مشترک مورد نظر درست است

امنیت شبکه مخابراتی و بررسی حملات رایج

محمدمهدی واعظی‌نژاد

GSM یکی از فناوری‌های مورد استفاده در شبکه‌های مخابراتی است که در بین شبکه‌های سلولی، حدود دو میلیارد نفر مشترک داشته و هم اکنون در کشور ما نیز برای ارتباطات سیار از آن استفاده می‌شود. از مهم‌ترین مشخصات GSM که بهره‌گیری از آن را برای بسیاری از کشورها نسبت به دیگر فناوری‌های مشابه، مقرون به صرفه کرده است می‌توان به داشتن دسترسی رادیویی TDMA و ترانکینگ PCM، استفاده از سیگنالینگ SS۷ (سیگنالینگ شماره ۷ در GSM) به منظور ارتباط سیگنالینگی و همچنین قابلیت تشخیص هویت و رمزنگاری آن اشاره کرد. با وجود این‌که این فناوری در دوران بلوغ خود قرار دارد و تاکنون نسل تکامل‌یافته را پشت سر گذاشته است، متاسفانه با مشکلات امنیتی متعددی روبه‌روست. اگرچه تاکنون مؤسسه استانداردسازی ارتباطات راه دور اروپا (ETSI) به منظور تأمین امنیت شبکه‌های GSM توصیه‌نامه‌هایی را به شماره‌های TS۲,۰۹ ، TS۲,۴۸ ، TS۳,۴۸، TS۳,۲۰ و TS۱۲,۰۳ منتشر کرده است، اما تمامی این توصیه‌نامه‌ها نتوانسته است به مشکلات امنیتی این فناوری پایان دهد. امروزه در شبکه‌های مبتنی بر GSM تقلب بسیاری روی می‌دهد و تاکنون راهی برای پایان دادن به آنها یافت نشده است؛ تقلب‌هایی که برای انجام آنها نیاز به تجهیزات پیشرفته یا فناوری‌های پیچیده‌ای نبوده و براحتی قابل انجام هستند. براساس گزارشی که GSMA نخستین بار سال ۲۰۰۲ منتشر کرد و در گزارش‌های بعدی نیز بر آن اذعان داشت، پنج نوع تقلب عمده در شبکه‌های GSM رخ می‌دهد که عبارت است از:

- تقلب در اشتراک سیمکارت (۴۱ درصد)
- تقلب در وضع رومینگ (۱۶ درصد)
- تقلب در کارت‌های تمدید اعتبار (۱۰ درصد)
- تقلب توسط کارمندان شرکت (۸ درصد)
- تقلب در گوشی (۵ درصد)

همچنین غیر از مواردی که در بالا ذکر شد، تقلب‌های دیگری نیز در GSM می‌تواند صورت پذیرد که عبارت است از:

- انتقال مکالمه به شماره‌های Premium Rate که به پرداخت تمام هزینه مکالمه توسط مشترک منجر خواهد شد.
- انتقال مکالمه به چند مشترک و برگزاری کنفرانس‌های تلفنی

منشا اصلی تقلب و مشکلات امنیتی در GSM به این ترتیب است که در این شبکه فقط امنیت دسترسی فراهم می‌شود و سازوکارهای امنیتی برای ارتباطات و ترافیک سیگنالینگ مربوط به شبکه ثابت در آن پیش‌بینی نشده است و از جهت اتصالات سیگنالینگی به شبکه ثابت، شبکه GSM تنها به میزانی امن است که شبکه ثابت ایمن شده باشد. در فناوری GSM آدرس‌دهی حملات انجام‌شده به بعضی عناصر فعال مانند BTSها امکان‌پذیر نبوده و شنود قانونی را نیز فقط زمانی می‌توان انجام داد که مشترک در شبکه باشد. همچنین نبود اطمینان از هویت صحیح ترمینال‌ها و اطمینان خاطر از رمزنگاری مشترک از دیگر مشکلات امنیتی GSM است.

برای کاهش تقلب در شبکه‌های GSM پیشنهاد می‌شود اپراتورها توسط یک سیستم مدیریت تقلب در شبکه با دقت موارد را بررسی و امور زیر را پیگیری کنند:

- برقراری تماس همزمان یک مشترک با چند مشترک دیگر
- وجود تغییرات زیاد در درآمد پرداخت شده توسط مشترک
- وجود تغییرات بسیار در مدت زمان تماس مشترک به نحوی که تماس‌ها گاهی خیلی کوتاه و گاه خیلی طولانی باشد.
- تغییرات ناگهانی در نوع استفاده مشترک (صوت به دیتا و بالعکس) که می‌تواند نشان‌دهنده دزدیده شدن تلفن همراه باشد.
- زیرنظر گرفتن نحوه استفاده مشترک از گوشی در یک دوره زمانی اتفاقی

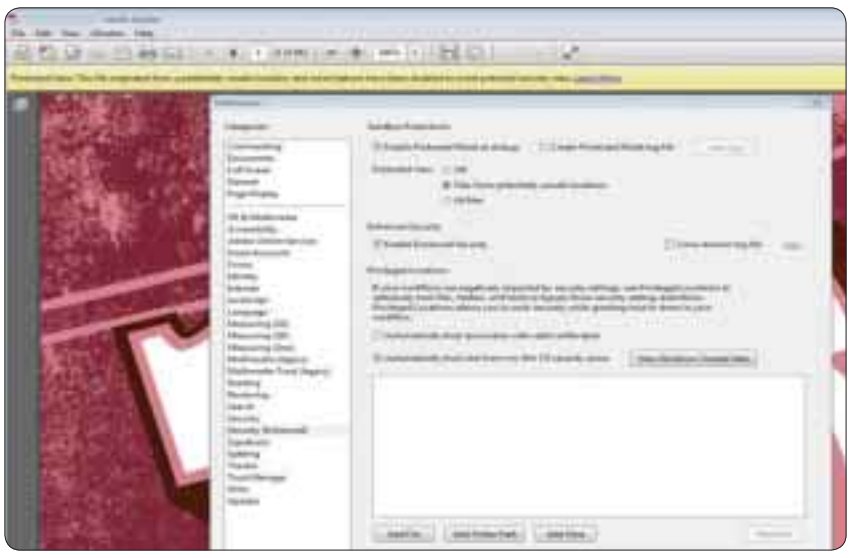
متاسفانه به دلیل مشکلات متعدد امنیتی که فناوری GSM با آن مواجه است و برخی آنها در بالا ذکر شد، امروزه حملات سازمان‌یافته‌ای به شبکه‌های GSM صورت می‌گیرد که در موارد بسیاری علاوه بر سرقت اطلاعات و مشخصات هویتی تعداد زیادی از مشترکان، باعث بروز مشکلاتی برای شهروندان شده است. از جمله حملاتی که توسط گوشی‌های تنظیم‌شده روی شبکه‌های GSM قابل اجراست، می‌توان به موارد زیر اشاره کرد:

- شنود مکالمات و امکان دزدی اتصالات سیگنالینگی و دیتایی سایر مشترکان
- جعل هویت یک مشترک با جا زدن نفوذگر به جای شخص واقعی و ارسال اطلاعات دیتایی به دیگر مشترکان
- ثبت غیرواقعی مشترک که با سوء استفاده از ضعف شبکه و سرقت پیغام‌های هویت از اینترفیس‌های هوایی صورت می‌گیرد. سپس مهاجم با ارسال پیام (IMSI) به شبکه، ثبت یک مشترک تقاضا می‌کند که در این صورت، شبکه مشترک را از VLR ثبت کرده و به HLR می‌فرستد و تقاضای ثبت موقعیت را در یکی از مناطقی که مشترک به آنجا رومینگ داشته است، انجام می‌دهد. آن گاه شبکه، مشترک را در یک منطقه جدید ثبت و اطلاعات را به آنجا ارسال می‌کند که البته در این حالت، مشترک امکان بهره‌مندی از سرویس MT را نخواهد داشت.

همچنین حملات شناخته شده‌ای که می‌توان به شبکه‌های GSM از طریق BTSهای تنظیم شده انجام داد، عبارت است از:

- جعل هویت شبکه و امکان ارسال اطلاعات سیگنالینگی به یک مشترک خاص به نحوی که آن مشترک خیال کند این اطلاعات از شبکه امنی برای او در حال ارسال است.
- امکان قرارگیری بین مشترک و شبکه، همانند حملات کاربر بدخواه (Man in the middle) در یک شبکه که در این روش، مهاجم می‌تواند خود را در بین مشترک و شبکه قرار داده و به دزدی، اصلاح، حذف، تغییر یا شنود غیرقانونی پیغام‌ها و ترافیک شبکه اقدام کند.

علاوه بر حملات ذکر شده، حملاتی بر نودهای شبکه GSM نیز می‌تواند انجام شود که از جمله می‌توان به CCBS، MSC، AUC، HLR و VAS اشاره کرد. در حملاتی که از طریق HLR صورت می‌پذیرد مهاجمان می‌توانند با دسترسی به HLR، به فعال کردن مشترکانی که در سیستم بیلینگ ثبت نشده‌اند و لذا قابل شارژ نیستند، اقدام و سرویس‌های مختلفی را هم برای این مشترکان جعلی ایجاد کند. همچنین با استفاده از دستورات مشخص، قادر به پایش مشترکان HLR بوده و دسترسی غیرمجاز به دیتا را برای خویش فراهم می‌آورند. متاسفانه در بیشتر موارد، اپراتورها به تصور این که مهاجمان شناخت کافی از دستورات یک فروشنده خاص تجهیزات ندارند، اقدام‌های کنترلی مناسبی را در این خصوص انجام نمی‌دهند؛ در حالی که این حملات معمولا با همکاری اشخاص خارجی و مشارکت کارمندان داخلی صورت می‌گیرد.



برای جلوگیری از این نوع حملات، باید کنترل دسترسی به HLR براساس پروفایل‌هایی باشد که حداقل از یک نام کاربری و کلمه عبور منحصر به فرد برای احراز هویت و تصدیق اطلاعات شناسایی کاربران مجاز استفاده می‌کند. دسترسی از راه دور نیز باید از مواردی همچون تقلب، جعل منبع و مقصد محافظت شود که برای تحقق آن لازم است تا حد امکان، نقاط اتصال به HLR کاهش یابد.

در حملاتی که توسط AUC انجام می‌شود نیز می‌توان با کاهش تعداد کارمندانی که به AUC دسترسی دارند و جداسازی AUC با HLR و جلوگیری از یکی بودن آنها امنیت بیشتری را فراهم کرد. رمزنگاری اطلاعات AUC با الگوریتم‌های رمزنگاری قدرتمند و محرمانه نگهداشتن الگوریتم رمزنگاری مربوط همراه مدیریت کلید رمزها می‌تواند در تامین امنیت بهتر، موثر واقع شود.

MSC هم که یکی از مهم‌ترین نودهای شبکه GSM بوده و تمام تماس‌های ورودی به مشترکان یا خروجی از آنها را در یک منطقه خاص، ساماندهی می‌کند می‌تواند با دسترسی غیرمجاز، به خطر افتاده و باعث فقدان امنیت اطلاعات مشترکان و سرویس‌های آنها شود. بنابراین توصیه می‌شود دسترسی فیزیکی و منطقی به MSC بشدت کنترل و محدود شده و مکان فیزیکی که MSC ها در آن قرار دارند نیز عمومی نباشد. در حالت هم‌مکانی باید MSCها امکانات توان و انتقال مستقلی داشته باشند تا در صورت بروز حادثه برای یکی از آنها، سایر MSCها تحت تاثیر قرار نگیرند.

در حملات CCBS نیز دسترسی غیرمجاز به سیستم صورتحساب B.C باعث می‌شود درآمد حاصل از CDRها از بین رفته و علاوه بر درنظر گرفتن تخفیف‌های غیرواقعی به سرویس‌ها، دسترسی غیرمجاز به سرویس‌ها هم فراهم شود.

بنابراین برای تامین امنیت بیشتر مشترکان و همچنین برخورداری آنها از جدیدترین سرویس‌های مخابراتی، بهتر است شبکه GSM ارتباطات سیار کشور به شبکه ۳G تغییر یابد و همگام با فناوری روز جهان، خدمات پیشرفته‌ای را به مردم عزیز کشورمان ارائه کند.

فناوری ۳G در مقایسه با فناوری GSM دارای ویژگی‌های امنیتی بسیاری است که آن را در مقابل حملات، امن‌تر می‌سازد. از جمله این موارد می‌توان به سازوکارهای پیش‌بینی شده امنیتی در BTSها اشاره کرد که شامل یک دنباله عددی است که تلفن‌همراه توسط آن، شبکه را تشخیص می‌دهد. مواردی همچون افزیش طول کلید جهت ایجاد الگوریتم‌های رمزنگاری قوی‌تر، پیاده‌سازی ویژگی‌های امنیتی در سوئیچ‌ها به جای BTS ها که با این کار، امنیت از لینک‌ها نیز فراهم می‌شود، توجه به سازوکارهای سلامت ترمینال از همان ابتدا، که این مساله اصلا در GSM مطرح نیست، ایجاد پنج پارامتر کلیدی تشخیص هویت در ۳G را که در GSM فقط ۳ مورد است می‌توان از دیگر ویژگی‌های امنیتی اضافه شده در فناوری ۳G دانست.

مدل امنیتی خاصی که در ۳G در پنج سطح اجرا می‌شود، عبارت است از:

۱. امنیت دسترسی به شبکه که مجموعه‌ای از ویژگی‌های امنیتی، امکان دسترسی کاربران به سرویس‌های ۳G را فراهم کرده و به طور خاص، شبکه را از حملات توسط لینک رادیویی محافظت می‌کند.

۲. امنیت در حوزه شبکه که در آن، مجموعه‌ای از ویژگی‌های امنیتی، نودها را قادر می‌سازد تا در ناحیه فراهم کننده، اطلاعات سیگنالینگی را به طور امن تبادل کند و در برابر حملات شبکه سیمی حفاظت شود.

۳. امنیت در حوزه کاربران که مجموعه‌ای از ویژگی‌های امنیتی، دسترسی به MSها را ایمن می‌سازد.

۴. امنیت در حوزه کاربردها که مجموعه‌ای از ویژگی‌های امنیتی، تبادل اطلاعات را بین حوزه‌های کاربر و فراهم کننده، برقرار می‌کند.

۵. قابلیت تنظیم امنیت که کاربر توسط مجموعه‌ای از ویژگی‌های امنیتی متوجه می‌شود که آیا ویژگی‌های امنیتی در شبکه در حال استفاده است و این که استفاده و تدارک سرویس‌ها به ویژگی‌های امنیتی بستگی دارد یا خیر.