دانشکده مهندسی کامپیوتر

تمرین امتیازی GSM فصل دوم

امنیت سیستم‌های کامپیوتری

مدرس: دکتر ابوالفضل دیانت

محمدحسین عباسپور، فرزان رحمانی

شماره دانشجویی: ۹۹۵۲۱۴۳۳، ۹۹۵۲۱۲۷۱

نیم سال دوم
سال تحصیلی ۱۴۰۳-۱۴۰۲

۱ شبکه GSM

شبکه GSM یک استاندارد بین‌المللی برای ارتباطات سلولی است که برای اولین بار در دهه ۱۹۹۰ معرفی شد. GSM به عنوان یک فناوری نسل دوم (2G) در ارتباطات سلولی شناخته می‌شود و هنوز تا به امروز در بسیاری از کشورها برای ارتباطات سلولی استفاده می‌شود.

۲ ویژگی‌های GSM

ویژگی‌ها و عملکرد شبکه GSM عبارتند از:

- استفاده از فرکانس‌های تقسیم شده : GSM از تکنیک تقسیم فرکانس برای تقسیم باند فرکانسی استفاده می‌کند. با استفاده از FDMA، فرکانس‌های موجود در یک منطقه جغرافیایی به صورت تقسیم شده بین کاربران تقسیم می‌شوند. این به شبکه GSM امکان ارائه خدمات به چندین کاربر به صورت همزمان را می‌دهد.
- استفاده از : GSM TDMA از TDMA برای تقسیم زمانی فرکانس‌های تقسیم شده برای ارسال اطلاعات استفاده می‌کند. با استفاده از TDMA، زمان ارسال اطلاعات بین کاربران تقسیم می‌شود، به طوری که هر کاربر در یک زمان مشخص قادر به ارسال و دریافت اطلاعات است.
- استفاده از SIM : GSM از کارت SIM برای شناسایی و تأیید هویت کاربران استفاده می‌کند. کارت SIM شامل اطلاعات شبکه و کاربر می‌باشد و در دستگاه تلفن همراه قرار می‌گیرد. با استفاده از کارت SIM، کاربران می‌توانند به شبکه GSM متصل شوند و خدمات مخابراتی را دریافت کنند.
- پشتیبانی از خدمات صوتی و داده: GSM امکان ارائه خدمات صوتی (مکالمات) و خدمات داده (از جمله پیامک‌های کوتاه - SMS و ارسال داده‌ها) را فراهم می‌کند. این خدمات به کاربران امکان ارتباط و تبادل اطلاعات را می‌دهند.

شبکه GSM به عنوان یک استاندارد بین‌المللی، امکان اتصال و تبادل اطلاعات بین اپراتورهای مختلف را فراهم می‌کند و اجازه می‌دهد تا کاربران در سراسر جهان با هم ارتباط برقرار کنند.

۳ GSM Active sys

شبکه GSM را می‌توان با استفاده از دستگاهی به نام GSM Active sys شنود کرد. این دستگاه که در حالت عادی به عنوان IMSI Catcher نیز شناخته می‌شود، یک دستگاه مخصوص است که برای شنود و در برخی موارد تغییر و مداخله در ارتباطات شبکه GSM استفاده می‌شود. این دستگاه قادر است ترافیک بی سیم مربوط به تلفن همراه‌های در حال مکالمه در یک شبکه GSM را شنود کند و حتی می‌تواند خود را در میان ارتباط کاربران قرار دهد.

۴ GSM Active sys چگونه کار می‌کند؟

نحوه کار این دستگاه به صورت کلی عبارت است از:

- شبیه‌سازی یک ایستگاه پایه سلولی: دستگاه GSM Active Sys قادر است به عنوان یک ایستگاه پایه سلولی عمل کند و اطلاعات لازم برای شبیه‌سازی ایستگاه پایه را در اختیار دارد. این ایستگاه پایه سلولی می‌تواند به تلفن‌های همراه در محدوده خود سرویس دهد و به آنها ارتباطی تقلبی ارائه دهد.
- تعامل با تلفن‌های همراه: هنگامی که تلفن همراه‌ها در محدوده تحت پوشش دستگاه GSM Active Sys قرار می‌گیرند، آنها سعی می‌کنند به شبکه ایستگاه پایه متصل شوند. در این مرحله، دستگاه GSM Active Sys به نماینده ایستگاه پایه سلولی می‌نماید و اطلاعات مورد نیاز برای برقراری ارتباط را از تلفن همراه دریافت می‌کند.
- شنود ترافیک ارتباطی: پس از برقراری ارتباط تقلبی با تلفن همراه، دستگاه GSM Active Sys قادر است ترافیک ارتباطی بین تلفن همراه و ایستگاه پایه را شنود کند. این شامل مکالمات صوتی، پیامک‌ها، داده‌ها و سایر ارتباطات است.

- تغییر و مداخله در ارتباطات: علاوه بر شنود، دستگاه GSM Active Sys در برخی موارد می‌تواند به صورت فعال در میان ارتباط قرار گیرد و تغییراتی در ارتباطات اعمال کند. به عنوان مثال، می‌تواند تماس‌ها را قطع کند، پیامک‌ها را مسدود کند یا دستکاری در داده‌های انتقالی انجام دهد.

به طور کلی، دستگاه GSM Active Sys با تقلید از ایستگاه پایه سلولی و ایجاد یک ارتباط تقلبی با تلفن همراه‌ها، قادر است ترافیک ارتباطی را شنود کند و در برخی موارد تغییراتی در ارتباطات اعمال کند. با این کار، قادر است به صورت غیرمجاز به اطلاعات حساس کاربران دسترسی پیدا کند.

۵ راه‌های مقابله از GSM Active Sys

برای جلوگیری از این نوع حملات، سازمان ۳GPP (سازمان مشترک تلفن همراه) تلاش کرده است تا استانداردها و روش‌های امنیتی را در شبکه‌های نسل سوم (۳G) و نسل چهارم (۴G) بهبود بخشد. این تلاش‌ها عمدتاً برای محدود کردن قابلیت ایجاد ارتباطات تقلبی و جعلی و تشخیص و جلوگیری از حملات IMSI Catcher صورت گرفته است. به طور کلی، این تلاش‌ها شامل موارد زیر است:

- استفاده از رمزنگاری: شبکه‌های نسل سوم و چهارم از رمزنگاری قوی تری نسبت به GSM استفاده می‌کنند. این رمزنگاری باعث کاهش امکان شنود و تقلب در ارتباطات می‌شود.
- استفاده از الگوریتم‌های امنیتی: استفاده از الگوریتم‌های امنیتی مانند A۵/۳ در شبکه‌های ۳G و الگوریتم‌های امنیتی مبتنی بر AES در شبکه‌های ۴G، امکان تقلب و شنود ارتباطات را به شدت کاهش می‌دهند.
- تشخیص تقلب: سازمان ۳GPP روش‌های تشخیص و جلوگیری از Catcher IMSI را در استانداردها و امکانات شبکه‌های شبکه همراه تعبیه کرده است. این روش‌ها شامل تشخیص تغییرات ناگهانی در پارامترهای شبکه، تشخیص ارتباطات تقلبی و تشخیص تغییرات ناگهانی در مسیرهای ارتباطی هستند. با تشخیص اینگونه حملات، شبکه توانایی جلوگیری از ادامه عملیات تقلبی را دارد.
- استفاده از شبکه‌های همراه نسل پنجم :(۵G) شبکه‌های ۵G از تکنولوژی‌ها و استانداردهای امنیتی پیشرفته‌تری نسبت به نسل‌های قبلی استفاده می‌کنند. این تکنولوژی‌ها شامل شناسایی ارتباطات تقلبی، رمزنگاری قوی‌تر، مدیریت دسترسی پیشرفته و امکانات امنیتی دیگر می‌شوند.

اگرچه تلاش‌های بسیاری برای جلوگیری از حملات Catcher IMSI انجام شده است، اما همچنان امکان وقوع این نوع حملات وجود دارد. بنابراین، شرکت‌های تولیدکننده شبکه و اپراتورهای تلفن همراه نیز باید بهبودهای امنیتی مستمری را در شبکه‌های خود اعمال کنند تا از حملات احتمالی جلوگیری کنند.