ارتباطات و پیام‌رسانی ایمن

- زمان: ۱ ساعت
- موضوع درس‌نامه : یادگیری تفاوت میان ارتباط ناشناس و ایمن، یادگیری ابزارهای انجام این کار

رمزنگاری یا ناشناس بودن

امروز در فضای مجازی نرم‌افزارهایی هستند که به شما اجازه می‌دهند تا به شکل ایمن ارتباط‌گیری کنید.
با این حال این نرم‌افزارها نیز همه کارها را نمی‌توانند انجام دهند. وحتی می توانند خطرناک هم باشند.

گاهی پیش می‌آید استفاده از یک ابزار پیام‌رسانی یا ارتباط‌گیری خطرناک تر از نرم‌افزاری باشد که به شما امکان ناشناس بودن را می‌دهد.

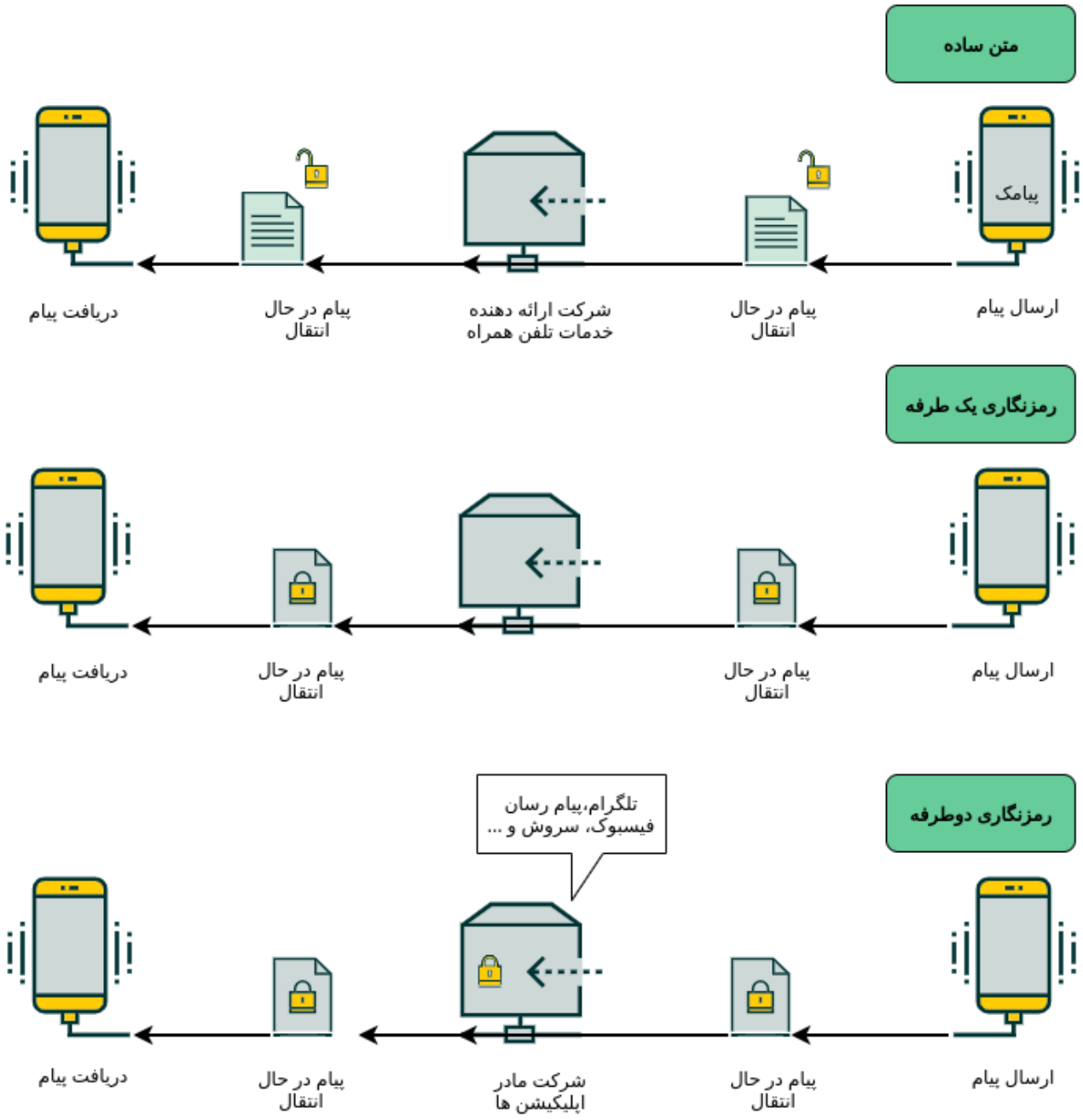
روزنامه‌نگاران برای حفاطت از داده‌های خود باید بتوانند با این ابزارها آشنا شوند و این امکان را داشته باشند تا داده‌های خود به راحتی در میان خیل پیام‌های دیگر ارسال کنند.

رمزنگاری یا ناشناس بودن؟

در هنگام استفاده از نرم‌افزارهای کاربردی مانند واتس‌آپ WhatsApp، مسنجر Messenger یا تلگرام Telegram ، محتوای پیام شما رمزنگاری می‌شود (این کم و بیش بستگی به نوع نرم‌افزار دارد) اما آدرس افرادی که با آنها ارتباط برقرار می‌کنید، رمزنگاری نمی‌شود. بنابراین اپراتورها (متا، فیسبوک، تلگرام) اگر به محتوای ارسالی شما نیزدسترسی نداشته باشد، اما می‌تواند بفهمد که شما با چه کسانی ارتباط برقرار می‌کنید.

پیام رسانی ایمن و رمزگزاری شد

- تنها راه تضمین محرمانه بودن پیام‌رسانی استفاده از روش رمزنگاری از مبدا تا مقصد است.
- **E2EE** (End-to-end encryption)
- با این روش پیام یا مقاله شما از مبدا و روی کامپیوتر یا گوشی هوشمند شما رمزنگاری و در مقصد برای مخاطب شما رمزگشایی می‌شود.
- هیچ واسطه‌ای در اینترنت نمی‌تواند محتوای پیام شما را بخواند.
- فراموش نکنیم که پیام‌های بانکی نیز چنین رد و بدل می‌شوند!


متن ساده
پیامک
ارسال پیام
پیام در حال انتقال
شرکت ارائه دهنده خدمات تلفن همراه
پیام در حال انتقال
دریافت پیام
رمزنگاری یک طرفه
ارسال پیام
پیام در حال انتقال
پیام در حال انتقال
دریافت پیام
رمزنگاری دوطرفه
تلگرام،پیام رسان فیسبوک، سروش و ...
ارسال پیام
پیام در حال انتقال
شرکت مادر اپلیکیشن ها
پیام در حال انتقال
دریافت پیام

Signal

پیام‌رسانی : سیگنال

- سیگنال یک برنامه برای گوشی‌های هوشمند است که پیام‌های شما را در گوشی شما رمزنگاری کرده و در گوشی یا گوشی‌های گیرنده آنها را رمزگشایی می‌کند. این رمزنگاری از از مبدا به مقصد (End To End Encrpytion) است. یعنی حتا در صورت هک شدن سرورهای سیگنال ، محتوای پیام‌ها

DATA

METADATA

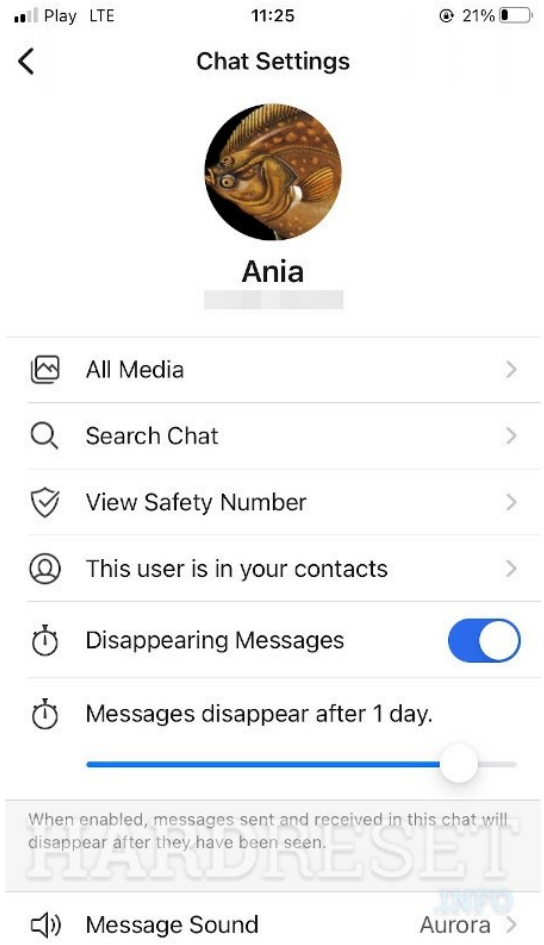
پیام‌رسانی ایمن: سیگنال

- سیگنال هیچ وسیله‌ای برای دانستن محتوای پیام‌های شما ندارد.
- سیگنال بر خلاف واتس آپ و تلگرام، داده‌های کلان را نگه‌داری نمی‌کند.
- داده‌های کلان metadata چون : شماره تلفن فرد مقابل، مدت‌زمان مکالمه، حجم داده‌های فرستاده شده و..... را فراتر از دوره مورد نیاز برای گردش پیام نگه‌داری نمی‌کند. و تنها یک نگه‌داری موقت به دلایل فنی است.

پیام‌رسانی ایمن: سیگنال

- **توجه داشته باشید**، پیام‌های ارسالی در گوشی‌ها ذخیره می‌شوند و اگر گوشی‌ها در دسترس کسی قرار گیرد و آن را رصد کند، در این صورت امکان دسترسی به پیام‌های شما وجود دارد.
- به همین دلیل سیگنال (و برخی دیگر از نرم‌افزارهای کاربردی) دارای ویژگی بسیار مفید هستند: پیام‌های موقت که امکان حذف خودکار آن‌ها برای ارسال کننده وجود دارد.

سیگنال و فعال کردن پیام موقت



تمرین

۱- https://signal.org/en/download/ را از App Store یا Play Store نصب کنید
۲- بر روی ارسال پیام جدید کلیک کنید؛ لست رابطین و آشنایان شما که از سیگنال استفاده می‌کنند نمایان می‌شود
۳- یک پیام به یکی از آنها ارسال کنید
۴- به تنظیمات گفتگوی جدید بروید و پیام‌های موقت را فعال کنید
۵- نرم‌افزار کاربردی را در دستآپ کامپویتر خود نصب کنید
۶- آن را با گوشی هوشمند خود هم گام و منطبق کنید

پیام‌رسانی ایمن و رمزنگاری شده

اگر از **دیگر نرم‌افزارهای کاربردی** استفاده می‌کنید به مانند WhatsApp، Discord ، Telegram، iMessage و غیره؟ دقت کنید که آیا نرم‌آفزار مورد استفاده از رمزنگاری از مبدا تا مقصد استفاده می‌کند؟ شما می‌توانید از این استفاده

این جدول نقاط قوت یا ضعف نرم‌افزارها را با هم مطابقت دهید.

پیام رسانی ناشناس

پیام رسانی ناشناس

گاهی برای خبرنگاران بهتر است که در ارتباط با منابع یا حتا برخی مخاطبان و همکاران خود از حالت ناشناس بودن استفاده کند.
در فضای مجازی و در میان خیل پیام‌های و گردش اطلاعات کمتر حساسیت ایجاد کند.

به اشتراک گذاشتن مقاله و نوشته به شکل آنلاین

CryptPad معادل Google Doc است که نوشته‌ها را به صورت رمزنگاری شده و آنلاین ذخیره می‌کند. می‌توانید از این امکان به مانند روش صندوق مرده استفاده کنید. اما برخلاف سرویس‌های ایمیلی مانند Gmail یا Yahoo ، Mail - cryptpad به محتوای پیام‌های شما دسترسی ندارد. زیرا آنها را به صورت رمزنگاری شده ذخیره می‌کند.

کلید رمزنگاری در URL پس از نویسه‌ی # نوشته می‌شود.بنا بر پروتکل این سیستم هر چیزی پس از نویسه‌ی # نوشته شود بردر آدرس URL برای سرور قابل دسترسی نیست.

//// **مثال انگلیسی**

https://cryptpad.fr/pad/#/2/pad/edit/J6KGLGTPSH1lJyc0U1U2zFLz/

آدرس الکترونیکی ای‌میل

ایمیل‌ها ایمن نیستند. پیام‌ها و مقالات شما در اینترنت به شکل غیر محرمانه در گردش است، یعنی همه‌ی محتوای آنها می تواند از سوی شرکت خدمات دهنده اینترنت شما دیده و خوانده شود. ای‌میل مثل نامه‌ای است که بدون پاکت فرستاده شود و پیام‌رسان آن را می‌تواند بخواند.

آدرس الکترونیکی ای‌میل

برای حفاظت از محتوای ای‌میل‌های خود می‌توانید از خدمات آنلاین مانند Proton Mail یا Tutanota

استفاده کنید.

توجه داشته باشید خدمات این شرکت‌ها برای ای‌میل‌های خود است. یعنی تنها ایمیل‌هایی از Protonmail به Protonmail یا از Tutanota به Tutanota فرستاده می‌شوند ایمن و رمزنگاری شده هستند. برای استفاده از این شرکت‌های خدمات دهنده برای مثال ازسال ای میل به جی میل خود باید اقدام به رمزنگاری کنید. و طبعا برای رمزنگاری باید یک رمز برای رمزنگاری و رمزگشایی ایمیل فرستاده شود.

آدرس الکترونیکی ای‌میل

Tutanota در نسخه رایگان خود یک گیگابایت فضای ذخیره‌سازی ارائه می‌دهد

Tutanota®

Tutanota

آدرس الکترونیکی ای‌میل

Proton Mail بر روی مدل freemium ی کار می‌کندو یعنی نخست یک سرویس رایگان با ۵۰۰ مگابایت فضای ذخیره‌سازی برای پیام‌های شما ارائه می‌دهد، اگر بیشتر نیاز داشته باشید باید فضای بیشتر را خریداری کنید.

Proton Mail

Pour aller plus loin

برای دانستن بیشتر ببینید :
دوره Totem آنلاین درباره پیام‌رسان‌ها و نرم‌افزارهای کاربردی ایمن (در زبان فارسی)