عنوان	**معرفی نرم افزار امنیتی رمزگذاری و پیشگیری از شنود مکالمات و پیامک تلفن همراه**
عنوان اصلی	**Secure Voice GSM and Secure SMS Software**
کلمات کلیدی	Secure , Voice , GSM , Cell Phone, Operator, Encrypt, intercept, Security, SMS, Call امنیت، پیامک، رمزنگای، شنود، استراق سمع، مکالمه، موبایل، تلفن همراه
مؤلف	
مرجع	http://www.securevoicegsm.com/
سطح	مبتدی
مترجم	مهدی عبداللهی (http://m0911.wordpress.com)
تاریخ انتشار	۲۴ بهمن ۱۳۸۹
تعداد صفحه	۸
فایل های ضمیمه	

آیا مکالمات موبایل شما امن است؟

رقبای شما، هکر ها و جاسوس ها به راحتی می توانند هر مکالمه ی موبایل شبکه های GSM را شنود کنند. شنود مکالمات موبایل به خصوص برای صاحبان صنایع و تکنولوژی، وکلا، دولتمردان و مدیران مراکز امنیتی و نظامی می تواند زیان های سنگین و جبران ناپذیر به دنبال داشته باشد.

یکی از روش های پیشگیری، رمزنگاری صدا در همان زمان مکالمه است بدین ترتیب که نرم افزار رمز نگاری روی گوشی تلفن هر دو طرف مکالمه نصب شود و رمز مشترکی که بین دو نفر مبادله شده است در یک طرف صدا را رمزنگاری کند و در طرف دیگر نیز با همان رمز، داده های صوتی را از حالت رمز درآورد و صدا را برای شنونده پخش کند.

نرم افزار Secure Voice GSM یک نرم افزار کدگذاری بلادرنگ (Rea Time) و دو طرفه (Full Duplex) است یعنی در آن واحد هم می توانید حرف بزنید و هم صدای طرف مقابل را بشنوید. این نرم افزار با اغلب مدل های گوشی نوکیا سازگار است و هیچ نیازی به تغییر در سخت افزار گوشی نیست.

شناسایی تماس توسط یک کلید رمز RSA بر مبنای الگوریتم ۱۰۲۴ بیتی کلید نامتقارن با یک کلید تصادفی صورت می گیرد. (این اصطلاحات توسط افرادی که تحصیلات و تخصص شان در زمینه ی رمزنگاری است به راحتی قابل تفسیر می باشد. مترجم) کدگذاری صدا توسط یک الگوریتم بسیار قوی ARC4 و با استفاده از همان کلید آغازین RSA انجام می شود. تماس های شما به هیچ وجه قابل شنود توسط شخص ثالث نخواهد بود و این صد در صد تضمین شده است. *این نرم افزار آزمایش های امنیتی فوق پیشرفته ی تخصصی را با موفقیت گذرانده و از وزارت دفاع اسرائیل تأییدیه ی امنیتی دارد*

شاید فکر کنید شنود مکالمات فقط توسط اپراتور های مخابراتی انجام می شود. ولی چنین نیست. در زیر به برخی راه ها اشاره می نماییم.

شرکت های خصوصی کارآگاهی (آمریکا و اروپا)

این شرکت ها در بسیاری کشور ها فعال هستند و در برابر هزینه های ناچیز شنود تلفن همراه را برای شما می توانند انجام دهند. در اروپای غربی ۵۰ تا ۱۰۰ یورو برای هر دقیقه مکالمه و در اروپای شرقی بسیار ارزان تر یعنی ۵ تا ۱۰ یورو به ازای شنود هر یک دقیقه مکالمه. همان طور که می بینید برای این کار نیاز به مقادیر زیاد پول ندارید. کافی است آدم این کار را پیدا کنید و بشناسید.

اپراتور های تلفن همراه

طبق قانون های مصوب در اتحادیه ی اروپا اغلب اپراتور ها موظف هستند که مکالمات مشترکان را به مدت ۳ تا ۶ ماه ضبط شده نگه دارند. البته برای این موارد نه فقط در اروپا بلکه در تمامی کشور ها مطابق با حکم قاضی دادگستری شنود و ضبط مکالمات انجام می گیرد و طبیعتا برای کشف موارد جرم و جنایت استفاده می شود. (آن را که حساب پاک است از محاسبه چه باک است!) پلیس اف بی آی به راحتی می تواند به مکالمات زنده ی شما گوش دهد و میکروفون روی موبایل شما را (حتی وقتی گوشی خاموش است) روشن کند.

جاسوسی یک واقعیت دنیای تجارت است

تجهیزات متنوعی در بازار هست که امکان می دهد تا به صورت کاملا پنهان و بدون رد پا مکالمات GSM شنود بشوند. این تجهیزات توسط کمپانی های امنیتی، اعضای شرکت ها و حتی اشخاص حقیقی خریداری می شوند. قیمت ها از ۱۵۰۰۰ دلار آمریکا شروع می شود. تقریبا بیشتر این تجهیزات به صورت سبک و کوچک هستند که به راحتی قابل حمل و نقل می باشند و در هر مکان و موقعیت دلخواه قابل استفاده اند. شنود مکالمات توسط این دستگاه ها در عرض چند دقیقه عملی می شود و به عبارت دیگر شما اصلا احساس نخواهید کرد که مکالمات شما را دارند شنود می کنند. چند مورد از این دستگاه ها را در اینجا معرفی می کنیم:

دستگاه شنود موبایل GSS ProA

این دستگاه موبایل های جی اس ام در باند فرکانس ۹۰۰، ۱۸۰۰ و ۱۹۰۰ مگاهرتز را شنود می کند. این دستگاه می تواند هم ایستگاه اصلی (Base Station) و هم ایستگاه موبایل را به طور هم زمان و مستقل شنود نماید. (برای مشاهده ی توضیح ایستگاه اصلی جی اس ام به آدرس http://en.wikipedia.org/wiki/Base_station_subsystem مراجعه نمایید. مترجم) این سیستم می تواند به صورت خودکار یا دستی تمام مکالمات بین دو تلفن همراه مشخص را شنود و با فورمت استاندارد WAV ذخیره نماید.

امکانات:

- شنود مکالمات موبایل جی اس ام به طور کاملا نامحسوس
- شنود کانال های صوتی رمزنگاری شده ی A5.1، A5.2 و A5.3
- استخراج کی کد (Ki code) یا همان Ki-Grab از فاصله ی ۴ مایلی
- تبدیل کامل عملیات به سمت هر دو تلفن همراه در حال شنود دقیقا مانند اپراتور همراه
- شنود خودکار تمامی تماس های ورودی و خروجی یک تلفن همراه علامت گذاری شده در بانک اطلاعاتی سیستم
- امکان شنود مکالمات بین المللی تلفن همراه
- نگارش استاندارد دارای ۴ کانال دو طرفه است یعنی می تواند همزمان ۴ مکالمه را به صورت زنده شنود و ضبط نماید.
- شنود پیامک، فکس و ایمیل

برای اطلاعات دقیق تر به آدرس http://www.global-security-solutions.com/ProA-GSMInterceptandTracking.htm مراجعه نمایید.

دستگاه نظارت و شنود مکالمات جی اس ام SCL-5020

این دستگاه برای جستجو، شنود و ثبت سیگنال های جی اس ام استاندارد با فرکانس ۹۰۰ و ۱۸۰۰ به صورت ثابت و متحرک ساخته شده است و امکانات آن به شرح زیر است:

نظارت همزمان روی ۱۶ کانال دو طرفه (Full Duplex) جی اس ام. شنود و نظارت و ثبت مکالمات با استاندارد های جی اس ام ۸۵۰، ۹۰۰، ۱۸۰۰ و ۱۹۰۰ مگاهرتز.

برخی از این دستگاه ها امکان اتصال به شبکه ی محلی و ایجاد یک ایستگاه مرکزی مانیتورینگ را دارند.

جستجو و تشخیص خودکار، رمزگشایی و ضبط مکالمات تلفنی و اطلاعات سیستمی شبکه در رسانه ی دیجیتال

برای اطلاعات دقیق تر به آدرس http://www.shoghi.co.in/passive_gsm_interception.htm مراجعه نمایید.

اطلاعات بیشتر در مورد امنیت مکالمات تلفن همراه جی اس ام را در این دو آدرس نیز می توانید ببینید:

- http://www.hackcanada.com/blackcrawl/cell/gsm/gsm-secur/gsm-secur.html
- http://www.securityprousa.com/cein.html

امکانات نرم افزار SV GSM

- بالا ترین میزان رمزنگاری با استاندارد نظامی
- رمزنگاری بسیار قوی نامتقارن به روش RSA ۱۰۲۴ بیت
- تولید خودکار کلید رمز RSA 1024
- تبادل کلید به روش دفی-هلمن ۴۰۹۶ بیت (Diffie-Hellman)
- حفاظت جریان RSA
- شناسایی با سه فاکتور
- پایین ترین حالت پنهان سازی صدا
- ترکیب مضاعف رمزنگاری متقارن و نامتقارن
- کلید تصادفی، با جایگزین ۱۰ مرتبه در هر ثانیه
- کیفیت صدای عالی بدون مکث
- قابل استفاده در اغلب شبکه های جی اس ام
- بدون نیاز به اتصال اینترنت
- دو طرفه
- رابط کاربری آسان بدون نیاز به دانش و مهارت امنیتی
- بدون نیاز به دخالت کاربر هنگامی که اتصال امن بین دو تلفن همراه برقرار شود
- تشخیص و رفع حالت استراق سمع توسط شخص ثالث
- قابل استفاده روی اغلب تلفن های همراه با سیستم عامل سیمبیان

کاملا سازگار با تلفن های همراه نوکیا مدل های زیر:

N70, N71, N72, N73, N73 Music Edition, N75, N76, N77, N93, N93i, N80, N90, N91, N91 8GB, E70, E61, E62, E63, E60, E50, 6630, 6680, 6681, Nokia 5230, Nokia 5530 XpressMusic, Nokia 5800 XpressMusic, Nokia N97, Nokia N97 mini, Nokia X6

این نرم افزار در گوشی های مدل زیر بسته به تنظیمات CSD شبکه ی جی اس ام کار خواهد کرد:

Nokia N76, Nokia N78, Nokia N79, Nokia N81 8GB, Nokia N82, Nokia N85, Nokia N91 8GB, Nokia N93i, Nokia N95, Nokia N95 8GB, Nokia N96, Nokia E61i, Nokia E63, Nokia E90, Nokia E66, Nokia E71, Nokia 6110 Navigator, Nokia 6121, Nokia 6124, Nokia 6210 Navigator, Nokia 6220 Classic,Nokia 6290

لازم به ذکر است که این نرم افزار در حال حاضر فقط با استاندارد شبکه ی جی اس ام سازگار است و همچنین امکان مکالمه ی CSD باید روی سیمکارت فعال باشد. (برای اطلاعات دقیق تر به آدرس http://www.securegsm.com/pages.php?pageid=42 مراجعه نمایید)

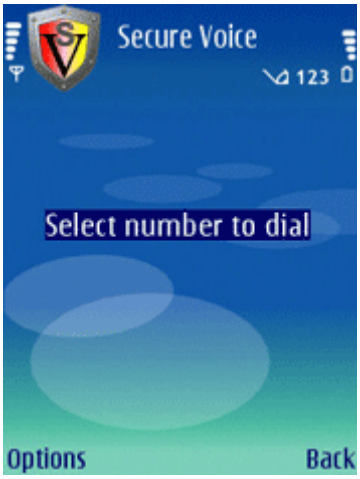
این سرویس توسط همه ی اپراتور ها پشتیبانی نمی شود و ممکن است برای استفاده از این نیاز به ثبت نام جداگانه داشته باشید.

نرم افزار SV GSM از کانال صوتی تلفن همراه استفاده نمی کند بلکه داده های صوتی رمزنگاری شده را از طریق کانال دیتا ی تلفن همراه ارسال می نماید. این کار باعث می شود که شنود کننده های کانال صوتی حتی متوجه نشوند که شما در حال مکالمه با تلفن همراه هستید. هزینه ی مکالمه ی رمزنگاری شده با هزینه ی مکالمه ی عادی برابر است. این نرم افزار در برابر هر نوع نرم افزار شنود جاسوس روی تلفن همراه نیز گارانتی شده است. (برای اطلاعات دقیق تر در خصوص این نرم افزارهای جاسوس به آدرس http://www.thespyphone.com مراجعه نمایید) *توجه داشته باشید که این نرم افزار باید روی تلفن همراه هر دو طرف مکالمه نصب شده باشد.*

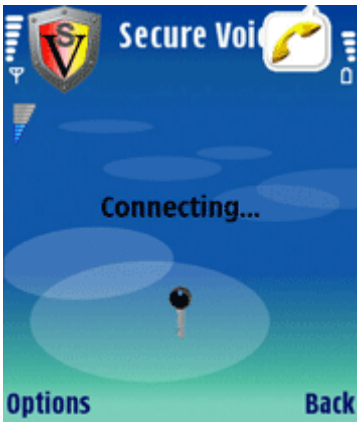
فعلا استاندارد شبکه های UMTS، 3G و CDMA توسط این نرم افزار **پشتیبانی نمی شوند**.

نحوه ی کار نرم افزار SV GSM

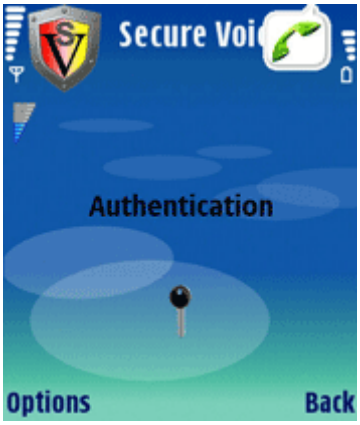
این نرم افزار در پس زمینه اجرا می شود و مقدار کمی از منابع سیستم را استفاده می نماید. در زیر تصاویری از نرم افزار را می بینید:



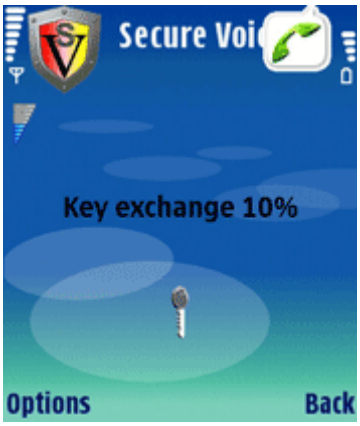
۱- صفحه ی اصلی برنامه: می توانید شماره ی تماس را مستقیم وارد کنید یا از دفتر تلفن فرد مرود نظر تان را انتخاب نمایید.



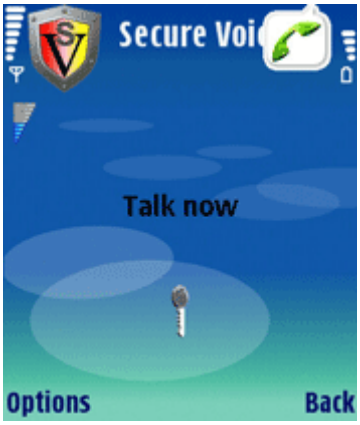
۲- با فشردن دکمه ی شماره گیری، برنامه ی SV GSM شروع به کار می کند تا یک اتصال امن با تلفن همراه مقصد ایجاد کند به شرط این که این نرم افزار روی تلفن همراه گیرنده هم نصب شده باشد.



۳- پس از برقراری تماس، فرایند شناسایی شروع می شود



۴- پس از شناسایی، تبادل کلید رمزنگاری آغاز می شود.



۵- در این مرحله اتصال رمزنگاری شده برقرار می گردد و شما می توانید به صورت ایمن مکالمه تان را آغاز نمایید.

اطلاعات فنی نرم افزار Secure Voice GSM

الگوریتم رمزنگاری صدا: AES 256 یا ARC4

الگوریتم تبادل کلید رمز: دفی – هلمن ۴۰۹۶ (Diffie-Hellman)

الگوریتم شناسایی تماس: RSA 1024 Key

فشرده سازی صدا: AMR-NB 4.75Kbps

کدینگ صدای رمزنگاری شده: دو طرفه (Full Duplex) و انتهایی End-to-End

پشتیبانی از رومینگ

تشخیص و پیشگیری استراق سمع (Man in the middle protection)

رمزنگاری پیامک

استاندارد فعلی ارسال پیامک ایمن نیست بدین معنی که به هنگام ارسال در چندین جا می تواند شنود گردد. این نرم افزار می تواند پیامک های شما را نیز رمزنگاری و محافظت نماید. رمزنگاری پیامک در شبکه های GSM و CDMA امکان پذیر است.

نرم افزار Secure SMS کاربری آسان و البته پشت صحنه و ساختار بسیار پیچیده ای دارد. این نرم افزار در مبداء پیامک را رمزنگاری و در مقصد رمزگشایی می نماید. (end-to-end encryption)

با استفاده از الگوریتم AES 256 برای رمزنگاری و بدون نیاز به سرویس های شبکه ی خاص مانند CSD، HSCSD، GPRS و 3G می تواند روی استاندارد شبکه ی GSM یا CDMA در هر جای دنیا پیامک های شما را رمزنگاری کند. (برای اطلاعات دقیق تر در خصوص الگوریتم رمزنگاری AES 256 به آدرس http://en.wikipedia.org/wiki/Advanced_Encryption_Standard مراجعه نمایید)

پیامک رمزنگاری شده قابل خوانده شدن نیست و مانند یک سری کاراکتر در هم و بر هم (خزعبلات) دیده خواهد شد. به علاوه اگر تلفن همراه گیرنده فاقد نرم افزار Secure SMS باشد، پیامک های رمزنگاری شده روی آن قابل خواندن نخواهد بود. پس از نصب این نرم افزار روی تلفن همراه، از طریق منوی اصلی می توان از آن استفاده کرد لیکن برای امنیت بیشتر امکان گذاشتن رمز عبور برای اجرای نرم افزار نیز فراهم می باشد. نحوه ی کار با این نرم افزار دقیقا مانند نرم افزار ارسال پیامکی است که از اول روی تلفن همراه قرار دارد.

کلید رمز نگاری در هر زمان توسط کاربر قابل تغییر است و بهتر است که به طور مداوم این کلید را تغییر دهید. در ضمن هیچکدام از کلید های رمزنگاری به هنگام ارسال پیامک، مبادله نمی شوند بلکه تطبیق کلید ها توسط نرم افزار و هنگام اجرا روی تلفن همراه انجام می شود که از این بابت می توان به ایمن بودن کلید های رمزنگاری نیز مطمئن بود.

گوشی های تلفن همراه سازگار با این برنامه

تقریبا تمامی اسمارت فون های سازگار با J2ME این نرم افزار را می توانند اجرا کنند. مدل های گوشی نوکیا سازگار با این نرم افزار عبارت است از:

Nokia E Series: E50, E51, E52, E55, E60, E61, E61i, E62, E63, E65, E66, E70, E71, E71x, E72, E75.
Nokia N Series: N73, N76, N77, N78, N79, N80, N81, N81 8GB, N82, N85, N86 8MP, N91, N95, N95 8GB, N96. N97, N97 mini.
Nokia: 3250, 5320 XpressMusic, 5500, 5630 XpressMusic, 5700 XpressMusic, 6110 Navigator, 6120 Classic, 6121 Classic, 6124, 6210 Navigator, 6220 Classic, 6710 Navigator, 6720 classic, Nokia 6730 classic, Nokia 6700 slide, Nokia 6788, Nokia X6, Nokia 6790 slide, Nokia 6760 slide, Nokia 6790 Surge, Nokia 5530 XpressMusic