آزمایشگاه و مرکز تخصصی آپا
در زمینه اختلالات امنیتی مرتبط با سیستم های رمزنگاری

مطالب علمی آموزشی

بررسی امنیت سرویس پیام کوتاه

محسن تورانی
دانشکده مهندسی برق
دانشگاه علم و صنعت ایران
mtoorani@ee.iust.ac.ir

محمود احمدیان
دانشکده مهندسی برق
دانشگاه خواجه نصیرالدین طوسی
mahmoud@eetd.kntu.ac.ir

حوزه علمی آموزشی

۱۳۸۷

چکیده: با توجه به گسترش روز افزون استفاده از تلفن همراه، تامین و تضمین امنیت ارتباطات امری اجتناب ناپذیر است. از سالها پیش مشخص شده که GSM، با وجود دارا بودن بیشترین تعداد کاربر، دارای اشکالات و معایب امنیتی فراوان و فاقد ویژگیهای یک شبکه امن است به گونه‌ای که تمامی مکالمات و حتی پیامهای کوتاه ارسالی به راحتی و تحت شرایط خاصی قابل شنود، کشف و یا تغییر می‌باشند. سرویس پیام کوتاه یکی از اولیه‌ترین و پراستفاده‌ترین سرویس‌های ارائه شده توسط GSM و سایر سیستمهای سیار است که توسط اکثر اپراتورهای تلفن همراه ارائه می‌شود. در این مقاله، موضوع امنیت سرویس پیام کوتاه مورد بررسی قرار خواهد گرفت. از آنجا که امنیت سرویس پیام کوتاه به امنیت شبکه سیار مورد استفاده نیز وابسته است، امنیت GSM و نسخ ارتقا یافته آن نیز به طور خلاصه در این مقاله مورد ارزیابی قرار خواهد گرفت.

کلمات کلیدی: امنیت سرویس پیام کوتاه (SMS)، امنیت GSM، امنیت انتها به انتها، شنود غیرقانونی

۱- مقدمه

استفاده از تلفن همراه در میان جوامع بشری با رشد و استقبال روز افزونی مواجه شده است. در انتهای سال ۲۰۰۷، تعداد مشترکین تلفن همراه در جهان از مرز ۳/۳۳ میلیارد نفر گذشت که از این میان، ۲/۸۸ میلیارد نفر مشترکین شبکه GSM[1] (با احتساب نسخ ارتقا یافته‌اش) بوده‌اند. این در حالی است که تعداد مشترکین UMTS[2] فقط ۱۹۶ میلیون نفر بوده است [۱]. سرویس پیام کوتاه (SMS)[3] یکی از ابتدایی‌ترین و پرکاربردترین سرویس‌های ارائه شده در GSM، IS-95 و سایر سیستمهای سیار است. SMS در سالهای اخیر بسیار پر طرفدار بوده است. طبق برآورد انجام شده حدود ۱۰ درصد درآمد اپراتورها از محل پیامهای کوتاه کاربران و فقط ۰/۵ درصد درآمد آنها از محل WAP[4] بوده است. SMS علاوه بر کاربرد گسترده و کم هزینه‌ای که در ارتباطات بین فردی دارد، می‌تواند در کاربردهایی مورد استفاده قرار گیرد که یک طرف ارتباط در آنها یک سیستم اطلاعاتی است. کنترل

[1] Global System for Mobile Communications
[2] Universal Mobile Telecommunications System
[3] Short Message Service
[4] Wireless Application Protocol

لوازم و تجهیزات از راه دور، آموزش الکترونیکی، برگزاری انتخابات و نظرسنجی، خدماتی نظیر سرویس مقایسه قیمتها، تبلیغات و در نهایت تجارت و پرداخت سیار، بخش کوچکی از این قبیل کاربردها است که در بسیاری از آنها، مقوله امنیت از اهمیت ویژه‌ای برخوردار است.

در این مقاله، امنیت سرویس پیام کوتاه مورد بررسی قرار خواهد گرفت. از آنجا که امنیت سرویس پیام کوتاه با امنیت سیستم سیار مورد استفاده پیوند خورده است، در بخش ۲ اصول امنیتی GSM (به عنوان پرکاربرترین سیستم تلفن همراه دنیا)، در بخش ۳ مشکلات امنیتی آن، در بخش ۴ امنیت نسخ ارتقا یافته GSM و در بخش ۵ امنیت سرویس پیام کوتاه و راهکارهای برقراری امنیت انتها به انتها مورد بررسی قرار خواهد گرفت.

۲- اصول امنیتی GSM

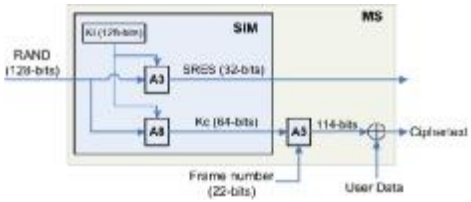
اهداف امنیتی در GSM عبارتند از:

- استفاده از سیم‌کارت به عنوان ماژول امنیتی
- احراز اصالت مشترک برای شبکه
- حفظ محرمانگی ترافیک کاربر و داده‌های کنترلی در مقابل شنود: با استفاده از رمزنگاری
- ناشناس یا محرمانه ماندن هویت مشترک (IMSI[۵]): با تخصیص TMSI[۶]
- استفاده از مشخصه تجهیزات (EID[۷]) که مطمئن می‌سازد هیچ ME[۸] غیرمجاز یا مسروقه‌ای در شبکه به کار نمی‌رود.

هر مشترک به یک سیم‌کارت احتیاج دارد و بدون آن هیچ سرویسی قابل ارائه نمی‌باشد. سیم کارت حاوی تمامی اطلاعات لازم جهت دسترسی به حساب کاربر است و به عنوان یک کارت هوشمند، از خصوصیات امنیتی ویژه‌ای برخوردار می‌باشد. بر روی سیم کارت هر مشترک IMSI[۹] و Ki[۱۰] ذخیره شده است. IMSI عددی عددی حداکثر ۱۵ رقمی است که به طور انحصاری به هر مشترک شبکه در جهان اختصاص داده می‌شود. Ki نیز کلید رمزنگاری ریشه و عبارت از یک عدد تصادفی ۱۲۸ بیتی است که به هر مشترک شبکه اختصاص می‌یابد. Ki به شدت حفاظت شده و فقط در سیم کارت مشترک و مرکز احراز اصالت شبکه (AuC[۱۱]) ذخیره

[5] International Mobile Subscriber Identity
[6] Temporary Mobile Subscriber Identity
[7] Equipment ID
[8] Mobile Equipment
[9] International Mobile Subscriber Identity
[10] Individual subscriber authentication Key
[11] Authentication Center

می‌شود. خود سیم کارت توسط PIN[12] کاربر محافظت می‌شود و چنانچه کاربر نتواند پس از چند بار تلاش PIN PIN را به درستی وارد نماید، از او PUK[13] تقاضا می‌شود و چنانچه پس از تعداد مشخصی تلاش، PUK نیز اشتباه وارد شود، سیم کارت دسترسی به اطلاعات محلی و توابع احراز اصالت خود را به طور دایم غیر فعال نموده و غیر قابل استفاده خواهد شد. احراز اصالت و محرمانگی داده‌های کاربر در گرو حفظ محرمانگی دو عدد IMSI و Ki است و در صورتی که این دو عدد لو برود، هر کسی می‌تواند خود را به جای مشترک مورد نظر جا بزند. بر روی سیم کارت هر مشترک، دو الگوریتم A3 (جهت احراز اصالت مشترک برای شبکه) و A8 (جهت تولید کلید جلسه Kc[14] که در رمزنگاری مکالمات و داده‌های مشترک مورد استفاده قرار می‌گیرد) نیز پیاده‌سازی شده است. شبکه در مواقع لازم یک چالش تصادفی (RAND) برای کاربر ارسال می‌نماید تا سیم کارت وی به کمک Ki و الگوریتم A3/A8، اصالت خود را برای شبکه ثابت و مبادرت به تولید کلید جلسه Kc جدید نماید. از آن پس، شبکه در هر زمان می تواند از MS[15] بخواهد که عملیات رمزنگاری را با استفاده از کلید جلسه تولید شده (Kc) انجام دهد. فرآیند احراز اصالت، تولید کلید جلسه و رمزگذاری GSM در شکل (۱) نشان داده شده است.



شکل ۱- فرآیند احراز اصالت، تولید کلید جلسه و رمزگذاری در GSM [۲]

الگوریتم‌های رمزنگاری بر روی گوشی تلفن همراه به صورت سخت افزاری پیاده‌سازی شده‌اند. شبکه می‌تواند از میان چندین نوع الگوریتم رمزی که گوشی کاربر قادر به پشتیبانی از آن می‌باشد, یکی را انتخاب کند. در حال حاضر سه نوع الگوریتم رمز A5/1، A5/2 و A5/3 تعریف شده‌اند که A5/1 و A5/2 الگوریتمهای اصلی هستند که در استاندارد GSM تعریف شده و از نوع الگوریتمهای رمز جریانی[16] می‌باشند؛ با این تفاوت که A5/1 به مراتب قوی‌تر از A5/2 است. الگوریتم رمز A5/3 نیز که در سال ۲۰۰۲ و برای استفاده در نسل سوم

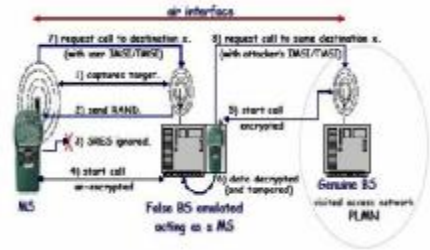
[12] Personal Identification Number
[13] PIN UnlocK
[14] Ciphering Key
[15] Mobile Station
[16] Stream cipher

تلفن همراه تعریف شد، نوعی الگوریتم رمز قالبی[17] است که مبتنی بر الگوریتم رمز کازومی بوده و از امنیت به مراتب بیشتری برخوردار است. توضیحات بیشتر در خصوص مبانی امنیت GSM را می‌توان در مراجع مرتبط یافت [۲، ۴ و ۵].

۳- مشکلات امنیتی GSM

علیرغم آنکه GSM با هدف ایجاد یک سیستم سیار امن طراحی شده و احراز اصالت کاربر و رمزنگاری مبادلات هوایی را مدنظر قرار داده بود، در برابر بسیاری از حملات که هر کدام بخشی از شبکه را هدف قرار می‌دهند, به شدت آسیب پذیر است. محرمانگی پیام، تمامیت[18]، احراز اصالت، عدم انکار[19]، کنترل دسترسی[20] و در دسترس بودن[21] از مهمترین سرویس‌های امنیتی هستند که باید توسط یک شبکه امن تامین شوند [۳] اما GSM در تامین این سرویس‌ها با مشکل مواجه است. در ادامه, به مهمترین مشکلات امنیتی GSM اشاره خواهد شد [۲].

۱- استفاده از پروتکل احراز اصالت یک سویه و امکان حمله مرد میانی[22]: به این معنی که کاربر باید اصالت خود را به شبکه ثابت کند و شبکه اصالت خود را به کاربر اثبات نمی‌نماید. این امر منجر به امکان انجام حمله مرد میانی از طریق اعمال BTS قلابی[23] می‌شود. در این حمله، حمله‌گر با قرار دادن یک ایستگاه فرستنده- گیرنده که کد شبکه موبایل واقعی را دارد، خود را به عنوان ایستگاه فرستنده- گیرنده پایه واقعی جا می‌زند و به عنوان واسطه‌ای بین کاربر و شبکه واقعی قرار گرفته، مبادرت به شنود و یا حتی تغییر پیامها و مکالمات کاربر می‌نماید. فرآیند این امر در شکل (۲) نشان داده شده است. سناریوهای متعددی جهت سوء استفاده از این نقطه ضعف قابل طرح و اجرا است که جهت اختصار به آنها نمی‌پردازیم.



[17] Block cipher
[18] Integrity
[19] Non-repudiation
[20] Access Control
[21] Availability
[22] Man-in-the-middle attack
[23] False BTS (Base Transceiver Station)

شکل ۲- ایستگاه پایه قلابی [۵]

۲- اشکال در پیاده‌سازی الگوریتمهای A3/A8: با وجود آنکه طراحی GSM به اپراتور اجازه می‌دهد تا هر الگوریتمی را که می‌خواهد برای توابع A3 و A8 انتخاب کند، بسیاری از اپراتورها از همان الگوریتم موسوم به COMP128 (یا COMP128-1) که توسط انجمن GSM و به صورت مخفیانه طراحی شده بود، استفاده می‌نمایند. ساختار COMP128-1 در نهایت به کمک مهندسی معکوس و اسناد لو رفته GSM مشخص و اشکالات امنیتی فراوانی در آن کشف شد. این الگوریتم علاوه بر اینکه امکان نشت کلید سری Ki را فراهم می‌کند (مخصوصا هنگامی که چالشهای تصادفی خاصی به آن اعمال شود)، ۱۰ بیت سمت راست کلید جلسه ۶۴ بیتی Kc تولید شده را تعمدا برابر صفر قرار می‌دهد که این امر منجر به کاهش فضای کلید الگوریتم رمز مورد استفاده خواهد شد و این امر مستقل از نوع الگوریتم رمزنگاری مورد استفاده، الگوریتم رمزنگاری را حدود ۱۰۲۴ مرتبه ضعیفتر و شکست پذیرتر خواهد نمود. برخی از اپراتورهای GSM, به سوی پیاده‌سازی جدیدتری از A3/A8، یعنی یک الگوریتم جدید و محرمانه، موسوم به COMP128-2 گام برداشته‌اند که به جز به ارث بردن یکی از ضعفهای عمده COMP128-1 یعنی فضای کلید کاهش یافته، اشکال امنیتی دیگری تاکنون در خصوص آن گزارش نشده است. از چندی پیش, الگوریتم COMP128-3 نیز پیشنهاد شده که مشابه COMP128-2 است؛ با این تفاوت که در آن، Kc به صورت کامل (۶۴ بیتی) تولید می‌شود و این امر، امکان بهره‌برداری از حداکثر قدرت الگوریتم رمزنگاری مورد استفاده را فراهم می‌آورد.

۳- حمله به سیم کارت و کپی سیم کارت[۲۴]: یکی از خطرناک‌ترین انواع حملات، استخراج کلید سری Ki از سیم کارت مشترک است. برای اولین بار انجمن توسعه دهندگان کارت هوشمند و گروه تحقیقاتی ISAAC، اشکال عمده‌ای در الگوریتم COMP128-1 کشف نمودند که به طور موثری آنها را قادر می‌ساخت با ارسال تعداد زیادی چالش به سیم کارت، کلید سری Ki را در حدود زمان هشت ساعت استخراج نمایند. پس از آن, حملات دیگری مبنی بر ارسال چالشهای انتخابی به سیم کارت نیز پیشنهاد شدند که قادر به استخراج کلید سری در مدت زمانی به مراتب کمتر بودند. سرانجام در سال ۲۰۰۲, یک تیم تحقیقاتی از شرکت IBM روش جدیدی مبتنی بر استفاده از کانالهای جانبی[۲۵] کشف نمودند که به وسیله آن، هکری که سیم کارت مشترک را فقط به مدت یک دقیقه در اختیار داشته باشد، قادر به استخراج کلید سری (Ki) وی خواهد بود. او به کمک

[24] SIM Card Cloning
[25] Side-Channel attack

عدد به دست آمده خواهد توانست سیم کارتی مشابه سیم کارت مشترک هدف تولید نموده و از آن سوء استفاده نماید. البته مشکل کوچکی نیز در استفاده از سیم کارتهای کپی شده وجود دارد و آن اینکه GSM در هر لحظه فقط به یک مشترک اجازه دستیابی به شبکه را می‌دهد. بنابراین اگر حمله‌گر و مشترک اصلی در یک زمان تلاش کنند تا به شبکه دسترسی پیدا کنند، شبکه خواهد فهمید که دو سیم کارت مشابه در دو موقعیت متفاوت وجود دارند و بلافاصله حساب مربوطه را مسدود و دسترسی هر دوی آنها را ممنوع خواهد ساخت.

٤- خطر استخراج کلید سری بدون تماس فیزیکی با سیم کارت: حمله‌گر می‌تواند از نقطه ضعف COMP128-1 استفاده نموده، حتی بدون در اختیار گرفتن سیم کارت مشترک مربوطه و از طریق ارتباطات رادیویی و ارسال چالشهای متعدد و دریافت پاسخ از مشترکی که TMSI یا IMSI او مشخص شده، اقدام به محاسبه کلید Ki وی نموده، یک کپی از سیم کارت او تهیه نموده و مبادرت به برقراری و یا دریافت تماسها و داده‌ها, با استفاده از حساب کاربری مشترک هدف قرار گرفته شده بنماید. البته استخراج کلید بدین طریق، چند ساعت به طول خواهد انجامید.

٥- ضعف شدید الگوریتمهای رمزنگاری مورد استفاده: باور عمومی بر این است که الگوریتم A5/2 با حدود 2^{16} گام در زمان واقعی[26] قابل شکست می‌باشد. در کاراترین حمله انجام شده بر این الگوریتم، احتیاج به کمتر از یک ثانیه مکالمه رمز شده با A5/2 می‌باشد تا در مدت زمانی کمتر از یک ثانیه، کلید رمز با استفاده از یک کامپیوتر معمولی استخراج شود [۶]. الگوریتم رمز A5/1 نیز که در ابتدا برای استفاده در اروپا طراحی شده بود, به دلیل مخفی کاری و مکتوم ماندن اشتباهات به درستی طراحی نشد و با حداکثر 2^{40} گام قابل شکست می‌باشد. مولفین [۷] از رخنه‌های ظریف موجود در ساختار فیدبک رجیسترها در A5/1 استفاده نموده و با فرض استفاده از COMP128-1 در پیاده‌سازی A3/A8، حمله‌ای را پیشنهاد داده‌اند که مبتنی بر یک مرحله پیش پردازش با 2^{48} عملیات می‌باشد و با استفاده از نتایج ذخیره شده این پیش پردازش، حمله به A5/1 بر روی یک کامپیوتر شخصی در زمان واقعی و به دو صورت زیر قابل انجام خواهد بود: در حالت اول به خروجی الگوریتم A5/1 در دو دقیقه اول مکالمه احتیاج است تا کلید Kc در کمتر از یک ثانیه استخراج شود و در حالت دوم، به خروجی الگوریتم A5/1 برای مدت دو ثانیه از مکالمه احتیاج است تا کلید Kc در زمان حدود دو دقیقه استخراج شود. تفاوت بین این دو حالت تنها در موازنه بین حافظه مصرفی و زمان می‌باشد.

[26] Real-time

۶- کوتاه بودن دامنه حفاظت و مشکلات امنیتی ستون فقرات GSM: احراز اصالت و محرمانگی در GSM صرفاً ارتباط بین MS و BTS سرویس دهنده را حفاظت می‌کند، در حالی‌که کلیه مبادلات بین سایر اجزا به صورت معمولی و رمز نشده انجام می‌شود. این در حالی است که ارتباط بین BTS ها با یکدیگر و یا شبکه معمولاً از طریق لینکهای مایکروویو -که به راحتی قابل شنود می‌باشند- انجام می‌شود. لذا نفوذگر با نفوذ به قسمت ثابت GSM خواهد توانست به اهداف خود دست یابد. سیستمهای سیار در اصل از سیستم سیگنالینگ شماره ۷ (SS7[۲۷]) به منظور ارتباط بین شبکه‌ها و برای فعالیتهایی نظیر احراز اصالت، به روز رسانی موقعیت، سرویس‌های تکمیلی و کنترل تماسها استفاده می‌نمایند، در حالی که امنیت SS7 به نوبه خود جای بحث دارد. بزرگترین آسیب‌پذیری SS7 ناشی از تعدد و پیچیدگی واسطهای بین موجودیتهای مستقل در آن است. همچنین استفاده از اتصالات داخلی شبکه و اینترنت به طور نمایی در حال رشد می‌باشد که زمینه‌ساز آسیب‌پذیری‌های مضاعفی خواهد بود. مشکل سیستمهای SS7 عمومی این است که پیامها به صورت غیرقابل کنترلی قابل تغییر، تزریق و یا حتی حذف می‌باشند. این امر، این امکان را فراهم می‌آورد تا حمله‌کننده با تولید پیامهای SS7 و اعمال آنها به شبکه، قادر به در هم گسیختن سرویس‌ها و حتی برقراری تراکنشهایی باشد.

۷- معلوم نبودن وضعیت رمزنگاری برای کاربر: کاربر اطلاعی از فعال بودن یا نبودن رمزنگاری ندارد و اختیار این امر با شبکه است و لذا یک BTS قلابی می‌تواند حالت بدون رمزنگاری را انتخاب نموده و مشترک شبکه را مجبور به ارسال داده‌ها در حالت آشکار و بدون رمزنگاری نماید.

۸- ضعف در حفظ گمنامی کاربران: در GSM این قاعده پیش‌بینی شده که اگر مشترک برای بار اول وارد شبکه شود و یا به هر دلیلی جدول نگاشت بین IMSI و TMSI در شبکه از بین برود، شبکه از مشترک تقاضای اعلام IMSI را بنماید. چون این اعلام در حالت آشکار و بدون رمزنگاری خواهد بود، حمله‌گر می‌تواند از این امر سوء استفاده کند.

۹- امکان حمله اختلال در سرویس[۲۸]: حمله‌کننده می‌تواند به طور مکرر با مشخصات مختلف با شبکه ارتباط برقرار نموده و تقاضای تخصیص کانال نماید و بدین نحو تمام کانالهای خالی یک سلول را اشغال نموده، مانع ارتباط سایر مشترکین با شبکه شود. این حمله از آن جهت امکان پذیر است که در پروتکل برپایی ارتباط، هیچ مکانیزمی برای احراز اصالت کاربر و حفظ تمامیت اطلاعات سیگنالینگ در نظر گرفته نشده است. این

[27] Signaling System #7
[28] Denial of Service attack (DoS attack)

حمله, هزینه‌ای برای حمله‌کننده در بر نخواهد داشت، ضمن آنکه شبکه نیز نخواهد توانست وقوع چنین حمله‌ای را تشخیص دهد.

۱۰- عدم حفظ تمامیت اطلاعات: علیرغم آنکه معماری امنیتی GSM احراز اصالت و محرمانگی را مدنظر قرار داده است، ملاحظه‌ای برای حفظ تمامیت اطلاعات صورت نگرفته است [۴]. بنابراین گیرنده نمی‌تواند مطمئن باشد که داده‌های دریافت شده همان داده‌های ارسال شده هستند.

۱۱- امکان استفاده از حملات تکرار[۲۹]: حمله‌کننده می‌تواند از اطلاعات مبادله شده قبلی بین کاربر و شبکه سوء استفاده نماید. به عنوان مثال, پروتکل چالش-پاسخ احراز اصالت در برگیرنده مهر زمانی نمی‌باشد. بنابراین چنانچه یک BTS قلابی به طرز موفقیت آمیزی خود را به عنوان BTS واقعی جا بزند, قادر به حفظ کلید جلسه خواهد بود که برای مدت احتمالا مدیدی به او اجازه رمزگشایی داده‌هایی را خواهد داد که با استفاده از این کلید، رمز می‌شوند. نمونه دیگری از حمله تکرار مبتنی بر استفاده مجدد از بردار احراز اصالت است که ممکن است چندین بار توسط شبکه مورد استفاده قرار بگیرد.

۱۲- افزایش افزونگی[۳۰] به دلیل انجام کدینگ قبل از رمزنگاری: در GSM، کدینگ تصحیح خطا قبل از انجام عمل رمزنگاری صورت می‌پذیرد که این امر باعث افزایش همبستگی پیام شده و انجام حمله به الگوریتمهای رمزنگاری را تسهیل می‌نماید.

موارد ذکر شده صرفا به تعدادی از مهمترین مشکلات امنیتی GSM اشاره دارند. سناریوهای متعددی برای سوء استفاده عملی از این اشکالات قابل طرح و اجرا است که به لحاظ اختصار، از بیان آن خودداری می‌شود. موارد ذکر شده به خوبی بیانگر این نکته است که GSM فاقد ویژگیهای یک شبکه امن است. شایان ذکر است که هم اینک تجهیزات شنود مکالمات GSM به شکل تجاری عرضه شده و مورد معامله قرار می‌گیرند [۸].

٤- امنیت نسخ ارتقایافته GSM

مشخصات و ویژگیهای GSM ثابت نبوده بلکه تاکنون بارها مورد بازنگری قرار گرفته است که این امر منجر به پیدایش GPRS[۳۱]، EDGE[۳۲] و ... شده است. مدل مورد استفاده در GSM با تغییرات گسترده هم اینک تا نسل سوم تلفن همراه نظیر UMTS نیز ادامه پیدا کرده است؛ به گونه‌ای که این تغییرات هم اینک نرخ انتقال داده را

[29] Replay attack
[30] Redundancy
[31] General Packet Radio Service
[32] Enhanced Data rates for GSM Evolution

از ۹/۶ Kbps در GSM نسل دوم به حداکثر ۲ Mbps در UMTS نسل سوم افزایش داده است. GSM همچنان پرکاربردترین سیستم تلفن همراه جهان است. البته به غیر از آفریقا و بخشی از خاورمیانه، در بسیاری از نقاط جهان از نسخ ارتقا یافته GSM, یعنی GPRS و EDGE استفاده می‌شود. سیستمهای تلفن سیار آمریکایی, مقوله جدایی است که مکانیزمهای امنیتی آن با GSM متفاوت است و در این مقاله به آن نخواهیم پرداخت.

در سال ۲۰۰۲ تلاشهایی جهت طراحی یک الگوریتم رمزنگاری جدید برای استفاده در GSM، ECSD[۳۳]، GPRS و EGPRS[۳۴] انجام شد تا این الگوریتم در گوشیهای دو موده[۳۵]–که هم در GSM و هم در UMTS نسل سوم کار می‌کنند– پیاده‌سازی شود. در نهایت الگوریتم A5/3 برای GSM و ECSD/EDGE، الگوریتم GEA3 برای GPRS و f8 برای UMTS پیشنهاد شد که تمامی این الگوریتمها دارای وجه مشترکی با یکدیگر می‌باشند. مکانیزمهای امنیتی GPRS شبیه به GSM است. در GPRS به جای استفاده از الگوریتم A5 از الگوریتم GEA[۳۶] استفاده می‌شود که در حال حاضر سه نسخه از آن موجود است: GEA1، GEA2 و GEA3. همچنین پایانه انتهایی رمزنگاری به نقطه عمیق‌تری در شبکه, یعنی از ایستگاه پایه به SGSN[۳۷] منتقل شده است. در GSM رمزنگاری در لایه فیزیکی انجام می‌شود در حالی‌که در GPRS, این عمل در لایه سوم شبکه یا به عبارت دقیق‌تر در لایه LLC[۳۸] صورت می‌پذیرد. در GPRS و EDGE، برخی از نقاط ضعف امنیتی GSM برطرف شده و برخی دیگر همچنان وجود دارند. ضمن آنکه به دلیل اتصال به اینترنت، زمینه جدیدی برای آسیب‌پذیری ایجاد شده است.

در UMTS نیز مشکلات امنیتی GSM مورد بازبینی عمیق قرار گرفته و بسیاری از آنها برطرف شده است. بررسی مکانیزمهای امنیتی UMTS در این مقال نمی‌گنجد ولی به طور کلی الگوریتمهای مورد استفاده در UMTS از لحاظ امنیتی با مشکل جدی روبرو نیستند و حملات انجام شده بر روی این الگوریتمها صرفا جنبه نظری داشته و در حال حاضر به صورت عملی قابل انجام نیستند. با این وجود در UMTS نیز برخی مشکلات امنیتی وجود دارد که غالبا مربوط به پروتکلهای مورد استفاده است. همچنین به دلیل ورود سرویس دیتا، نقطه جدیدی برای آسیب‌پذیری از طریق حملات مبتنی بر IP ایجاد شده است.

[33] Enhanced Circuit Switched Data
[34] Enhanced GPRS
[35] Dual-mode
[36] GPRS Encryption Algorithm
[37] Serving GPRS Support Node
[38] Logical Link Control

۵- امنیت سرویس پیام کوتاه

سرویس پیام کوتاه یکی از پرکاربردترین سرویس‌های ارائه شده توسط GSM، IS-95 و سایر سیستمهای سیار است. SMS یک سرویس مبتنی بر ذخیره- و- ارسال[۳۹]، آسان برای استفاده، عمومی و مردم پسند و با هزینه‌ای بسیار پایین است. سرویس پیام کوتاه در عرصه مخابرات بی‌سیم از سال ۱۹۹۱ و در اروپا ظاهر شد و استانداردهای GSM از همان ابتدا، در برگیرنده سرویس پیام کوتاه بودند. SMS مکانیزمی جهت انتقال پیام کوتاه به و از وسایل بی سیم در اختیار می‌گذارد. این سرویس از یک مرکز سرویس پیام کوتاه (SMSC)[۴۰] بهره می‌گیرد که به عنوان یک سیستم ذخیره و ارسال برای پیامهای کوتاه عمل می‌کند و شبکه بی‌سیم، مسئولیت انتقال پیامهای کوتاه بین SMSC و ادوات سیار را بر عهده می‌گیرد. SMS از طریق یک مسیر سیگنال مجزا ارسال می‌شود و قابلیت انتقال همزمان با صوت، داده و دورنگار را دارد. در مقایسه با برخی سرویس‌های انتقال پیامهای متنی موجود نظیر فراخوانی الفماری[۴۱]، این سرویس چنان طراحی شده که ضمانتی برای دریافت پیامهای متنی در مقصد را نیز فراهم آورد. بدین ترتیب که فرستنده پیام کوتاه پس از ارسال، پیامی مبتنی بر ارسال موفقیت آمیز پیام کوتاه از شبکه دریافت می‌دارد و پیام کوتاه ذخیره شده در SMSC تا زمان انقضای مدت اعتبار آن و تا زمانی که مشترک هدف در دسترس نباشد باقی می‌ماند و به محض در دسترس قرار گرفتن مشترک هدف، پیام کوتاه ذخیره شده برای وی ارسال خواهد شد. یکی دیگر از ویژگیهای SMS ارسال به صورت پاکتی و کم بودن پهنای باند انتقال آن می‌باشد. سرویس پیام کوتاه، امکان تبادل پیامهای کوتاه ۱۴۰ بایتی (حداکثر ۱۶۰ کاراکتری) را ممکن می‌سازد. کاربردهای اولیه SMS متمرکز بر ارسال الفماری با قابلیت ارسال دو طرفه پیامهای همه منظوره و سرویس‌های اطلاع رسانی بودند. با رشد تکنولوژی و توسعه شبکه‌ها، سرویس‌های جدیدی مشتمل بر پست الکترونیکی، اضافه نمودن فاکس، بانکداری و سرویس‌های اطلاعاتی نظیر ارائه آمار بورس نیز اضافه شدند. SMS یک تکنولوژی مفید برای ارسال اطلاعات به تعداد زیادی گیرنده و با هزینه‌ای قابل قبول می‌باشد. با این وجود SMS به اندازه‌ای امن نیست که به عنوان حاملی برای تراکنش‌های مالی مورد استفاده قرار گیرد. در کل مشکلات امنیتی سرویس پیام کوتاه را می‌توان به دو دسته تقسیم نمود:

الف) مشکلات امنیتی که SMS به عنوان یک روش انتقال داده, از شبکه سیار مورد استفاده به ارث می‌برد.

ب) تعدادی آسیب‌پذیری اضافه که معمولا ارتباطی به شبکه سیار مورد استفاده ندارد.

---

[39] Store-and-forward
[40] Short Message Service Center
[41] Alphanumeric paging

در خصوص دسته اول از مشکلات امنیتی، در واقع کلیه مشکلات امنیتی GSM -که در بخش ۳ به آنها اشاره شد- به تمام سرویس‌ها و مسیرهای انتقال داده GSM و از جمله SMS قابل اعمال می‌باشند، چرا که حملات ذکر شده کلیه داده‌ها و اطلاعات سیگنالینگ مبادله شده را هدف قرار می‌دهند. همانگونه که اشاره شد، سرویس پیام کوتاه خاص GSM نبوده و توسط بسیاری از سیستمهای سیار ارائه می‌شود. با این وجود، به دلیل گستردگی استفاده از GSM، در این مقاله تمرکز ما بر روی GSM بوده است. سرویس پیام کوتاه در GSM، برای حفاظت از پیامها از مکانیزم رمزنگاری GSM در واسط رادیویی (یعنی همان الگوریتم A5) استفاده می‌کند و در سایر قسمتهای شبکه، پیامها به صورت آشکار و رمز نشده مبادله یا نگهداری می‌شوند. همچنین مکانیزمی برای بررسی تمامیت داده در سرویس پیام کوتاه پیش بینی نشده است. در صورت انجام حمله مرد میانی و استفاده از ایستگاه فرستنده-گیرنده قلابی، حمله کننده قادر به ایجاد، تغییر یا حذف پیامهای کوتاه ارسالی و یا دریافتی خواهد بود. همچنین در صورت کپی سیم کارت (یا اطلاع از دو عدد IMSI و Ki مشترک مربوطه)، حمله‌کننده قادر به دریافت SMSهایی که برای مشترک هدف ارسال شده است، خواهد بود. او همچنین می‌تواند با استفاده از حساب کاربری مشترک هدف قرار گرفته، SMSهایی را به نام مشترک هدف ارسال و خسارتهایی را وارد نماید. به عنوان مثال، چنانچه یک سیستم بانکداری سیار به صورت ساده لوحانه‌ای قابلیت واریز و یا جابه‌جایی موجودی حساب را با ارسال SMS برای مشتریان خود فراهم نموده باشد، حمله‌کننده با استفاده از حملات ذکر شده خواهد توانست دستوراتی مبنی بر برداشت و یا انتقال وجه از حساب مشترک هدف قرار گرفته شده صادر نماید.

همانگونه که ذکر شد، سرویس پیام کوتاه تعدادی آسیب‌پذیری اضافه نیز دارد که یکی از آنها مربوط به خاصیت ذخیره و ارسال است. در واقع پیامهای کوتاه در SMSC به صورت آشکار و رمز نشده ذخیره می‌شوند. ذخیره پیامها در SMSC می‌تواند مشکلاتی نظیر امکان مشاهده یا تغییر پیامها توسط حمله‌کننده را ایجاد نماید. مشکل دیگر مربوط به SMSهای جعلی[۴۲] است که می‌توانند از طریق اینترنت هدایت شوند. هنگامی‌که یک کاربر در حال فراگردی[۴۳] است، محتویات SMS از شبکه‌های مختلف و حتی گاهی اینترنت عبور می‌کنند که این امر می‌تواند آن را در معرض آسیب‌پذیری‌ها و حملات مختلف قرار دهد. مشکل دیگر مربوط به ذخیره پیامهای کوتاه ارسالی و دریافتی قبلی، به صورت آشکار و حفاظت نشده بر روی وسیله سیار است که با دسترسی فیزیکی غیر مجاز به گوشی و یا سرقت و مفقود شدن آن، چنین اطلاعاتی در معرض آسیب خواهند بود.

[42] Fake SMS
[43] Roaming

برای استفاده از SMS به عنوان یک حامل امن، لازم است سرویس‌های امنیتی موردنیاز در کاربرد موردنظر را به کمک مکانیزمهای امنیتی در آن ایجاد نماییم. محرمانگی، تمامیت، احراز اصالت و انکارناپذیری از مهمترین سرویس‌های امنیتی هستند که در بسیاری از کاربردهای امن می‌بایست مورد توجه قرار گیرند. اما این ملزومات، توسط سیستم پیام رسانی فعلی SMS تامین نمی‌شوند. لذا چنین کاربردهایی می‌توانند امنیت مورد نیاز خود را به صورت انتها به انتها و یا به عبارتی، از طریق تامین امنیت در لایه کاربرد شبکه برقرار نمایند که در آن، احتیاج به تغییر در زیرساخت شبکه نمی‌باشد. امنیت انتها به انتها در سیستمهای سیار عموما با استفاده از یک یا چند مورد از موارد زیر فراهم می‌شود [۲ و ۹]:

۱) قابلیت پردازشی ME با استفاده از زبانهای برنامه‌نویسی: با افزایش روز افزون توان پردازشی گوشی‌های موبایل، یکی از بهترین گزینه‌ها است. گوشی‌های موبایل همانند کامپیوترهای شخصی دارای زبانهای برنامه‌نویسی متعدد و مخصوص به خود هستند و با استفاده از این زبانها، می‌توان به صورت نرم‌افزاری از قدرت پردازشی گوشی استفاده نمود. امروزه در شرایطی که از این روش حتی می‌توان برای رمزنگاری انتها به انتهای صدا (البته بر روی کانال داده GSM) نیز استفاده نمود، استفاده از آن در برقراری امنیت انتها به انتها در سرویس پیام کوتاه -که به دلیل محدودیت حجم داده، توان پردازشی کمتری نیز احتیاج دارد- به مراتب ساده‌تر است. بسته به سیستم عامل گوشی، می‌توان از یکی از زبانهای برنامه‌نویسی استفاده نمود. البته زبانهایی مانند جاوا نیز وجود دارند که به سیستم عامل گوشی بستگی ندارند و نرم افزار تهیه شده در این حالت، بر روی طیف وسیعی از گوشی‌ها قابل اجرا خواهد بود. J2ME[۴۴] نسخه ویژه‌ای از جاوا است که برای ادوات با محدودیت منابع نظیر گوشی‌های موبایل و PDA[۴۵]ها طراحی شده است. J2ME قابلیت دسترسی به ویژگی‌های توسعه یافته سیم کارت را با استفاده از بسته SATSA[۴۶] و قابلیت ارسال و دریافت SMS را با استفاده از WMA[۴۷] فراهم می‌آورد. البته J2ME در برگیرنده توابع رمزنگاری نمی‌باشد و لازم است یا راسا نسبت به نوشتن کدهای لازم برای توابع رمزنگاری اقدام نمود و یا از APIهای بهینه‌ای که توسط برخی گروه‌ها نظیر Bouncy Castle تهیه شده، استفاده نمود.

۲) قابلیت پردازشی سیم کارت با استفاده از SAT[۴۸]: SAT یا STK[۴۹]، امروزه به عنوان ابزاری مورد استفاده قرار می‌گیرد که یک منو کنترل شده توسط اپراتور را برای سرویس‌های صوتی و SMS فراهم می‌آورد. این

[44] Java 2 Mobile Edition
[45] Personal Digital Assistant
[46] Security and Trust Service API
[47] Wireless Messaging API
[48] SIM Application Toolkit

قابلیت به اپراتورها اجازه می‌دهد که کاربردهای ویژه‌ای را برای SIM مشترکین تعریف نمایند. SAT، SIM را قادر می‌سازد تا به عملکردهای MS نظیر کنترل صفحه نمایش، اخذ اطلاعات از صفحه کلید، ارسال پیامهای کوتاه و سایر عملکردهای موردنیاز -که برای انجام یک خدمت با ارزش افزوده مورد نیاز است- دسترسی داشته باشد. STK درست مانند SMS استاندارد جا افتاده‌ای است که از سال ۱۹۹۵ وارد بازار شده و هم اینک در تمام استانداردهای مهم مخابرات سیار وارد شده است. در استاندارد SAT [۱۰]، سرویس‌های امنیتی از قبیل احراز اصالت، تمامیت و محرمانگی پیام مدنظر قرار گرفته است. همچنین برخی مکانیزمها جهت اثبات دریافت بسته ارسالی و جلوگیری از حمله تکرار نیز در نظر گرفته شده است. جهت رمزنگاری پیام نیز استفاده از الگوریتمهای DES در مود CBC و ECB، 3-DES در مود CBC و همچنین سایر الگوریتمهای رمز بلوکی مناسب، با اطلاع و توافق طرفین پیش‌بینی شده است. اطلاعات امنیتی مورد استفاده در SAT می‌بایست مستقل از اطلاعات امنیتی و کلیدهای رمز موجود در GSM باشند. STK توسط تمام گوشی‌های فاز +۲ موجود در بازار پشتیبانی می‌شود. با این وجود، قابلیت STK در همه سیم کارتها (به خصوص سیم کارتهای قدیمی) تعریف نشده است. نکته دیگری که باید به آن توجه داشت محدودیت توان پردازشی سیم کارت در مقایسه با گوشی است که البته با توجه به محدودیت حجم داده در پیامک، این تفاوت ممکن است در عمل چندان ملموس نباشد.

۳) قابلیت پردازشی یک کارت هوشمند دیگر نظیر جاواکارت[۵۰]: این راهکار به گوشی‌های گران قیمت‌تر دو تراشه‌ای احتیاج دارد و گوشی‌های معمولی امکان استفاده از این قابلیت را ندارند.

۴) قابلیت پردازشی یک پردازنده رمزنگاری که در داخل ME جاسازی شده است [۱۱]: انجام این کار می‌بایست به هنگام ساخت گوشی توسط سازنده صورت پذیرد و کاربر امکان دستکاری در سخت‌افزار را ندارد. همچنین گوشی تهیه شده ممکن است مشمول محدودیتهای صادراتی به برخی کشورها شود.

۵) قابلیت پردازشی یک کامپیوتر شخصی قابل حمل که به ME متصل شده است: برای آن دسته از مکانیزمهای امنیتی مفید است که احتیاج به حافظه و توان محاسباتی بالایی دارند (مثلا رمزنگاری انتها به انتهای صدا بر روی کانال صوتی GSM [۱۲]).

[49] SIM ToolKit
[50] JavaCard

با توجه به موارد ذکر شده و بسته به کاربرد مورد نظر، می‌توان از هریک از این روشها بهره جست ولی باید توجه داشت که راهکار اول و دوم عمومیت بیشتری داشته و ممکن است برای بسیاری از کاربردهای معمول، مناسب‌تر باشند.

٦- نتیجه

در این مقاله، امنیت GSM و همچنین سرویس پیام کوتاه به اختصار مورد بررسی قرار گرفت. GSM به عنوان پرکاربرترین سیستم تلفن همراه در دنیا، با مشکلات امنیتی متعددی مواجه است. با وجود آنکه تلاش شده که در نسلهای بالاتر تلفن همراه این مشکلات برطرف شوند، هنوز تعداد زیادی اپراتور وجود دارند که از سیستمهای قدیمی استفاده می‌نمایند. برخی از مشکلات امنیتی موجود در GSM می‌توانند برای عموم مردم ایجاد مشکل نمایند، در حالی که برخی دیگر صرفا افراد خاص را هدف قرار خواهند داد. سرویس پیام کوتاه نیز به عنوان یکی از پرکاربردترین مسیرهای انتقال داده در GSM و بسیاری دیگر از سیستمهای سیار، مشکلات امنیتی خاص خود را دارد که بخشی از آنها را از سیستم سیار مورد استفاده به ارث برده و برخی دیگر مربوط به آسیب‌پذیری‌هایی است که مستقل از شبکه سیار مورد استفاده می‌باشد. با این وجود می‌توان به کمک راهکارهایی، امنیت GSM و همچنین سرویس پیام کوتاه را بهبود بخشید که یکی از بهترین و کم هزینه‌ترین آنها، برقراری امنیت به صورت انتها به انتها است.

۷- منابع

[1] GSM World News – Statistics: http://www.gsmworld.com/news/statistics/pdf/gsma_stats_q4_07.pdf. Access date: July 20, 2008.
[2] M. Toorani, and A.A. Beheshti Shirazi, “Solutions to the GSM Security Weaknesses,” Proceedings of the 1st IEEE Workshop on Wireless and Mobile Security (WMS'08), pp.576-581, Cardiff, UK, Sept. 2008.
[3] W. Stallings, “Network Security Essentials: Applications and Standards,” Prentice Hall, 2000.
[4] P. Chandra, “Bulletproof Wireless Security: GSM, UMTS, 802.11 and Ad hoc Security,” Elsevier, 2005.
[5] S.M. Siddique, and M. Amir, “GSM Security Issues and Challenges,” Proceedings of the Seventh IEEE International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD'06), pp.413-418, June 2006.
[6] E. Barkan, E. Biham, and N. Keller, “Instant Ciphertext-Only Cryptanalysis of GSM Encrypted Communication,” pp.600-616, CRYPTO 2003.

[7] A. Biryukov, A. Shamir, and D. Wagner, “Real Time Cryptanalysis of A5/1 on a PC,” pp.1-18, FSE 2000.
[8] http://www.alarm.de.
[9] M. Toorani, and A.A. Beheshti Shirazi, “SSMS - A Secure SMS Messaging Protocol for the M-payment Systems,” Proceedings of the 13th IEEE Symposium on Computers and Communications (ISCC'08), pp.700-705, Morocco, July 2008.
[10] European Telecommunications Standards Institute, “Digital cellular Telecommunications system (Phase 2+), Security mechanisms for the SIM Application Toolkit,” GSM 02.48 version 6.0.0 Release 97, April 1998.
[11] A.B. Rekha, B. Umadevi, Y. Solanke, and S.R. Kolli, “End-to-End Security for GSM Users,” IEEE International Conference on Personal Wireless Communications, pp.434-437, Jan. 2005.
[12] N.N. Katugampala, K.T. Al-Naimi, S. Villette, and A.M. Kondoz, “Real-time End-to-end Secure Voice Communications Over GSM Voice Channel,” 13th European Signal Processing Conference (EUSIPCO'05), Turkey, Sept. 2005.