک شریک حسود که می خواهد پیام های خصوصی شما را بخواند، یا کسانی که می خواهند به ترافیک بین فرستنده و گیرنده دسترسی پیدا کنند. البته در این میان کسانی که از طریق ارتباط مستقیم در تلاش برای دسترسی به حریم شما هستند مورد نظر گرفته نشده اند. بنابراین اگر به کسی که برایتان پیامی می فرستد اعتماد ندارید بهترین و ساده ترین کار این است که جوابی به پیام آنها ندهید!

بیایید نگاهی به گزینه های ارائه شده فعلی بیاندازیم.

توهم امنیت

این دسته از مسنجر ها آنهایی هستند که امنیت را به حد نیاز رعایت نمی کنند و یا هیچ تضمینی برای دزدیده نشدن اطلاعات در حین انتقال نمی دهند.

Confide

این مسنجر تا حدی منحصر به فرد است: تمام پیام هایی که از طریق Confide ارسال می شوند در جعبه های مستطیلی شکلی مخفی هستند و تا زمانی که بر روی آنها دست کشیده نشود نمایان نمی شوند. بعلاوه این اپلکیشن تاریخچه پیام ها را برای مدت طولانی بر روی حافظه دستگاه نگه داری نمی کند، بنابراین حتی اگر کسی به تلفن شما دسترسی پیدا کند چیزی از مکالمات را نمی تواند به دست آورد. اگر کاربری سعی کند که از صفحه مکالمات اسکرین شات بگیرد فرد از صفحه مکالمه اخراج شده و همچنین یک اخطار به طرف دیگر مکالمه نیز ارسال می گردد. این ویژگی ها توسط سازندگان این اپلیکیشن بسیار برجسته شده اند. هر چند که اگر کسی بخواهد مکالمه ای را ذخیره کند و امکان اسکرین شات گرفتن نداشته باشد می تواند با استفاده از یک دوربین دیگر آن را کلمه به کلمه ذخیره کند. این همان چیزی است که از آن به عنوان 'امنیت نمایشی' نام برده می شود. گزینه های ارائه شده توسط این برنامه به کاربر تنها توهمی از امنیت می دهد. این برنامه شاید بتواند برای کسانی که می خواهند در نقش مامور مخفی ظاهر شوند مناسب باشد.

wickr

این اپلیکشن با وجود این که از طراحی ظاهری خوبی برخودار نیست، اما با داشتن قابلیت پاک کردن تاریخچه پیام ها از هر دو دستگاه و از سرور (که در برخی موارد غیر قابل بازگشت است) و تضمین عدم دسترسی دولتمردان به الگوریتم های، امنیتی خود را در میان اپلیکشن های امن برای انتقال پیام جا داده است. فراهم آوردن ابزاری برای کنترل زمان نگه داری مکالمات و غیرفعال سازی امکان کپی کردن پیام ها از دیگر ویژگی های این مسنجر به حساب می آید. هر چند که گزینه آخر مانند آنچه در بالا دیده شد بیشتر نمایشی از امنیت است.

Telegram

وقتی درباره برنامه های پیام رسان امن حرف می زنیم چطور می توانیم تلگرام را نادیده بگیریم؟ این برنامه که در میان عامه مردم به عنوان یک برنامه «امن» به شهرت رسیده است. اما چه چیزی باعث میشود که از امنیت آن به «نمایش امنیت» تعبیر شود؟ امنیت انتقال پیام «بی سابقه» ای که سازندگان آن ادعایش را می کنند هرگز به طور واقعی به اثبات نرسیده است.

شاید عده ای از جایزه ۲۰۰هزار دلاری که برای هک کردن پروتکل MTProt تلگرام یاد کنند. در حقیقت این اعتماد به نفس یک شناسه قدرتمند برای نشان دادن امنیت این برنامه نیز محسوب می شود، اما ابزار های هک کردن این مسنجر ناکافی هستند و نمی توانند این پروتکل را تست کنند. لازم است اشاره شود که یک نویسنده در cryptofails اشاره کرده است که «تلگرام بسیار نا امن و غیر قابل اعتماد است و تمام الگوریتم های معنادار رمزنگاری ۲۰ سال گذشته را نادیده گرفته است.» و به سازندگان آن پیشنهاد کرده تا با یک متخصص رمزنگاری واقعی همکاری کنند.

بدون توجه به پروتکل های پیچیده ای که اساس تلگرام را تشکیل می دهند این برنامه در برابر حملات مستقیم آسیب پذیر است. در هنگام ثبت نام کاربر یک اس‌ام‌اس حاوی کد امنیتی دریافت

می کند و باید آن را برای فعال سازی در اپلیکیشن وارد کند. اما اگر هکر به اس‌ام‌اس های موبایل شخص دسترسی داشته باشد می تواند آن کد را بر روی دستگاه دیگری وارد کرده و در نتیجه به تمام مسج های رد و بد شده دسترسی پیدا کند. در عین حال گزینه «گفتگوی امن» بطور پیش فرض فعال نشده است که باعث می شود امنیت مکالمات تا حدود زیادی در خطر باشد.

ویژگی خوب تلگرام سرعت آن است: پیام ها به معنی واقعی کلمه بی درنگ ارسال و دریافت می شوند که به طور چشم گیری از هر مسنجر دیگری سریع تر است.

در نهایت دو سوال مهم در مورد تلگرام به وجود می آید: آیا این مسنجر سریع است؟ بله. آیا امن است؟ فقط تا حدودی!

صداقت امنیت

این دسته از مسنجرها سطح قابل قبولی از امنیت را با ویژگی هایی که به طور رسمی اعلان شده اند فراهم می کنند و اساسا دسترسی به ارتباط از طرف شخص ثالث را قطع می کنند.

Theema

این یک پروژه سوییسی است که پس از خریداری آن توسط واتس‌اپ به شهرت رسید. توسعه دهنده گان آن امنیت مکالمه را تضمین می کنند: نخست آن که اپلیکیشن رمزگذاری قابل اعتمادی برای انتقال داده فراهم می کند. دوم آنکه از حریم خصوصی کاربر با استفاده از تایید رو در رو وقتی یک اتصال جدید اضافه می شود، انجام می گیرد. این مورد آخر به طور پیش فرض باید با دیدن شخص اضافه شده به لیست و اسکن کردن QR Code از روی دستگاه وی صورت پذیرد که از نظر امنیتی بسیار بالاست و در عمل دشوار است. هر چند امکان اضافه کردن شخص به روش های مرسوم نیز امکان پذیر است اما سطح امنیت کمتری برای آن در نظر گرفته می شود. سازندگان این اپلیکیشن هیچ تضمینی برای امن بودن سیستمشان در برابر روش های «جدیدی» که برای از بین بردن امنیت مورد استفاده قرار می دهد، نمی دهند. و نکته آخر این که برای داشتن این اپلیکیشن لازم است یک بار ۲ دلار هزینه کنید که البته ارزشش را دارد.

Silent circle

این اپلیکیشن یکی از معدود پروژه هایی است که توسط گروهی از رمزنگاران واقعی نوشته شده.

تیم توسعه دهنده شامل فیل زیمرمن، نویسنده تکنولوژی PGP encryption، است و مشابه تلگرام از الگوریتم هدفمند شده SCIMP استفاده می کند. امکان پاک کردن پیام های ارسال شده بدون آن که هیچ ردی از آنها چه در سمت فرستند و چه در سمت گیرنده باقی بماند، برتری آن است. بدین ترتیب هیچ یک از دو طرف هرگز قادر با بازیابی هیچ بخشی از مکالمات پاک شده نیستند. این ویژگی هم به طور دستی هم به طور خودکار فعال شده است. بر حسب توافق پیام ها پس از یک بازه زمانی مشخص پس از ارسال پاک خواهند شد. اما برتری اصلی این برنامه رمزنگاری فوق العاده آن در حین انتقال است که هیچ راهی برای دزدی اطلاعات هنگام انتقال باقی نمی گذارد. اما خب این مسنجر ایرادهایی هم دارد. به عنوان مثال روند ثبت نام پیچیده اولیه و قیمت ۱۰۰ دلاری آن برای برای یک سال.

TextSecure

نام این اپلیکیشن رایگان ارائه شده توسط WhisperSystems بسیار از ادوارد اسنودن شنیده میشد. این برنامه یک مسنجر بسیار ساده است که هیچ تنظیمات خاص و پیچیده ای ندارد اما دارای رمزگذاری بسیار قوی برای انتقال و ذخیره روی ابزارهای موبایل و سرور است. از معایب آن می توان به قابلیت های کم و دسترسی آن فقط برای کاربران اندروید اشاره کرد. هر چند که قرار است نسخه iOS آن هم به زودی ارائه شود. لازم به ذکر است که یکی از سرمایه گذاران آن ماکسی مارلینسپایک متخصص معروف رمزنگاری است.

SJ

۵۰ دلار قیمت گرانترین و قابل اعتمادترین اپلیکیشن iOS برای انتقال پیام است. SJ نام این برنامه است. برتری اصلی آن توانایی استفاده از کلیدهای متمم مجزا برای هر کاربر و انتقال آن با هر پیام است، که می تواند بر اساس دانش کاربر اصلی ترین عیب آن نیز شناخته شود. رابط کاربری این برنامه برای کسانی که با اسکایپ یا واتس‌اپ کار کرده باشند، بسیار پیچیده است. در واقع کاربران در دو راهی انتخاب بین سادگی استفاده از برنامه و امنیت تامین شده آن قرار می گیرند.

Pidgin

این برنامه با مجموعه کاملی از پروتکل های امنیتی یکی از مسنجرهای معروف است که رایگان بوده و با سیستم عامل های ویندوز، لینوکس و مک سازگار است. توسعه دهندگان به کاربران مک پیشنهاد می کنند که از Adium استفاده کنند و تا از امنیت بیشتری هم برخوردار باشند. این برنامه

از پروتکل OTR یا عدم ضبط ارتباط پشتیانی می کند تا تضمینی برای امنیت ارتباط فراهم کند. مزیت ویژه آن پشتیبانی از پروتکل XMPP/Jabber است که سیستم پیام رسانی امن را فراهم می کند.

CryptoCat

این مسنجر نیز مانند همه آنهایی که پیشتر به آنها اشاره شد دارای قابلیت رمزنگاری پیام است. این مسنجر امکان نصب به صورت افزونه را روی کروم، فایرفاکس، سافاری و اپرا دارد. هر چند برای کاربران مک و آیفون دارای اپلیکیشن مجزای دیگری نیز هست. چندی پیش سازندگان آن تلاشی چشمگیر برای رمزنگاری و افزایش امنیت اطلاعات ذخیره شده بر روی دستگاه و یا در حین انتقال انجام دادند. نکته مهمی در مورد کریپتوکت این است که به طور دائم در حال به روز رسانی است. با این وجود سازندگانشان بر روی وبسایتشان نوشته اند که «کریپتوکت معجزه نیست. با وجود این که ما رمزنگاری مفیدی را تامین می کنیم اما هیچ گاه به هیچ نرم افزاری در زندگی تان اعتماد نکنید. حتی به کریپتوکت.»

به زودی

Heml.is

با وجود این که اپلیکیشن هنوز در حال ساخت و توسعه است، توجه بسیاری را به خود جلب کرده است. در میان سرویس های ارائه شده پروتکل XMMP و کتابخانه PGO پایه های رمزگذاری هستند. بر اساس آنچه تا کنون دیده شده این اپلیکشن دارای طراحی زیبایی و قابلیت سازگاری بین پلتفرم ها است.

ختم کلام

واضح است که هیچ مسنجر رمزنگاری شده ای ایده آل نیست و شما باید میان سادگی استفاده، بودجه و امنیت به توافق و انتخاب برسید. بعلاوه این که امنیت ارتباطات آنلاین هرگز توسط یک برنامه تامین نمی شود و معیارهای زیادی برای این منظور وجود دارند که باید در نظر گرفته شوند.

به علاوه این که هیچ برنامه ای نمی تواند برای شما امنیت ۱۰۰٪ را تضمین کند اگر شما به شخص مقابلتان اطمینان کافی را نداشته باشید.

ديجياتو