



گزارش سمینار کارشناسی ارشد

مهندسی فناوری اطلاعات - گرایش مخابرات امن

بررسی امنیت انتها به انتهای مکالمات و سرویس پیام کوتاه در شبکه GSM

محسن تورانی

خرداد ماه ۱۳۸۶

چکیده

با توجه به گسترش روز افزون و همه گیر شدن استفاده از تلفن همراه، تامین و تضمین امنیت مکالمات امری اجتناب ناپذیر می باشد. از سالها پیش در مجامع علمی دنیا ثابت شده است که شبکه GSM دارای اشکالات و معایب امنیتی فراوان و فاقد ویژگیهای یک شبکه امن می باشد به گونه ای که تمامی مکالمات و یا حتی پیامهای کوتاه ارسالی به راحتی و تحت شرایط خاصی قابل شنود، کشف و یا تغییر می باشند.

در این گزارش سمینار، خلاصه ای از معضلات امنیتی شبکه GSM، موضوع برقراری امنیت انتها به انتها، مشتمل بر رمزنگاری مکالمات و مبادلات سرویس پیام کوتاه (SMS) در شبکه موبایل GSM مورد بررسی قرار می گیرد.

کلمات کلیدی: امنیت شبکه GSM، معضلات امنیتی شبکه GSM، امنیت انتها به انتها، شنود غیرقانونی مکالمات، رمزنگاری SMS، رمزنگاری صدا.

فهرست مطالب

۱	مقدمه
۳	فصل اول: مروری بر شبکه GSM
۳	۱-۱- مقدمه
۸	۱-۲- ساختار شبکه GSM
۱۰	۱-۳- ایستگاه سیار
۱۱	۱-۳-۱- وظایف ایستگاه سیار
۱۳	۱-۳-۲- شکل بندی ایستگاه سیار
۱۴	۱-۳-۳- کارت SIM
۱۶	۱-۳-۴- عددهای شناسایی موبایل
۱۸	۱-۴- سیستم ایستگاه پایه
۲۰	۱-۴-۱- BTS
۲۱	۱-۴-۱-۱- ترانسکدر
۲۲	۱-۴-۲- BSC
۲۳	۱-۵- زیر سیستم های سوئیچینگ
۲۵	۱-۵-۱- MSC
۲۶	۱-۵-۲- VLR
۲۹	۱-۶- ثبات محل اقامت
۳۱	۱-۷- مرکز احراز اصالت
۳۲	۱-۸- ثبات مشخصه تجهیزات
۳۳	۱-۹- مرکز نگهداری و عملیات
۳۴	۱-۱۰- مرکز مدیریت شبکه
۳۵	۱-۱۱- مرکز صدور صورت حساب
۳۷	فصل دوم: اصول امنیتی شبکه GSM
۳۷	۲-۱- مقدمه
۴۰	۲-۲- هویت موقتی مشترک موبایل
۴۲	۲-۳- احراز اصالت در شبکه GSM

۴۷	۲-۴- رمزنگاری در شبکه GSM
۵۱	۲-۵- الگوریتم‌های احراز اصالت و رمزنگاری
۵۲	۲-۵-۱- الگوریتم A3
۵۳	۲-۵-۲- الگوریتم A8
۵۶	۲-۵-۳- الگوریتم A5
۵۹	۲-۶- مشخصات SIM
۶۲	۲-۶-۱- سیر تکاملی سیم کارت
۶۶	۲-۶-۲- امنیت سیم کارت
۶۶	۲-۶-۳- خصوصیات امنیتی تراشه کارت هوشمند
۶۸	۲-۶-۴- خصوصیات امنیتی سیستم عامل کارت
۶۸	۲-۶-۵- خصوصیات امنیتی واسط کارت
۷۰	۲-۷- احراز اصالت تجهیزات
۷۲	فصل سوم: ارزیابی امنیت شبکه GSM
۷۵	۳-۱- ارزیابی امنیت ارتباط هوایی
۷۸	۳-۲- ارزیابی امنیت ستون فقرات GSM
۸۳	۳-۳- مشکلات امنیتی GSM
۹۱	۳-۴- حملات پیشرفته‌تر بر GSM
۹۹	فصل چهارم: مسیرهای انتقال داده در GSM و امنیت آنها
۹۹	۴-۱- WAP
۱۰۳	۴-۲- سرویس پیام کوتاه (SMS)
۱۰۵	۴-۲-۱- معماری SMS
۱۰۷	۴-۲-۲- عملکرد SMS
۱۰۸	۴-۲-۳- سیگنالینگ SMS
۱۰۹	۴-۲-۴- گردش پیام SMS
۱۱۴	۴-۲-۵- امنیت SMS
۱۱۵	۴-۳- داده سرویسهای تکمیلی ساخت نیافته (USSD)
۱۱۶	۴-۳-۱- عملکرد USSD
۱۱۷	۴-۳-۲- مزایای USSD
۱۱۷	۴-۳-۳- تفاوت بین USSD و SMS
۱۱۸	۴-۳-۴- امنیت USSD
۱۲۱	۴-۴- کانال صوتی

۱۲۳	فصل پنجم: امنیت انتها به انتها در شبکه GSM
۱۲۳	۵-۱-SAT
۱۲۴	۵-۱-۱- تاریخچه SAT
۱۲۷	۵-۱-۲- عملکرد SAT
۱۳۰	۵-۱-۳- امنیت SAT
۱۳۵	۵-۲- تکنولوژی دروازه اینترنت بی سیم (WIG)
۱۳۶	۵-۲-۱- معماری WIG
۱۳۶	۵-۲-۲- عملکرد WIG
۱۳۸	۵-۲-۳- امنیت WIG
۱۳۸	۵-۳- رمزنگاری انتها به انتها در شبکه تلفن همراه
۱۳۹	۵-۳-۱- رمزنگاری متقارن
۱۴۰	۵-۳-۲- رمزنگاری نامتقارن
۱۴۳	۵-۳-۳- اعتبارنامه‌ها
۱۴۶	۵-۳-۴- WPKI
۱۴۸	۵-۳-۵- زیرساختهای امن
۱۵۰	۵-۳-۶- تکنولوژی جاوا برای وسایل بی سیم
۱۵۳	۵-۳-۷- رمزنگاری انتها به انتهای صدا
۱۵۷	۵-۳-۷-۱- گوشی GSM
۱۵۹	۵-۳-۷-۲- گوشی GSM امن
۱۶۲	۵-۳-۷-۳- مودم GSM
۱۶۴	۵-۳-۷-۴- رمزنگاری انتها به انتها بر روی کانال صوتی
۱۶۹	۵-۳-۸- رمزنگاری انتها به انتهای پیام کوتاه
۱۷۱	نتیجه گیری
۱۷۲	پیوست ۱: آمار مشترکین تلفن همراه
۱۷۳	پیوست ۲: ادوات کپی سیم کارت
۱۷۷	پیوست ۳: ارزیابی امنیت GSM
۱۷۹	پیوست ۴: پیشنهاداتی جهت افزایش امنیت شبکه تلفن همراه کشور
۱۸۲	منابع مورد استفاده