**تلفن امن:** راهی جدید برای ارتباط صوتی و متنی خصوصی.

مجموعه ای از فن آوری های سخت افزاری و نرم افزاری جدید به منظور محافظت از حق دسترسی شما به حریم خصوصی مکاتبات.

**رمزگذاری سرتاسر**

کلید های نامتقارن RSA 4096

رمزگذاری قطعه‌ای AES-256

کلید جدیدی برای هر جلسه ایجاد می شود.

کلید خصوصی (RSA) در اولین فعال سازی تولید شده و بر روی گوشی شما، بطور امنی ذخیره می شود.

کاربران می توانند در هر زمانی، به هر دلیلی، برای امنیت بیشتر، یک کلید جدید تولید کنند.

**کرنل یا هسته سفارشی**

هسته سفارشی ما، تنها شامل حداقل مقدار مطلق مورد نیاز برای عملکرد است و به عنوان ملاحظات اولیه، با امنیت طراحی شده است.

**سپر حمله MITM**

ما الگوریتم خودمان را برای حفاظت دربرابر حملات MITM اجرا می کنیم. به اعتبار متعارف CA اعتماد نمی کنیم. گواهینامه ما درون نرم افزار، بصورت سخت افزاری کدگذاری شده است، کلید خصوصی CA-root بر روی رایانه ای با فاصله هوایی ایجاد می شود.

**مبتنی بر آندروید**

 ویژگی های اختصاصی مبتنی بر اندروید، در حداقل نگه داشته شده و در درایورهای مربوطه­ی آنها قرنطینه شده اند.

**اتصال نظیر به نظیر**

اتصال صوتی به طور مستقیم بین مشترکان در یک مدل نظیر به نظیر اتفاق می افتد. در مورد NAT متقارن از ISP شما، ما از سرورهای­مان به عنوان یک پروکسی استفاده می کنیم. تمام اطلاعات به صورت پیوسته و پشت سرهم رمزگذاری می شود.

**GSM بی صدا**

ماژول GSM فقط برای اتصال به اینترنت استفاده می شود. حملات ارائه دهنده فلش اس ام اس، MMS، SMS و حملات با برنامه های مخرب، که از طریق SMS / MMS ارسال شده، بوسیله سخت افزار و نرم افزار جلوگیری می شود.

**آدرس مک تصادفی Wi-Fi**

به منظور جلوگیری از جمع آوری متادیتا یا فراداده در MAC-broadcast، یک آدرس MAC تصادفی در هر بازه (unlock) تولید می شود.

**بدون ثبت نام**

ما هیچ اطلاعات بکار رفته ای را روی سرورها یا دستگاه های مشتری مان ثبت نمی کنیم. سرورها فقط برای ارتباطات و اعطای مجوز به کاربران استفاده می شوند. تنها اقداماتی که به زیرساخت های­مان حمله کنند، ثبت می شود.

**سرورها بر اساس OpenBSD/FreeBSD**

تمام سرورها، روی یونیکس واقعی (Unix) اجرا می شوند. به روز رسانی های به موقع، فایروال به خوبی پیکربندی شده، حداقل مجموعه نرم افزار، توسط حرفه ای های امنیت محور و با تجربه اجرا می شوند.

**فایروال**

هر تلفن دارای فایروال ساکن پیکربندی شده است. این قوانین اجازه دسترسی، تنها به سرورهای ما را می دهند. همه پورت های ورودی و خروجی بسته هستند، تمام انواع اتصال به جز اتصالهای "جدید" و "برقرار شده" مسدود می شوند. برنامه کمکی ما به کسی اجازه نمیدهد که قوانین فایروال را تغییر دهد.

**زره برنامه بر اساس SELinux**

مجموعه محدودی از برنامه های کاربردی. فقط نرم افزار مورد نیاز نصب می شود (حداقل سبک گنتو).

حق دسترسی این برنامه ها به سیستم و حافظه، دقیقاً کنترل می شود.

**داده های محلی رمزگذاری شده**

کلید برای رمزنگاری داده های ذخیره شده، در محل ذخیره ی کلید سخت افزار موجود نیست. هر بار که تلفن روشن می شود، کاربر باید کلید را وارد کند. در حالی که دستگاه فعال است، کلید تنها در حافظه RAM ذخیره می شود. رمزنگاری داده - AES-256. در تلفن های معمولی، کلید رمزگذاری هنگامی ایجاد می شود که ابتدا روشن شده و در یک بخش خاص از حافظه فقط خواندنی یا read-only ذخیره شود. اگر گذرواژه را عوض کنید، تنها کلید اصلی، مجدداً رمزگذاری می شود. در این مورد ما، هنگام تغییر رمز عبور، داده ها با کلید های جدید دوباره رمزگذاری می شوند.

**PIN پنهان یا Panic PIN**

در صورتی که مجبور هستید کد PIN را وارد کنید، PIN پنهان را برای باز کردن قفل صفحه استفاده کنید. همه اطلاعات کاربر را از دستگاه پاک می کند.

کدک های صوتی HD

کدک صدای با کیفیت بالا

**رابط ساده یا حداقلی**

این رابط، ساده اما کامل است، و مجموعه ای از برنامه های کاربردی برای بیشترین کارکردهای مورد استفاده را دارد.

**کارت حافظه موقت (scratch card) برای فعال سازی**

کارت حافظه موقت برای فعال کردن و بازیابی یک دستگاه.

کارت حافظه موقت بر روی کامپیوتر با یک شکاف هوا تولید می شود. لایه خراش، با استفاده از استاندارد PCI DSS اعمال می شود. کارت های حافظه موقت، دارای شماره سریال نیستند. شماره مشترک، پس از فعال سازی اختصاص داده می شود. بنابراین، هیچ کس به جز شخصی که لایه را پاک می کند، عددی را که روی کارت حافظه موقت قرار داده شده و اینکه کدام عدد توسط سرور اختصاص داده است، نمی داند.

**سرورهای مبتنی بر سوئیس**

 تمام سرورها در سوئیس واقع شده اند و با قوانین حریم خصوصی بسیار قوی محافظت می شوند.  تیم خوبی از وکلای سوئیس در انتظار هر گونه چالش هستند. صرفنظر از این، سرورهای ما نمی توانند هیچ گونه مکاتبات یا اطلاعات مشتری را ذخیره کنند و این کار را انجام نخواهند داد.