فصلنامه‌ی علمی و پژوهشی شریف
تابستان ۱۳۸۶، شماره‌ی سی و هشتم، ص. ۳۱-۴۱

معماری امنیتی سیستم تلفن همراه نسل دوم (GSM) و آسیب‌پذیری‌های آن

محسن بهداری (کارشناس ارشد)
دانشکده‌ی مهندسی برق، دانشگاه صنعتی شریف
محمود سلماسی‌زاده (استادیار)
جواد مهاجری (مربی)
پژوهشکده‌ی الکترونیک، دانشگاه صنعتی شریف

«باگذشت ۲۵ سال از عمر ارتباطات سیار، تعداد کاربران تلفن همراه از تعداد کل کاربران تلفن ثابت (با عمر بیش از ۱۲۰ سال) پیشی گرفته است.» این جمله به‌تنهایی می‌تواند نشانگر رشد سریع ارتباطات سیار در سال‌های اخیر باشد که حجم قابل توجهی از صنعت مخابرات را به خود اختصاص داده است.

در ایران نیز برای گسترش ارتباط سیار سرمایه‌گذاری بسیار سنگینی به‌عمل آمده و مشترکین نیز برای استفاده از این سرویس‌ها هزینه‌ی قابل توجهی می‌پردازند. نکته‌ی مهم این که علیرغم این سرمایه‌گذاری سنگین و استفاده‌ی گسترده، سیستم GSM [۱] قابل تغییر یا بهبود نیست و به شکل یک مجموعه هر آنچه هست خریداری، نصب و استفاده می‌شود.

این رشد و فراگیری روزافزون از یک سو، و وجود چالش‌ها و مشکلات امنیتی نظیر جعل سیم‌کارت، برقراری مکالمه‌ی رایگان و شنود مکالمات مشترکین از سوی دیگر، ضرورت توجه بیشتر به امنیت مخابرات سیار را آشکار می‌کند. با مطرح‌شدن روش‌های جدید تحلیل پروتکل‌ها و الگوریتم‌ها، به‌تدریج نقاط ضعف امنیتی شبکه‌ی تلفن همراه آشکار، و حملات مؤثری به اهداف امنیتی شبکه‌ی تلفن همراه (نظیر محرمانگی، اصالت و جامعیت داده) وارد شد.

در این نوشتار معماری امنیتی نسل دوم سیستم تلفن همراه به شکل کاملاً جامع استخراج، و نقاط ضعف امنیتی و آسیب‌های احتمالی ناشی از آنها برای کاهش میزان آسیب‌پذیری امنیتی سیستم تلفن همراه GSM به تفصیل بیان می‌شود.

مقدمه

اولین فاز شبکه جهانی تلفن همراه(GSM) کشور در مرداد ماهِ ۱۳۷۳ در شهر تهران، با استفاده از ۱۷۶ فرستنده و گیرنده در ۲۴ ایستگاه رادیویی و با ظرفیت ۹٫۲۰۰ شماره راه‌اندازی و مورد بهره‌برداری قرار گرفت. به دنبال استقبال غیر منتظره‌ی مشترکین از این پدیده، شرکت مخابرات ایران درصدد گسترش پوشش آن از تهران به کل کشور برآمد، به‌طوری که در سال ۱۳۷۴ تعداد تلفن‌های دایری به ۱۵٫۹۰۷ شماره افزایش یافت و علاوه بر تهران شهرهای مشهد، اهواز، تبریز، اصفهان و شیراز نیز تحت پوشش شبکه‌ی تلفن همراه قرار گرفت. با گسترش نیاز متقاضیان به استفاده از فناوری برتر و بهره‌مندی از امکانات این شبکه در سال ۱۳۷۹ علاوه بر افزایش تعداد تلفن‌های دایری به ۹۶۲٫۵۹۵ شماره، تعداد شهرهای تحت پوشش نیز به ۳۳۷ شهر افزایش یافت. در پایان سال ۱۳۸۲ شبکه‌ی تلفن همراه شرکت مخابرات ایران با ظرفیتی معادل ۳٫۶۴۰٫۵۸۷ مشترک در بیش از ۶۵۰ شهر گسترده شده و علاوه بر آن ۱۰٫۳۵۰ کیلومتر از جاده‌های کشور تحت پوشش شبکه تلفن همراه قرار گرفته است. لازم به ذکر است که در طول برنامه‌ی پنج‌ساله‌ی سوم توسعه و در پایان سال ۱۳۸۳، مطابق انتظار تعداد مشترکین تلفن همراه درکشور به ۴٫۵۰۹٫۵۲۲ رسید. همچنین در برنامه‌ی پنج‌ساله‌ی چهارم واگذاری ۵٫۶۰۰٫۰۰۰ شماره توسط شرکت مخابرات، ۵٫۰۰۰٫۰۰۰ شماره توسط اپراتور دوم، و ۲٫۰۰۰٫۰۰۰ مشترک اعتباری تلفن همراه برنامه‌ریزی شده است.[۱] آمارهای جهانی و منطقه‌یی تلفن همراه نیز به‌خوبی نشانگر اهمیت موضوع است؛ مثلاً تعداد مشترکین تلفن همراه پس از گذشت ۴ سال به مرز ۵۰ میلیون رسیده است در حالی‌که تلفن ثابت این مسیر را طی ۷۴ سال پیموده‌است، همچنین تعداد کاربران تلفن همراه در سال ۲۰۰۲ به بیش از یک میلیارد نفر رسیده که در این سال ضریب نفوذ جهانی تلفن همراه ۲۵ درصد بوده است. از سوی دیگر در سال ۲۰۰۰ در بیش از ۳۵ کشور جهان، تعداد کاربران تلفن همراه بیش از تلفن ثابت بوده است. به‌طور متوسط هر سال به میزان ۵۰ درصد به تعداد کاربران تلفن همراه در منطقه‌ی خاورمیانه افزوده می‌شود. این تعداد که در سال ۹۷ حدود ۳٫۲ میلیون نفر بوده، در سال ۲۰۰۴ به بیش از ۳۸ میلیون نفر رسیده است. ضریب نفوذ تلفن همراه در خاورمیانه ۱۰ درصد است که این رشد بیانگر نقش و اهمیت حضور تلفن همراه در ارتباطات است. در این نوشتار پیرامون کلیات شبکه‌ی تلفن همراه، اهداف امنیتی GSM و چگونگی دست‌یابی به

آنها، نقاط ضعف و حملات مطرح شده به GSM بحث شده و در انتها یک نتیجه‌گیری جامع از امنیت تلفن همراه نسل دوم (GSM) ارائه خواهد شد.

کلیات شبکه‌ی جهانی تلفن همراه (GSM)

در یک شبکه‌ی سلولی، هر سلول نمایانگر ناحیه‌یی است که در حوزه‌ی دسته‌یی از فرکانس‌های ارسالی از یک آنتن ایستگاه پایه‌ی رادیویی قرار دارد. GSM یک سیستم تمام اروپایی است و در بسیاری از کشورهای جهان به‌عنوان بهترین راه حل برای تلفن همراه برگزیده شده است. شبکه‌ی GSM متشکل است از سه بخش شامل: سیستم سوئیچینگ (SS)[۲]، سیستم ایستگاه پایه(BSS)[۳] و پایانه‌ی همراه (MS)[۴]. پایانه‌ی همراه (گوشی تلفن همراه با سیم کارت) دستگاهی است که مشترک در اختیار خود دارد. سیستم ایستگاه پایه، کارکردهای مرتبط با ارتباطات رادیویی را برقرار می‌سازد و از دو بخش ایستگاه فرستنده ـ گیرنده‌ی پایه (BTS)[۵] و کنترل‌کننده‌ی ایستگاه پایه(BSC) [۶] تشکیل شده است. ایستگاه فرستنده ـ گیرنده‌ی پایه دستگاهی است که برای برقراری مکالمات در سلول‌های مجاور خود به‌کار می‌رود. این دستگاه دارای یک سیستم آنتن هوایی، تقویت‌کننده‌های قدرت فرکانس رادیویی و دستگاه پردازشگر سیگنال دیجیتال است. کنترل‌کننده‌ی ایستگاه پایه دارای تمام تجهیزات واسط رادیویی و فرستنده‌ی مورد نیاز در سایت رادیویی است و ضمن عهده‌داری مدیریت منابع رادیویی یک یا چند BTS، بر BTSها و ارتباطات رادیویی آنها کنترل و نظارت می‌کند و نقش یک واسط اتصال میان پایانه‌ی همراه و سیستم سوئیچینگ را دارد. سیستم سوئیچینگ شامل مرکز سوئیچینگ خدمات سیار(MSC)[۷]، ثبت‌کننده‌ی مکان مراجعه‌کننده (VLR)[۸]، ثبت‌کننده‌ی مکان اصلی (HLR)[۹]، مرکز احراز اصالت (AUC)[۱۰] و ثبت‌کننده‌ی هویت دستگاه (EIR) [۱۱] است. ثبت‌کننده‌ی مکان اصلی، مخزن اطلاعاتی است که در آن اطلاعات مشترک تلفن همراه، از جمله اسم، نشانی و صورت حساب او ذخیره می‌شود. هر مشترک با شناسه‌ی بین‌المللی مشترک (IMSI) [۱۲] و شناسه ISDN مشترک سیار(MSISDN)[۱۳] شناسایی می‌شود. اطلاعات مربوط به دسته‌بندی مشترکین، خدمات تکمیلی و خدمات مخابراتی پایه در مکان اصلی (HLR) ذخیره می‌شود. علاوه بر این در HLR اطلاعات مربوط به محدودیت خدمات، مکالمات انتقال یافته به شماره‌ها و محدودیت‌های شماره‌گیری بین‌المللی قرار دارد. مرکز سوئیچینگ خدمات سیار (MSC) سوئیچی است که ترافیک سیار مبدأ و مقصد را به انجام می‌رساند. این مرکز عهده‌دار کارکردهای سوئیچینگ تلفنی سیستم GSM است. ثبت‌کننده مکان مراجعه کننده (VLR) نیز یک مخزن اطلاعاتی است و به‌مثابه یک HLR تقسیم شده برای یک ناحیه‌ی خاص است به‌طوری که اطلاعات مربوط به تمام مشترکینِ این ناحیه در آن گنجانده شده است. اطلاعات تمام مشترکین تلفن همراه، همیشه در یک VLR و یک HLR ذخیره می‌شوند. مرکز احراز اصالت (AUC) عهده‌دار تأمین شاخص‌های مورد نیاز تائید یا رد برای احراز اصالت و حفظ محرمانگی تمام مکالمات است. ثَبّات مشخصات دستگاه (EIR) یک مخزن اطلاعاتی در مورد مشخصات فیزیکی دستگاه سیار است.[۲و۳]

اهداف امنیتی GSM

اهداف امنیتی درنظر گرفته شده توسط طراحان برای GSM عبارتند از:

۱. احراز اصالت مشترکین به‌منظور عدم ارائه‌ی خدمات به مشترکین غیر مجاز (مانند جلوگیری از بهره‌برداری سیم‌کارت‌های جعلی از شبکه‌ی تلفن همراه).

۲. تأمین گمنامی مشترکین سرویس گیرنده با اختصاص شناسه‌ی موقت TMSI [۱۴].

۳. جلوگیری از شنود مکالمات مشترکین در مسیر رادیویی بین MS و BTS با تأمین محرمانگی مکالمات.

۴. ذخیره‌سازی و انتقال اطلاعات مهم با تأمین ویژگی‌های محرمانگی، جامعیت و احراز اصالت (بین فرستنده و گیرنده).

۵. ایجاد امنیت و مقابله با حملات مطرح علیه کانال‌های رادیویی.

اهداف امنیتی در GSM توسط الگوریتم‌ها و پروتکل‌های رمزنگاری متفاوت و با استفاده از کلیدهای مختلف تأمین می‌شوند. طراحی تجهیزات و سیستم‌های امنیتی GSM توسط کنسرسیوم GSM به‌طور محرمانه انجام شد و فقط اطلاعات کلی مربوط به تجهیزات سخت‌افزاری و نرم‌افزاری در اختیار اپراتورها قرار گرفت. در این میان الگوریتم‌های مربوط به رمزنگاری و احراز اصالت (در زمان طراحی و قبل از پیاده‌سازی شبکه) در اختیار عموم و مورد بررسی قرار نگرفت. در حقیقت کنسرسیوم GSM پایه‌های امنیتی خود را بر ابهام الگوریتم‌های طراحی شده در GSM بنا نهاد، با این فرض که اگر الگوریتم‌ها در دسترس عموم نباشد شکسته شدن آنها سخت‌تر خواهد بود. سرانجام با انتشار الگوریتم‌های رمزنگاری، متخصصین توانستند در تحلیل آنها شرکت کنند. البته قبل از انتشار این الگوریتم‌ها، الگوریتم رمزنگاری A۵ به‌کمک مهندسی معکوس کشف شده بود.[۲و۴] فهرست الگوریتم‌ها، کاربرد آنها و کلیدهای مرتبط با هر الگوریتم در جدول ۱ ارائه شده است. در این نوشتار AUC بیانگر مرکز احراز اصالت، SMC نماینده‌ی مرکز مدیریت امنیت، و PCS نماینده‌ی مرکز اختصاصی کننده‌اند که

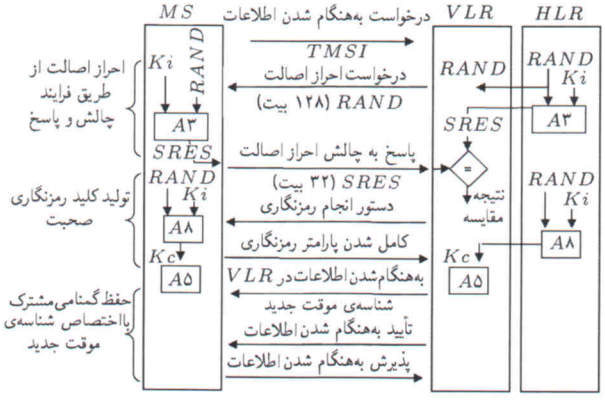
جدول ۱. فهرست الگوریتم‌ها، کاربرد آنها و کلیدهای متناظر.

نام الگوریتم	نوع الگوریتم	کاربرد الگوریتم	نام و طول کلید متناظر با الگوریتم
A۲	قطعه‌یی	این الگوریتم برای ذخیره‌سازی امنKi ها در حافظه‌ی مرکز احراز اصالت به‌کار می‌رود.	K۲، ۱۲۸(بیت)
A۳	قطعه‌یی	این الگوریتم برای احراز اصالت مشترکین توسط HLR به‌کار می‌رود و از عدد تصادفی RAND استفاده می‌کند. کلید Ki برای هر مشترک منحصر به‌فرد است و برای ایجاد تمایز بین مشترکین به‌کار می‌رود.	Ki، ۱۲۸ (بیت)
A۴	قطعه‌یی	این الگوریتم برای انتقال امن کلید Ki از مرکز اختصاصی‌کننده به مرکز احراز اصالت به‌کار می‌رود. به ازاء هر مرکز اختصاصی‌کننده می‌توان تا ۱۰ کلید K۴ مختلف داشت.	K۴، ۱۲۸ (بیت)
A۵	دنباله‌یی	الگوریتم تأمین محرمانگی مکالمات که در فاصله‌ی هوایی بین MS و BTSبه‌کار می‌رود.	Kc، ۶۴ (بیت)
A۷	کلید عمومی	این الگوریتم برای ایجاد محرمانگی و احراز اصالت بین مراکز اختصاصی‌کننده، مدیریت امنیت و احراز اصالت به‌کار می‌رود. زوج کلیدهای عمومی و خصوصی مراکز متفاوت‌اند. نمادهای Kp و Ks به‌ترتیب معرف کلیدهای عمومی و خصوصی به مرکز است.	Kp, smc/auc/pcs، ۱۲۸ (بیت) Ks, smc/auc/pcs، ۱۲۸ (بیت)
A۸	قطعه‌یی	این الگوریتم برای تولید Kc به‌کار می‌رود و از عدد تصادفی ۱۲۸ بیتی RAND استفاده می‌کند.	Ki، ۱۲۸ (بیت)
A۹	درهم‌ساز	این الگوریتم برای ایجاد چکیده پیام بین مراکز مدیریت امنیت و احراز اصالت به‌کار می‌رود و تمامیت فایل حاوی Kiهای رمزنگاری شده را تأمین می‌کند.	——

به‌ترتیب عهده‌دار وظایف احراز اصالت، مدیریت امنیت و تخصیص کلید Ki به سیم‌کارت‌ها هستند.

فرایند احراز اصالت و حفظ گمنامی مشترک توسط شبکه‌ی GSM و تولید کلید رمزنگاری صحبت

پروتکل وارد شدن مشترک تلفن همراه به شبکه و سرویس گرفتن از آن در شکل ۱ نشان داده شده است. در این شکل ابتدا پروتکل احراز اصالت و پس از آن پروتکل تولید Kc اجرا می‌شود، به این ترتیب که تلفن همراه (MS) همزمان با روشن شدن، درخواست به هنگام شدن اطلاعات مربوط به موقعیتش را همراه با شناسه‌ی موقت مشترک (TMSI) به VLR ارسال می‌کند، سپس پروتکل احراز اصالت که یک پروتکل چالش و پاسخ است از طریق VLR بین MS و HLR اجرا



شکل ۱. فرایند ورود مشترک به شبکه‌ی GSM با اجرای پروتکل احراز اصالت و تولید کلید رمزنگاری صحبت.

می‌شود؛ به این صورت که HLR چالشی را با ارسال یک عدد تصادفی ۱۲۸ بیتی بنام RAND برای مشترک ایجاد می‌کند. سپس مشترک (MS) الگوریتم A۳ را با استفاده از عدد تصادفی دریافتی و کلید اختصاصی خود (Ki) اجرا می‌کند. الگوریتم A۳ از نوع الگوریتم‌های رمزنگاری متقارن قطعه‌یی، و خروجی آن ۳۲ بیتی SRES[۱۵] است که به‌عنوان پاسخ به VLR باز می‌گردد. از سوی دیگر HLR نیز مستقیماً با استفاده از کلید اختصاصی مشترک، Ki و RAND، و الگوریتم A۳ به محاسبه‌ی SRES می‌پردازد و نتیجه را برای VLR می‌فرستد. VLR مقدار دریافتی از HLR و مقدار دریافتی از مشترک را مقایسه می‌کند؛ در صورتی که هر دو مقدار یکسان باشند، مشترک به چالش پاسخ صحیح داده و به‌عنوان یک مشترک مجاز در HLR و VLR ثبت می‌شود و در غیر این‌صورت شبکه از ارائه‌ی سرویس به مشترک غیرمجاز خودداری می‌کند. پروتکل تولید Kc کاملاً شبیه پروتکل احراز اصالت است، با این تفاوت که در اینجا الگوریتم A۸ با استفاده از عدد تصادفی RAND و کلید Ki اجرا می‌شود. خروجی الگوریتم A۸ کلید ۶۴ بیتی Kc است. پروتکل رمزنگاری مکالمات در GSM به این نحو است که مشترک پس از تولید Kc، پیام کامل شدن پارامترهای رمزنگاری را به VLR اعلام می‌دارد و با تزریق کلید Kc به الگوریتم A۵، دنباله‌ی شبه تصادفی مورد نیاز برای رمزنگاری مکالمه تولید می‌شود. سپس برای گمنام ماندن مشترکین، VLR یک شناسه‌ی موقت جدید به‌صورت تصادفی انتخاب و به مشترک اختصاص می‌دهد. بدین‌ترتیب در فاصله‌ی هوایی از مبادله‌ی شناسه بین‌الملل مشترک (IMSI) جلوگیری شده و امکان شناسایی مشترکین توسط حمله‌کنندگان از بین می‌رود.

جلوگیری از شنود مکالمات مشترکین در مسیر رادیویی بین MS وBTS با تأمین محرمانگی مکالمات

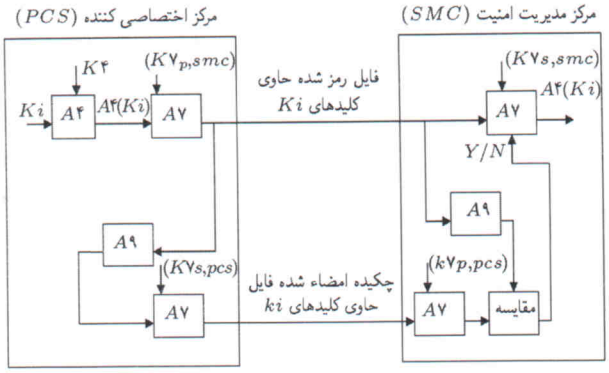
الگوریتم مورد استفاده برای رمزنگاری مکالمات در فاصله‌ی هوایی بین MS و BTS، الگوریتم A۵ است. کلید این الگوریتم Kc و ۶۴ بیت است. این الگوریتم از خانواده‌ی الگوریتم‌های رمز دنباله‌یی و شامل دونسخه‌ی A۵/۱ و A۵/۲ است که الگوریتم A۵/۱ نسبتاً از A۵/۲ قوی‌تر است. الگوریتم A۵/۱ برای کاربری در کشورهای اتحادیه‌ی اروپا و A۵/۲ برای سایر کشورها، از جمله ایران، تخصیص یافته است. هر دو الگوریتم با دریافت Kc و شماره فریم اطلاعات، یک دنباله‌ی شبه‌تصادفی که دوره‌ی تناوب بزرگی دارد، تولید می‌کنند. این دنباله‌ی شبه تصادفی تحت عنوان دنباله‌ی کلید، با دنباله‌ی دیجیتال اطلاعات صحبت ترکیب شده و یک متن رمزنگاری شده را تولید می‌کند، چنان‌که محتویات متن اصلی را از دید حمله‌کنندگان مخفی می‌سازد. ساختار الگوریتم A۵ بسیار ساده است و دارای سه تَبّات به طول‌های ۱۹، ۲۲ و ۲۳ بیت و یک واحد کنترل انتقال است که عهده‌دار انتقال نامنظم[۱۶] تَبّات‌ها است.[۵و۶]

ذخیره‌سازی و انتقال اطلاعات مهم با تأمین ویژگی‌های محرمانگی، جامعیت و احراز اصالت (بین فرستنده و گیرنده)

کلید Ki ایفاگر نقش اصلی در امنیت شبکه‌ی تلفن همراه است. همان‌طور که در پروتکل احراز اصالت مشترکین و تولید کلید رمزنگاری اشاره شد، تنها پارامتر پنهان از دید افراد غیرمجاز کلید Ki بوده و در صورت آشکار شدن آن، اساس امنیت شبکه‌ی تلفن همراه دچار خطر شده و از این طریق جعل سیم‌کارت و شنود مکالمات امکان‌پذیر می‌شود. لذا ذخیره‌سازی و انتقال آن با تأمین ویژگی‌های محرمانگی، جامعیت و احراز اصالت بین فرستنده و گیرنده از اهمیت خاصی برخوردار است.

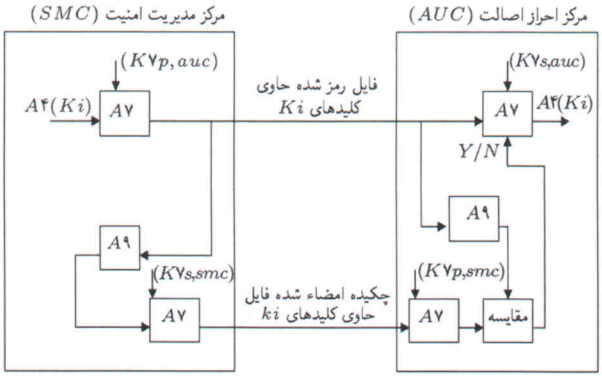
مرکز اختصاصی‌کننده (PCS)[۱۷] مسئول تولید و گنجاندن کلید Ki در تراشه‌ی سیم‌کارت است، و به هر سیم‌کارت Ki مربوط به خودش را تخصیص می‌دهد. فایل حاوی کلیدهای Ki، با استفاده از پروتکل‌هایی که متعاقباً تشریح می‌شود، از مرکز اختصاصی‌کننده به شکل محرمانه به مرکز مدیریت امنیت[۱۸] و از این مرکز به مرکز احراز اصالت منتقل می‌شود. بدین ترتیب فایل حاوی کلیدهای Ki به شکل محرمانه و با احراز اصالت فرستنده و جامعیت فایل برای مراکز احراز اصالت ارسال می‌شود.

برای این منظور مطابق شکل ۲ مرکز اختصاصی‌کننده، Kiها را توسط الگوریتم A ۴ رمز می‌کند و توسط الگوریتم رمزنگاری نامتقارن

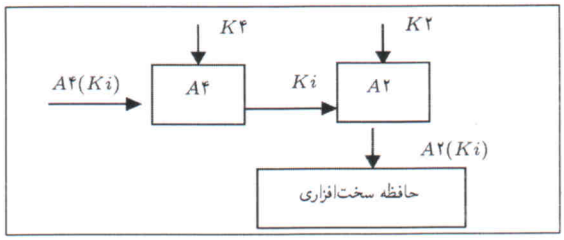


شکل ۲. انتقال فایل رمزشده‌ی Ki با ویژگی‌های محرمانگی، جامعیت و احراز اصالت بین مراکز اختصاصی‌کننده و مدیریت امنیت.

A۷ وکلید عمومی ۱۲۸ بیتی مرکز مدیریت امنیت (K۷p, smc) رمز می‌نماید و به‌صورت فایل حاوی Kiهاکه از تعداد مورد نیاز Ki رمز شده به فرمت A۷(A۴(Ki۱)+A۴(Ki۲)+...+A۴(Kin)) تشکیل شده است به مرکز مدیریت امنیت ارسال می‌کند. در این حالت فایل حاوی Kiها به‌صورت محرمانه به مرکز مدیریت امنیت ارسال می‌شود. از سوی دیگر توسط الگوریتم در هم‌ساز A۹ چکیده‌ی فایل حاوی اطلاعات رمز شده Kiها توسط A۴ تولید و توسط الگوریتم A۷ و کلید خصوصی مرکز اختصاصی‌کننده (K۷s, pcs) امضای دیجیتال می‌شود. در مرکز مدیریت امنیت بار دیگر چکیده‌ی فایل حاوی مقادیر رمز شده Kiها تولید و با چکیده رمزگشایی شده توسط الگوریتم A۷ و کلید عمومی مرکز اختصاصی کننده مقایسه می‌شود. در صورتی‌که دو مقدار یکسان باشند، هویت فرستنده‌ی Kiها (مرکز اختصاصی‌کننده) و جامعیت فایل حاوی Kiها به اثبات رسیده است؛ لذا با استفاده از الگوریتم A۷ و کلید خصوصی مرکز مدیریت امنیت فایل حاوی Kiها رمزگشایی می‌شود. برای ارسال فایل حاوی Kiها به مرکز احراز اصالت مطابق شکل ۳ روال فوق مجدداً تکرار می‌شود با این تفاوت که



شکل ۳. انتقال فایل رمز شده‌ی Ki با ویژگی‌های محرمانگی، جامعیت و احراز اصالت بین مراکز مدیریت امنیت و احراز اصالت.



شکل ۴. روند ذخیره‌سازی Kiها در حافظه‌ی مراکز احراز اصالت با تأمین ویژگی‌های محرمانگی.

اینجا برای امضای فایل حاوی Kiها از کلید خصوصی مرکز مدیریت امنیت (K۷s,smc) و برای رمزکردن آن از کلید عمومی مرکز احراز اصالت (K۷p,auc) استفاده می‌شود. درنتیجه در مرکز احراز اصالت می‌توان با اطمینان از هویت فرستنده و جامعیت فایل Kiها این فایل‌ها را رمزگشایی کرد. از طرفی کلید رمزنگاری K۴ تحت تدابیر امنیتی به مرکز احراز اصالت تحویل می‌شود و عملاً رمزگشایی کلید Ki در آنجا انجام می‌شود. برای ذخیره‌سازی محرمانه‌ی کلید Ki در حافظه‌ی سخت‌افزاری مرکز احراز اصالت، از الگوریتم A۲ با کلید ۱۲۸ بیتی K۲ استفاده می‌شود. البته کلید K۲ در زمان راه‌اندازی مرکز در برد سخت‌افزاری مربوطه تحت تدابیر امنیتی لازم گنجانده شده و راهبرها فقط با اعمال دستورات مربوطه به سیستم، امکان استخراج کلید Ki را دارند. در مرکز احراز اصالت و به‌واسطه‌ی سطوح امنیتی که توسط نام و کلمه‌ی عبور هر راهبر در سیستم به‌وجود می‌آید، راهبرها قادر به در اختیار داشتن قابلیت اجرای دستورات مربوط به استخراج کلید Ki خواهند بود.[۳] شکل ۴ روند رمزگشایی و ذخیره‌سازی کلیدهای Ki در مرکز احراز اصالت را نشان می‌دهد. در یک مقیاس کوچک از شبکه‌ی تلفن همراه می‌توان مرکز مدیریت امنیت را حذف کرد و مرکز اختصاصی‌کننده را مستقیماً عهده‌دار ارسال فایل حاوی Kiها به مرکز احراز اصالت کرد، ولی به‌علت زیاد بودن تعداد مراکز اختصاصی‌کننده و مراکز احراز اصالت در شبکه‌های مختلف حضور مرکز مدیریت امنیت برای انجام عملیات مدیریت کلیدهای عمومی و خصوصی ضروری است تا از این طریق هر مرکز با دانستن کلید عمومی مرکز مدیریت امنیت قادر به بررسی امضای دیجیتال باشد و در نتیجه از به‌کارگیری تعداد زیادی کلید عمومی و خصوصی در شبکه اجتناب شود.[۳]

ایجاد امنیت در کانال‌های رادیویی

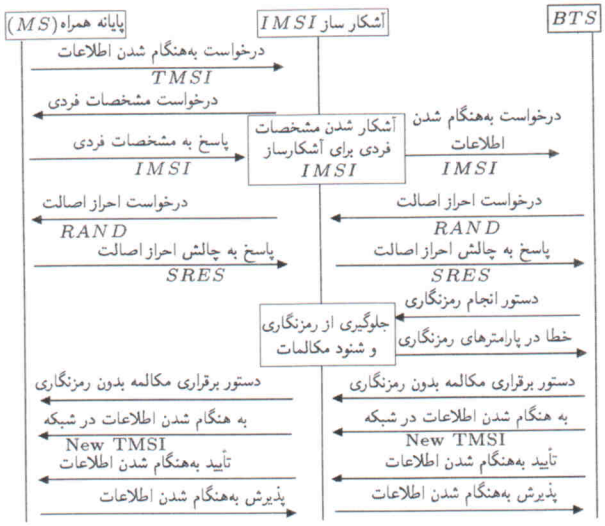
در ارتباطات رادیویی شبکه‌ی تلفن همراه نسل دوم (GSM) از دو روش «مالتی پلکس فرکانس» (FDMA) و «مالتی پلکس زمان» (TDMA) استفاده می‌شود. کلّ طیف فرکانسی به قطعاتی به پهنای ۲۰۰khz (FDMA)، و هر قطعه به هشت فاصله‌ی زمانی ۴٫۶ms (TDMA) تقسیم می‌شود. هر یک از این قطعات را یک کانال رادیویی می‌نامند.[۳] در شبکه‌ی GSM برای انجام سیگنال‌سازی‌های مختلف از کانال‌های متفاوت با موقعیت معین استفاده می‌شود. به‌عبارت دیگر هر کانال سیگنال‌سازی در فرکانس و فاصله‌ی زمانی معینی واقع شده است، لذا همگان می‌توانند به این کانال‌ها دسترسی داشته باشند. از سوی دیگر، در صورتی که کانال برای انتقال صوت مشترک تلفن همراه معلوم باشد می‌توان مکالمه‌ی او را شنود کرد؛ لذا برای مقابله با شنود مکالمات در GSM از شیوه‌ی طیف‌گسترده استفاده شده است. یکی از روش‌های گسترش طیف، گسترش توسط پرش‌های فرکانسی[۱۹] (FH) موج مدوله کننده است که به مشترک اجازه می‌دهد در طول مکالمه از کانال‌های ترافیکی متعددی به‌جای یک کانال ترافیکی استفاده کند.[۳] از طرف دیگر چون محیط انتقال در شبکه‌ی GSM یک فاصله‌ی هوایی است و به‌علت وجود ساختمان‌ها، تونل‌ها، درختان و موانع مختلف این محیط انتقال در طیف توان خود از افت‌ها و تقویت‌های مختلفی برخوردار است، لذا روش گسترش فرکانسی به مشترکین تلفن همراه این امکان را می‌دهد تا از تمامی طیف فرکانسی محیط انتقال استفاده کنند و محیط انتقال برای همه‌ی آنها یکسان باشد.

نقاط ضعف امنیتی شبکه GSM

نقاط ضعف امنیتی شبکه‌ی GSM به سه دسته ضعف ناشی از پروتکل‌های شبکه GSM، ناشی از الگوریتم‌های رمزنگاری شبکه GSM، و ضعف‌های ناشی از ترکیب این دو حالت تقسیم می‌شوند. این نقاط ضعف آسیب‌های امنیتی مختلفی مانند جعل سیم کارت، برقراری مکالمه‌ی رایگان و شنود مکالمات را به شبکه وارد می‌کنند. در ادامه‌ی این بخش هر سه دسته ضعف‌های امنیتی به تفصیل مورد بررسی و تحلیل قرار می‌گیرند.

آشکارسازی IMSI وTMSI

عملکرد این حمله مبتنی است بر نقطه ضعفی که در پروتکل‌های شبکه‌ی GSM وجود دارد. این جمله ویژگی امنیتی راکه باعث گمنامی مشترکین تلفن همراه می‌شود از بین می‌برد و نقطه‌ی آغازین برای انجام حملات دیگر است. به‌عبارت دیگر، حمله کننده می‌تواند مشترک تلفن همراه مورد نظر خود را از میان تمام مشترکین دیگر تشخیص داده و حملاتی مثل شنود و نفی سرویس (DoS)[۲۰] را به مشترک تلفن همراه اعمال کند. در اینجا حمله از طریق یک عامل غیرمجاز بنام «آشکار ساز IMSI» صورت می‌گیرد. IMSI شماره‌یی منحصر به‌فرد برای هر مشترک است و شبکه فقط از آن طریق می‌تواند مشترکین درون شبکه را از یکدیگر تشخیص دهد. همان‌طورکه در شکل ۵ نشان داده شده، «آشکار ساز IMSI» می‌تواندIMSI تمام مشترکین را به‌صورت غیرمجاز آشکار



شکل ۵. «آشکارساز IMSI» به‌عنوان نمونه‌یی از نقاط ضعف پروتکلی GSM.

کند و بدین ترتیب محرمانه بودن نام مشترکین تلفن همراه را که از طریق TMSI حاصل شده بود، از بین ببرد. در این حالت با دانستن IMSI هر مشترک می‌توان با تمرکز یافتن بر آن حملاتی از قبیل حمله‌ی نفی سرویس از طریق عامل میانی[۲۱] و jamming را بر آن اعمال کرد. «آشکار ساز IMSI» حتی می‌تواند روند رمزنگاری در فاصله‌ی هوایی را تحت‌الشعاع قرار داده و از رمزنگاری مکالمات نیز جلوگیری کند. حمله‌ی «آشکارسازIMSI» بسیار ساده و از طریق عامل میانی صورت می‌گیرد. در واقع «آشکارساز IMSI» نقش یک BTS را برای MS و نقش یک MS را برای BTS بازی می‌کند، بدون اینکه BTS و MS واقعی از وجود «آشکارساز IMSI» مطلع شوند.

یادآور می‌شود که MS به هر BTS که دارای توان سیگنال بالاتری باشد پاسخ می‌دهد. این موضوع برای BTS هم صدق می‌کند، یعنی به هر MSیی که دارای توان سیگنال بالاتری باشد پاسخ می‌دهد؛ در نتیجه «آشکارساز IMSI» با افزایش توان خود می‌تواند نقش MS را برای BTS و نقش BTS را برای MS بازی کند. همان‌طور که در شکل ۵ نشان داده شده، زمانی که MSخواهان به هنگام کردن اطلاعات TMSI از BTS به‌عنوان عضو ابتدایی شبکه می‌شود، «آشکارساز IMSI» می‌تواند طبق پروتکل GSM، IMSI را از MS تقاضا کند، و در نتیجه MS، IMSI خود را به «آشکارساز IMSI» تحویل می‌دهد. حال «آشکارساز IMSI» با ارائه‌ی IMSI مشترک به شبکه (از طریق BTS)، پروتکل احراز اصالت را فعال می‌کند. در زمانی که شبکه می‌خواهد بر سر کلید Kc و روش رمزنگاری به توافق برسد، «آشکارساز IMSI» پیام خطا (عدم امکان رمزنگاری توسط MS) را به شبکه می‌دهد و در نتیجه شبکه به‌صورت از قبل تعریف شده، حالت بدون رمزنگاری را برای برقراری مکالمه در نظر می‌گیرد. در این حالت علاوه بر امکان آشکارسازی IMSI، امکان شنود مکالمه‌ی مشترکین نیز به‌وجود آمده است.

دلیل موفقیت این حمله پروتکل احراز اصالت یک‌سویه است؛ به‌عبارت دیگر تنها MS، اصالت خود را به شبکه اثبات می‌کند در صورتی‌که اگر شبکه نیز اصالت خود را به MS اثبات کند، حمله از طریق عامل میانی، «آشکارساز IMSI»، امکان‌پذیر نخواهد بود.

آشکارسازی Ki و تولید سیم‌کارت جعلی

این حمله مبتنی بر نقطه ضعف موجود در الگوریتم‌های رمزنگاری GSM است. الگوریتم‌های احراز اصالت و مولّد کلید Kc به‌ترتیب تحت عنوان A۳ و A۸ در داخل سیم‌کارت مشترکین پیاده‌سازی می‌شوند. ساختار هر دو الگوریتم یکسان و به‌نام COMP۱۲۸ معروف است. به‌علت گسترش سریع شبکه‌ها و اپراتورهای مختلف GSM، استفاده از الگوریتم COMP۱۲۸ به‌سرعت فراگیر شد بدون آنکه این الگوریتم به‌طور کامل مورد تجزیه و تحلیل امنیتی قرار گیرد. بعد از آشکار شدن نقاط ضعف COMP۱۲۸، بعضی از اپراتورها اقدام به جایگزینی نسخه‌های جدیدتر و مقاوم‌تر کردند ولی به‌علت پرهزینه‌بودن، فرایند جایگزینی به‌کندی صورت می‌گیرد. یکی از حملات مطرح شده به الگوریتم COMP۱۲۸ حمله‌ی چالش‌های انتخابی است. باید توجه داشت که به‌علت پروتکل احراز اصالت یک‌سویه، سیم‌کارت خود را ملزم به پاسخگویی به هر چالش می‌داند، لذا می‌توان سیم کارت را توسط کارت‌خوان به PC متصل، و از آن طریق چالش‌های مورد نظر را برای سیم‌کارت ایجاد، و سیم‌کارت مقادیر SRES و Kc معادل آنها را تولید کرد. با دانستن ۱۵۰٫۰۰۰ چالش و SRES و Kc متناظر با آن می‌توان Ki را محاسبه کرد، به‌صورتی که اگر کارت‌خوان و PC تعداد ۵٫۲۵ چالش در ثانیه برای سیم‌کارت ایجاد کنند، مدت زمان کل محاسبه‌ی Ki هشت ساعت می‌شود. بنابراین برای اعمال چنین حمله‌یی باید سیم‌کارت به‌مدت هشت ساعت در دسترس باشد. حمله از کانال‌های جانبی با استفاده از اطلاعات نشتی، نوع دیگری از حمله به الگوریتم COMP۱۲۸ است. حملات کانال جانبی، راه حل غیر مستقیمی را برای حمله به الگوریتم‌های رمزنگاری از طریق تعیین روابط بین ورودی وخروجی الگوریتم در حین اجرای الگوریتم (مثل رابطه‌ی زمان اجرای الگوریتم، توان مصرفی الگوریتم، تشعشع الکترومغناطیسی و غیره) به‌وجود می‌آورد. کاراترین روش در حملات جانبی، حمله‌ی تفکیکی[۲۲] است.[۷]

تنها الگوریتم‌هایی در مقابل حملات کانال‌های جانبی مقاوم‌اند که اطلاعات نشتی جانبی آنها مستقل از داده‌های ورودی یا خروجی، و یا کلیدی باشد. حمله‌ی تفکیکی زیرمجموعه‌یی از حملات کانال

جانبی است که توسط محققان IBM مطرح شده است.[۸] این حمله روشی است که می‌کوشد اطلاعات حساس را از طریق وابستگی‌های آماری اطلاعات نشتی جانبی استخراج کند و از قابلیت کاربرد مؤثر در پیاده‌سازی حملاتی که الگوریتم مورد حمله‌ی آنها از اصول مقابله با حملات کانال جانبی بی‌بهره است، برخوردار می‌باشد. الگوریتم COMP۱۲۸ در GSM دارای شرایط فوق‌الذکر است و برای اعمال موفقیت‌آمیز حملات تفکیکی بسیار مناسب و مستعد است به‌طوری که با اعمال کمتر از ۱۰۰۰ ورودی تصادفی یا ۲۵۵ ورودی منتخب، و یا فقط ۸ ورودی منتخب منطبق با شرایط خاص، می‌توان ضمن تحلیل الگوریتم COMP۱۲۸ کلید Ki را به‌دست آورد. بدین ترتیب طبق این روش زمان حمله به الگوریتم COMP۱۲۸ می‌تواند کمتر از یک دقیقه باشد.[۹] با آشکار شدن یک Ki معتبر می‌توان سیم‌کارت‌های جعلی منطبق با Ki آشکار شده را تولید و در شبکه‌ی تلفن همراه مورد بهره‌برداری قرار داد.

شنود مکالمات

این حمله ممکن است مبتنی بر نقاط ضعف موجود در الگوریتم‌های A۵/۲ و A۵/۱ مورد استفاده برای رمزنگاری اطلاعات صحبت و یا ترکیبی از نقاط ضعف الگوریتم و پروتکل‌های GSM باشد. اطلاعات تنها در فاصله‌ی هوایی بین MS و BTS رمزنگاری، و در شبکه‌ی سیمی، آشکارا مبادله می‌شوند، لذا در صورت دسترسی به شبکه‌ی سیمی GSM این موضوع می‌تواند باعث شنود مکالمات شود. حفظ محرمانگی مکالمات به‌خصوص در کاربردهای راهبردی (نظامی، تجاری، امنیتی و سیاسی) از اهمیت ویژه‌یی برخوردار است. شنود مکالمات توسط عامل غیرمجاز، اساساً می‌تواند به سه روش انجام گیرد: روش اوّل در بخش آشکارسازی IMSI و TMSI مورد بحث قرار گرفت؛ روش دوّم دست‌یابی به کلید Kc با استفاده از نقاط ضعف پروتکل‌های به‌کار رفته را شامل می‌شود؛ و در روش سوّم الگوریتم A۵/۱ و A۵/۲ تحلیل می‌شوند.

دستیابی به کلید Kc از طریق دسترسی به شبکه‌ی انتقال سیمی

حمله به الگوریتم A۵ امکان‌پذیر است ولی به‌علت پر هزینه بودن تاحدودی دشوار است. امواج ارسالی و دریافتی بین MS و BTS تنها راه برای شنود مکالمات و کسب اطلاعات لازم نیست. همان‌طور که قبلاً نیز اشاره شد، اطلاعات تنها در فاصله‌ی هوایی بین MS و BTS رمزنگاری می‌شوند و در شبکه‌ی سیمی، اطلاعات آشکارا مبادله می‌شوند. این خود می‌تواند رخنه‌یی جدید برای اعمال انواع گوناگونی از حملات باشد و حمله‌کننده قادر به‌کسب همه‌ی پارامترهای مورد نیاز برای شنود مثل SRES، RAND و Kc خواهد بود. اگر حمله‌کنندگان بتوانند مستقیماً به‌شبکه‌ی انتقال سیمی دسترسی داشته باشند شبکه‌ی تلفن همراه کاملاً ناامن خواهد بود.[۵و۱۰] دست‌یابی به شبکه‌ی انتقال سیمی چندان دشوار نیست؛ زیرا اگر چه BTSها از طریق کابل به BSC متصل می‌شوند، در بیشتر موارد این ارتباط از طریق مسیر ماکروویو یا مسیرهای ماهواره‌یی حاصل می‌شود که با استفاده از تجهیزات مناسب، دست‌یابی به اطلاعاتی که در این مسیرها مبادله می‌شوند دور از دسترس نیست. البته این امکان نیز وجود دارد که حمله‌کننده بتواند به کابل رابط BTSها و BSC نیز دسترسی داشته باشد، که در این حالت با به‌دست آوردن Kc برای یک مشترک تلفن همراه خاص، می‌تواند بلادرنگ مکالمه‌ی مشترک را در فاصله‌ی هوایی شنود کند.[۵]

دست‌یابی به کلید Kc از طریق آشکارسازی کلید Ki با دسترسی به سیم‌کارت

با توجه به نقاط ضعف بیان‌شده در قسمت جعل سیم‌کارت، حمله کننده با دسترسی به سیم‌کارت و اعمال چالش‌های انتخابی می‌تواند Ki را از آن استخراج کند و در هنگام برقراری مکالمه سیم‌کارت اصلی، به چالش شبکه پاسخ داده و Kc را محاسبه کند و به راحتی اطلاعات صحبت رمزشده در فاصله‌ی هوایی را رمزگشایی و شنود کند.

دست‌یابی به کلید Kc از طریق آشکارسازی کلید Ki بدون دسترسی به سیم‌کارت از طریق فاصله‌ی هوایی

این حمله از نقطه ضعف ترکیبیِ ناشی از پروتکل و الگوریتم شبکه GSM استفاده می‌کند. در GSM، همواره MS موظف به پاسخ به هر چالش شبکه است، در حقیقت پروتکل احراز اصالت یک‌سویه است و شبکه‌ی تولیدکننده‌ی چالش، توسط MS احراز اصالت نمی‌شود. به‌طورکلی یکی از نقطه ضعف‌های بزرگ GSM که منجر به رخنه‌های امنیتی فراوانی در آن شده است، عدم وجود فرایندی برای احراز اصالت شبکه به MS است. در اینجا یک BTS مجازی می‌تواند با افزایش توان خروجی خود، نقش یک BTS حقیقی را برای MS بازی کند و با بمب باران چالش‌ها برای یک MS خاص همان حمله‌ی چالش‌های انتخابی را به MS اعمال کند. باید توجه داشت که در این حالت، حمله کننده باید با احتیاط بیشتری به ایجاد چالش برای MS بپردازد تا حمله‌ی او به‌صورت غیرفعال باشد و کاربر پایانه همراه به‌دلیل تخلیه‌ی

سریع باطری پایانه همراه متوجه حمله نشود. با توجه به این شرایط، مدت زمان این حمله می‌تواند بین هشت تا سی ساعت به طول بینجامد.

حمله به الگوریتم A5

در این بخش چهار حمله مطرح و شناخته شده به الگوریتم رمز A5 به‌طور خلاصه معرفی می‌شود.

حمله‌ی جستجوی کامل کلید الگوریتم A5

احتمال انجام حمله‌ی جست‌وجوی کامل فضای کلید به‌صورت بلادرنگ به الگوریتم A5 بسیار دشوار است. تنها با تقبل هزینه‌های بالا می‌توان این نوع حمله را برای یافتن کلید به A5 اعمال کرد زیرا این نوع حمله اصولاً از نوع حملات سخت‌افزاری است. پیچیدگی زمانی این نوع حمله، 2^{54} است (زیرا ۱۰ بیت از کلید همواره صفر است و در نتیجه فضای جست‌وجو از 2^{64} به 2^{54} کاهش می‌یابد). برای اعمال حمله ابتدا باید چندین فریم مبادله شده بین MS و BTS را ذخیره، و سپس حمله را آغاز کرد.

اگر از تراشه‌یی معادل با پردازشگر Pentium III که دارای ۲۰ میلیون ترانزیستور است استفاده کنیم و اگر پیاده‌سازی تَبّات‌های الگوریتم A5/1 حدوداً نیاز به ۲۰۰۰ ترانزیستور داشته باشد، در هر تراشه می‌توان ۱۰۰۰۰ عدد الگوریتم A5/1 را به‌صورت موازی پیاده‌سازی کرد و اگر تراشه‌ها با کلاک ۶۰۰ مگاهرتز کار کنند و هر الگوریتم A5/1 دنباله‌ی خروجی معادل ۳۲۸=۱۱۴+۱۱۴+۱۰۰ بیت را با سرعت یک بیت در هر کلاک تولید کند، می‌توان در هر ثانیه ۱۰۰۰ × ۱/۸۲۹/۲۶۸ دنباله کلید را تولید کرد. با توجه به فضای جست‌وجوی 2^{54}، برای پردازش کامل فضای جست‌وجو زمان مورد نیاز ۹۸۴/۷۸۷ ثانیه یا به‌عبارتی ۲۷۳ ساعت است. اگر به‌جای محاسبه‌ی کامل کلید و مقایسه‌ی آن با دنباله‌ی کلید اصلی، دنباله‌ی کلید را بیت با بیت مقایسه کنیم می‌توان زمان حمله را به نسبت یک سوم کاهش داد. همچنین با استفاده از تعداد تراشه‌های بیشتر می‌توان زمان حمله را به‌صورت مؤثرتر و با شدت بیشتر کاهش داد ولی همان‌طور که گفته شد این حمله نیاز به هزینه‌ی بالایی دارد.[۹]

حمله‌ی تقسیم و حل برای دست‌یابی به کلید الگوریتم A5/1

اعمال این نوع حمله باعث می‌شود تا پیچیدگی زمانی حمله جست‌وجوی کامل از 2^{54} به 2^{45} کاهش یابد (در حقیقت حمله $2^9 = 512$ برابر سریع‌تر انجام می‌شود.)[۵] حمله‌ی تقسیم و حل یک حمله با فرض دانستن متن اصلی و متن رمزگذاری شده‌ی متناظر با آن است. حمله‌کننده سعی می‌کند تا حالت اولیه‌ی ثبات‌ها را از روی دنباله‌ی کلید خروجی به دست آورد. در حقیقت حمله‌کننده از روی تعدادی از متن‌های اصلی و متن‌های رمز شده معادل آنها، ۶۴ بیت کلید را محاسبه می‌کند در حمله‌ی تقسیم و حل، ابتدا یک مقدار برای محتوای دو تَبّات کوچک‌تر حدس می‌زنند و سپس می کوشند تا محتوای تَبّات سوم را از روی محتوای دو تَبّات کوچک‌تر و دنباله‌ی کلید خروجی محاسبه کنند. در این حالت اگر شیفت یافتن تَبّات سوم مستقل از دو ثبات دیگر باشد، پیچیدگی زمانی برابر 2^{40} می‌شود ولی چون بیت میانی هر سه ثبات در شیفت یافتن ثبات‌ها مؤثر است، باید برای بیت‌های میانی تا بیت LSB تَبّات سوم مقادیر را حدس بزنیم. در نتیجه پیچیدگی زمانی به 2^{45} افزایش پیدا می‌کند.[۵و۳]

گالیچ نوع دیگری از حمله تقسیم و حل را پیشنهاد کرد که در آن پیچیدگی زمانی به 2^{24} کاهش می‌یابد.[۱۱] گالیچ نشان داد که فضای حالت‌های تَبّات‌ها به‌جای 2^{64} در واقع 2^{30} است. او با در نظر گرفتن این فرض نشان داد که چگونه می‌توان یک سری معادلات خطی را بین حالت‌های هر سه تَبّات نوشت. پیچیدگی حل این معادلات خطی 2^{25} است که برای حل این معادلات به‌ازای تمام حالت‌ها به‌طور متوسط 2^{24} عمل محاسباتی مورد نیاز است (نصف کل حالات). همچنین گالیچ یک نوع حمله‌ی مصالحه‌ی زمان ـ حافظه را پیشنهاد کرد که در آن، هدف یافتن Kc از روی دنباله‌ی کلید خروجی و شماره‌ی فریم معادل آن است.[۱۱]

حمله‌ی روز تولد اریب به الگوریتم A5/1 [۴]

این حمله که مبتنی بر نقطه ضعف موجود در الگوریتم رمزنگاری و امکان شنود مکالمات در شبکه‌ی GSM است، از نوع حمله با استفاده از متن‌های اصلی معلوم بوده و هدف از آن، به‌دست آوردن کلید Kc و تعیین یک حالت اولیه‌ی مناسب برای الگوریتم رمز طی یک دوره‌ی زمانی مشخص است.

حمله از دو بخش پیش‌پردازش اولیه که می‌تواند مستقل از کلید جلسه به انجام رسد، و محاسبات ثانویه که وابسته به Kc است تشکیل شده است.

ایده‌ی اصلی حمله برگرفته از معاوضه‌ی حافظه و زمان برای حمله به الگوریتم‌های رمز دنباله‌یی است که توسط گالیچ[۱۱] مطرح شده است. به این منظور ابتدا به‌عنوان پیش‌پردازش، مجموعه‌یی بزرگ از حالت‌های اولیه تشکیل و در حافظه‌ی کامپیوتر ذخیره می‌شوند. این حالت‌های اولیه منجر به تولید دنباله‌هایی در خروجی الگوریتم می‌شوند که در یک زیردنباله مانند α با طول ثابت K مشترک‌اند. تعداد عناصر مجموعه‌ی A حدوداً 2^{64-K} است. سپس به‌عنوان مرحله‌ی ثانویه مجموعه B از حالت‌های اولیه با توجه به دنباله‌ی خروجی در دسترس، تشکیل و نقاط اشتراک دو مجموعه‌ی A و B برای دست‌یابی به حالت اولیه‌ی واقعی مورد جست‌وجو قرار می‌گیرند. با استفاده از این حمله و در صورت در اختیار داشتن ۲ دقیقه از خروجی الگوریتم رمز و پیش‌پردازش 2^{24} حالت اولیه، و ذخیره‌ی آنها بر روی حافظه‌یی برابر

با ۲۹۲ گیگا بایت، می‌توان حالت اولیه و کلید Kc را در مدت ۱ ثانیه به‌دست آورد.

حمله به الگوریتم A۵/۲

اهمیت بررسی و تحلیل الگوریتم A۵/۲ بدان سبب است که الگوریتم مورد استفاده برای رمزنگاری صحبت مشترکین تلفن همراه در کشور ما است. الگوریتم A۵/۲ نسبت به الگوریتم A۵/۱ ضعیف‌تر است و حملات متعددی بر علیه آن طراحی و پیاده‌سازی شده است.[۱۲و۱۳] مثلاً در یکی از این حملات چهارفریم نامتوالی از دنباله‌ی بیت‌های خروجی الگوریتم A۵/۲ برای مشخص‌کردن بقیه‌ی بیت‌های دنباله‌ی خروجی به‌کار برده می‌شود.[۱۲] در بدترین حالت پیچیدگی زمانی اجرای این حمله برابر با 2^{17} می‌شود، که این مقدار برابر تعداد عناصر موجود در فضای زیرکلید (محتوای ثبات R۴) است. این فضا می‌تواند به فضاهای مستقل از هم تقسیم، و توسط رایانه‌های جداگانه‌یی پردازش شود. به این طریق تحلیل الگوریتم برای یافتن بیت‌های خروجی را می‌توان به‌صورت بلادرنگ انجام داد. در حمله‌ی دیگری که بسیار مؤثرتر از حمله قبلی به الگوریتم A۵/۲ است.[۱۳] در این حمله فقط به متن رمز شده‌ی مکالمات مشترکین تلفن همراه مورد نیاز است که این موضوع خود یکی از امتیازات این حمله نسبت به دیگر حملات است، زیرا پیاده‌سازی این حمله نسبت به حملات قبلی عملاً بسیار مؤثرتر بوده و به اطلاعات غیر واقعی مانند دنباله‌ی خروجی A۵/۲ نیاز ندارد. در این حمله با استفاده از مدت زمان محدودی (در حدود چند میلی ثانیه) از خروجی مکالمات رمز شده‌ی مشترکین (که در فاصله‌ی هوایی بین MS و BTS مبادله می‌شوند)، و در مدت زمانی کم‌تر از یک ثانیه، توسط یک رایانه‌ی شخصی، می‌توان کلید Kc را محاسبه کرد. پیچیدگی زمانی این حمله 2^{16} است که بیانگر حمله‌یی بلادرنگ است. این حمله شامل دو مرحله‌ی کلی است:

۱. مرحله‌ی اول یک حمله متن اصلی معلوم به A۵/۲ است که حالت اولیه (محتوی ثبات‌ها پس از تزریق کلید و شماره فریم) را مشخص می‌کند. این قسمت از حمله دارای ماهیت جبری است که از نقطه ضعف پایین بودن مرتبه‌ی تابع تولید بیت خروجی A۵/۲ استفاده می‌کند. در این قسمت از حمله ابتدا بیت خروجی A۵/۲ را به‌صورت یک تابع چندمتغیره نسبت به حالت اولیه ثبات‌های A۵/۲ تعریف می‌کنند. پس از آن سیستمی از معادلات فوق‌الذکر را با استفاده از بیت‌های خروجی در فرایند تولید دنباله‌ی کلید به دست می‌آورند و با تشکیل حالت اولیه‌ی ثبات‌ها در هر مرحله از این فرایند، به حل معادلات می‌پردازند.

۲. در مرحله‌ی دوم حمله‌ی متن اصلی معلوم به حمله‌ی متن رمز شده توسعه می‌یابد. این کار با توجه به به‌کارگیری کدهای تصحیح خطا قبل از برقراری رمزنگاری انجام می‌شود.

نتیجه‌گیری

شبکه GSM در حال حاضر توسط بیش از یک میلیارد مشترک تلفن همراه مورد استفاده قرار می‌گیرد. توسعه‌ی چشم‌گیر شبکه‌ی GSM به‌علت تقاضای فراوان مشترکین برای دریافت سرویس از آن بوده است. اهداف امنیتی GSM عبارت از احراز اصالت مشترکین تلفن همراه، تامین گمنامی مشترکین سرویس‌گیرنده از دید عامل غیرمجاز، محرمانگی اطلاعات صحبت مشترکین تلفن همراه، انتقال و ذخیره‌سازی اطلاعات مهم با تأمین ویژگی‌های محرمانگی، جامعیت و احراز اصالت و مقابله با حملات مطرح شده به کانال‌های رادیوئی است. برای رسیدن به این اهداف، الگوریتم‌های رمزنگاری و پروتکل‌های مختلفی توسط طراحان GSM پیشنهاد و در شبکه پیاده‌سازی شده است.

در حال حاضر در ایران تقریباً روزانه ۲۵ میلیارد ریال برای استفاده از تلفن همراه پرداخت می‌شود که سالیانه بالغ بر ۹۰۰۰ میلیارد ریال می‌شود. از سوی دیگر، وزارت ارتباطات و فناوری اطلاعات سرمایه‌گذاری کلانی برای توسعه‌ی شبکه تلفن همراه در همین مقیاس انجام داده است. ارقام فوق‌الذکر میزان گسترش استفاده از تلفن همراه را در انواع کاربری‌ها در کشور نشان می‌دهد. نکته‌ی مهم این که علی‌رغم چنین سرمایه‌گذاری سنگین و دامنه‌ی استفاده‌ی گسترده، سیستم GSM قابل تغییر، تنظیم یا بهبود نیست و به شکل موجود آن باید خریداری، نصب و استفاده شود. برای کاهش میزان آسیب‌پذیری امنیتی این سیستم پروتکل‌های جایگزینی در کنفرانس‌ها و مجامع علمی گوناگون پیشنهاد شده است ولی عملاً به‌دلیل سرمایه‌گذاری‌های سنگینی که در سیستم فعلی صورت گرفته، پذیرفته و پیاده‌سازی نشده‌اند. لذا در موقعیت کنونی آگاهی کامل و دقیق از جزئیات معماری و ویژگی‌های امنیتی سیستم تلفن همراه GSM و استفاده از تمام گزینه‌های موجود در سیستم و توجه به نقاط ضعف امنیتی آن برای کاهش میزان آسیب‌پذیری امنیتی آن ضرورتی اجتناب‌ناپذیر است.

در پیاده‌سازی GSM کلیه‌ی ملاحظات امنیتی لازم لحاظ نشده است. به‌عنوان مثال الگوریتم‌های رمزنگاری به‌کار رفته در آن بدون انجام تحلیل‌های کافی، طراحی شده‌اند. الگوریتم COMP۱۲۸ یکی از این مواردی است که نقاط ضعف موجود در آن باعث تولید سیم‌کارت‌های جعلی در GSM شد. عدم وجود امنیت لازم در الگوریتم‌های A۵/۱ و A۵/۲ نیز باعث شنود مکالمات مشترکین در مسیر رادیویی می‌شود. پروتکل‌های موجود در GSM نیز آسیب‌پذیرند، به‌طوری که حملاتی مثل

جدول ۲. آسیب‌های ناشی از عدم استفاده از ویژگی‌های امنیتی GSM.

ردیف	ویژگی امنیتی	چگونگی فراهم شدن ویژگی امنیتی	آسیبی که در صورت عدم استفاده از ویژگی امنیتی به‌وجود می‌آید
۱	گمنام بودن مشترکین سرویس گیرنده	استفاده از شماره موقت TMSI به‌جای استفاده مستقیم از IMSI	می‌توان سیم‌کارت مشترک مورد نظر را تشخیص داده و به آن حمله کرد.
۲	احراز اصالت مشترکین	از طریق الگوریتم A۳ و چالش شبکه و پاسخ سیم‌کارت فراهم می‌شود	سرویس گرفتن مشترکین غیرمجاز (جعلی) از شبکه
۳	محرمانگی مکالمات	استفاده از الگوریتم A۵ در فاصله‌ی هوایی	شنود مکالمات مشترکین
۴	محرمانگی کلید Ki	استفاده از الگوریتم‌های A۴ ,A۲	آشکار شدن کلید Ki و جعل سیم‌کارت
۵	جامعیت فایل حاوی Kiها	استفاده از الگوریتم‌های A۹ ,A۷	تعریف Ki جعلی و نهایتاً جعل سیم‌کارت

جدول ۳. آسیب‌پذیری الگوریتم‌های GSM.

ردیف	آسیب	نقطه ضعف	نوع حمله
۱	آشکار شدن IMSI	پروتکل ورود MS به شبکه GSM (پروتکل احراز اصالت یک‌سویه)	حمله از طریق عامل میانی
۲	جعل سیم‌کارت	الگوریتم A۳ (COMP۱۲۸)	اعمال چالش‌های منتخب به سیم‌کارت
۳	جعل سیم‌کارت	الگوریتم A۳ و پروتکل احراز اصالت GSM	ترکیبی از حمله از طریق عامل میانی و اعمال چالش‌های منتخب به سیم‌کارت
۴	جعل سیم‌کارت و شنود مکالمات	الگوریتم A۸ (COMP۱۲۸)	اعمال چالش‌های منتخب به سیم‌کارت و حمله تفکیکی
۵	شنود مکالمات	الگوریتم A۵	جست‌وجوی کامل کلید
۶	شنود مکالمات	الگوریتم A۵	حمله تقسیم و حل
۷	شنود مکالمات	پروتکل موجود در شبکه انتقال سیمی	دسترسی مستقیم به شبکه انتقال سیمی
۸	شنود مکالمات	پروتکل ورود MS به شبکه GSM و صدور دستور عدم رمزنگاری	حمله از طریق عامل میانی
۹	شنود مکالمات	الگوریتم A۵/۱	حمله تحلیلی از نوع متن اصلی معلوم
۱۰	شنود مکالمات	الگوریتم A۵/۲	حمله تحلیلی از نوع متن اصلی معلوم
۱۱	شنود مکالمات	الگوریتم A۵/۲	حمله تحلیلی از نوع فقط متن رمز شده
۱۲	ایجاد اختلال عمدی در مکالمات	کانال‌های رادیویی GSM و تایمرهای موجود در MSC	حمله نفی سرویس
۱۳	ایجاد اختلال عمدی در مکالمات	پروتکل احراز اصالت GSM	حمله از طریق عامل میانی

آشکارساز IMSI و حمله از طریق عامل میانی به‌راحتی امکان‌پذیرند. تحلیل الگوریتم COMP۱۲۸ تنها راه محاسبه‌ی Ki و شنود مکالمات مشترکین نیست؛ حملات جست‌وجوی کامل، حمله‌ی تقسیم و حل، حمله از طریق دسترسی به شبکه‌ی انتقال سیمی، بازیابی کلید Kiاز درون سیم‌کارت با بمباران چالش‌ها به سیم‌کارت و از طریق فاصله‌ی هوایی، بازیابی Ki از طریق مرکز احراز اصالت و محاسبه‌ی Ki از طریق تحلیل الگوریتم A۸، از جمله حملاتی است که محاسبه‌ی Kiو شنود مکالمات مشترکین را ممکن می‌سازد. به‌طور کلی GSM در هر دو مقوله‌ی الگوریتم‌های رمزنگاری پیاده‌سازی شده و پروتکل‌های به‌کار رفته در آن دارای نقاط ضعف فراوانی است، به‌طوری که استفاده از آن برای کاربری‌های راهبردی و در پاره‌یی از کاربری‌های تجاری از امنیت لازم برخوردار نیست. در ادامه خلاصه‌یی از بررسی‌های صورت گرفته در این نوشتار در جداول ۲ و ۳ ارائه شده‌اند. جدول ۲ ویژگی‌های امنیتی موجود در GSM به همراه چگونگی حصول این اهداف توسط الگوریتم‌ها و پروتکل‌های مربوطه و آسیبی که در صورت عدم استفاده از این ویژگی‌های امنیتی به‌وجود می‌آیند را شامل می‌شود. جدول ۳ به‌ارائه‌ی انواع آسیب‌هایی که به GSM وارد می‌شود، به‌همراه نقطه ضعف مؤثر در به‌وجود آمدن آسیب و نوع حمله پرداخته است.

قدردانی

این نوشتار از حمایت مالی نسبی سازمان مدیریت و برنامه‌ریزی کشور وزارت ارتباطات و فنّاوری اطلاعات از محل اعتبارات موضوع بند الف ماده‌ی ۱۰۲ طی قرارداد شماره‌ی ۱۷۲۰ منعقده با معاونت پژوهشی دانشگاه صنعتی شریف برخوردار بوده است.

پانوشت

1. Global System for Mobile Communication
2. swithcing system
3. base station system
4. mobile station
5. base transiver station
6. base station controller
7. mobile swithing center
8. visitor location register
9. home location register
10. authentication center
11. equipment identity register
12. international mobile subscirber identity
13. mobile subscriber ISDN number
14. temporary mobile subscriber identity
15. sign response
16. clock controlled
17. personalization center
18. secutity management center
19. frequency hopping
20. denial of service
21. man in the middle
22. partition attack

منابع

۱. سایت اینترنتی شرکت مخابرات ایران-http:// www. irantele .com.ir/

2. Berson, T., "GSM system security study", Technical Reports, 20 April 1988, available at http://jya.com/gsm061088.pdf.

۳. «بررسی امنیت در تلفن همراه GSM و پیاده‌سازی حملات مطرح شده به الگوریتم‌های رمزنگاری A۵/۱ و A۵/۲» محسن بهداری، *پایان‌نامه کارشناسی ارشد، دانشکده‌ی مهندسی برق، دانشگاه صنعتی شریف*، (آبان ۱۳۸۲).

4. Briyukov, A., Shamir, A., Wagner, A., "Real time cryptanalysis of A5/1 on a PC", Advances in Cryptology, proceedings of Fast Software Encryption'00, Lecture Notes in Computer Science 2000, Springer-Verlg, pp. 1-18, (2001).

5. Brookson, C., "GSM (and PCN) Security Encryption", available at http: //www.brookson.com/gsm/gsmoc.pdf.

6. Briceno, M., Goldberg, I., Wagner, D., "A pedagogical implementation of A5/1", available at http://lis.fh-aargau.ch/LISApplectures/lectures/GSM.pdf.

7. Ryan, I., "GSM-Based", German Motorway Toll Trial, available at Technical Reports http://cryptome.org/gsma512.html.

8. Singh, M., Chen Khong, T., "SingAREN and IBM collaborate on advanced internet technologies", http: //www.singaren.net.sg/ library/presantations/28apr 99-3.pdf.

9. Rao, J.R., Scherzer, P., "Partition Attacks: Or How to Rapidly Clone Some GSM Cards", available at https: //infocentre.gsm.org /fraud/simcard-clone.ps.

10. Bortzmeyer, S., "Data encryption and the law(s) results", available at http://web.cnam. fr/Network/Crypto/survey. html.

11. Golic, I., "Cryptanalysis of alleged A5 stream cipher", Advances in Cryptology, proceedings of Eurocrypt'97, LNCS 1233, pp. 230-255, (1997).

12. Petrovic, S., Fuster, A., "An improved cryptanalysis of A5/2 algorithm", Proceedings of the IASTED International Conference on Communication Systems and Networks, Malaga, Spain, pp. 437-442. (2000).

13. Barkan, E., Biham, E., Keller, N., "Instant ciphertext-only cryptanalysis of GSM encrypted communication", Advances in Cryptology - CRYPTO 2003, 23rd.*Annual International Cryptology Conference,* Santa Barbara, California, USA, August 17-21, 2003, Proceedings. Lecture Notes In Computer Science, Volume 2729, pp. 600-616 (2003).