تمرین امتیازی اول امنیت

عرفان زارع

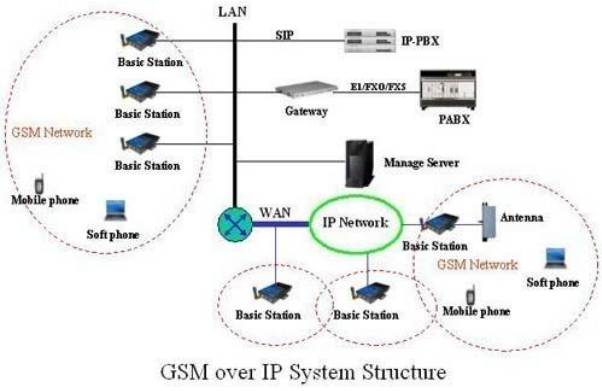
امیررضا ویشته

آبان 1402

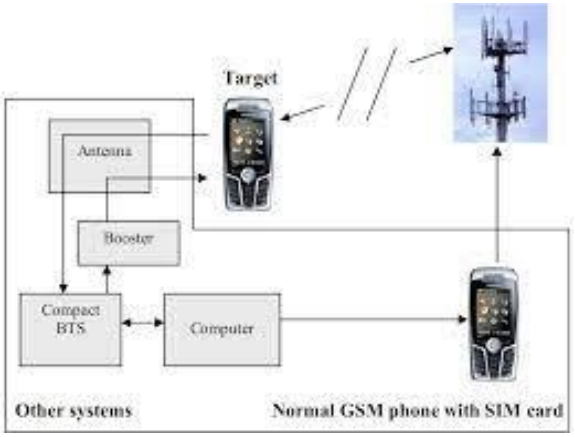
سوال:

در یک شبکه نسل دو می توان با یک دستگاه به نامSys Active GSM، ارتباط کاربران را شنود کرد و حتی به صورت Active در وسط ارتباط قرار گرفت. این سامانه چگونه کار می کند و چگونه GPP3 تلاش کرده است تا جلوی این حمله را بگیرد؟

پاسخ:



GSM over IP System Structure



طبق نظرات مقاله اول، امکان شنود مکالمات کاربران در شبکه نسل دوم (GSM) وجود دارد. دستگاه GSM Active Sys ، برای شنود واستراق سمع در شبکه سنل دوم کاربرد دارد. این دستگاه از ضعف های موجود در پروتکل GSM و رمزنگاری مخفی استفاده شده در این روش ، سود می برد و امکان رهگیری و دستکاری فعال جریان ارتباط را فراهم می نماید.. دستگاه بدین گونه عمل می نماید که سیگنال های GSM frequenciesوGSM Active Sys را دریافت و دیجیتالی

نموده ، و میتواند بدین سان بین دستگاه تلفن همراه و ایستگاه پایه، رهگیری انجام داده و رمزگشایی نماید. همچنین به دلیل آنکه امکان قرار گرفتن در وسط ارتباط با این دستگاه ها فراهم شده است، می تواند سبب شود که توانایی کنترل و اصلاح داده های مبادله شده را داشته باشد.

الگوریتم رمزنگاری A5/1 می آمد سیگنال دیجیتالی را قبل از ارسال با کلیدی رمز می نمود و در مقصد هم با کلید مخفی باز می شد که به دلیل امنیت و قدرت پایین در هردو بخش راحت رمز شکسته می شود . از دلایل اسیب پذیری آن طول نسبتا کوتاه کلید می باشد که از کلید مخفی 64 بیتی استفاده می نماید که تعداد کمی کلید رمزنگاری قابل امکان را فراهم می نماید که مستفد حمله BRUTE-FORCE می باشد و مهاجم میتواند تمام کلید های ممکن را تست وکلید صحیح امتحان شده را در نظر بگیرید.

از دیگر مشکلات آن به تولید اولیه کلید مربوط می باشد که از سه مرحله بازخورد خطی (LSFR) سود می برد که برای ترکیب با متن ساده استفاده می شود. در این سبک کلید نشان داده شده است که initializeکردن می تواند سبب همبستگی و سوگیری در جریان کلید شده و سبب آسان شدن رمزگشایی داده ها شود. بدین سان تکنیک های مختلفی همچون حملات time-memory trade-off attacks (حمله مبادله حافظه زمانی) و rainbow table attacks (حمله جدول رنگین کمانی) برای بازیابی کلید مخفی و رمزگشایی ارتباط ، توسعه یافت.

در جهت جلوگیری از حملات و افزایش امنیت شبکه های GSM ، پروژه نسل سوم 3GPP که وظیفه توسعه استانداردهای GSM را دارد، فعالیت هایی همچون استفاده از الگوهای رمزنگاری قوی تر به جای A5/1، معرفی مکانیسم امنیتی احراز هویت ، تقابل و پروتکل های توافق کلیدی درجهت جلوگیری از دسترسی و رهگیری غیرمجاز را اجرا نمود.همچنین 3GPP چندین روش

امنیتی دیگر را در شبکه نسل دوم GSM در جهت کاهش حملات استراق سمع پیاده سازی نمود که در پایین به توضیح نمونه هایی از آن می پردازیم.

1) الگوهای رمزنگاری پیشرفته تر:

همانطور که در متن اولیه توضیح دادم، تلاش برآن شد که الگوریتم های قویتری برای رمزنگاری پیام ها استفاده نماید.

بدین سان 3GPP الگوریتم ارتقا یافته A5/3 که به نام KASUMI هم شناخته می شود ، معرفی نمود تا جانشین الگوریتم ضعیفتر A5/1 شود. این الگوریتم با بکار گیری کلیدی قوی تر و مکانیزم رمزنگاری پیشرفته تر ، محافظت بالاتری روی پیام انجام می دهد.

2) احراز هویت و توافق کلید:

شبکه های GSM از سیستم احرازهویت و موافقت نامه کلید استفاده می نمایند تا اطمینان حاصل نمایند که دستگاه های مجاز به شبکه دسترسی دارند و کانال ارتباطی میانشان امن است. بدین سان که احراز هویتی متقابل میان دستگاه تلفن همراه و شبکه ، تائید هویت آنها و تولید کلید برای برقراری ارتباطی امن میانشان است.

3) حفاظت از مسیر هوایی:

3GPP اقداماتی را برای ایمن سازی رابطه هوایی بین دستگاه های تلفن همراه و ایستگاه های پایه ارائه کرده است. این شامل محافظت از پیام های سیگنالینگ و داده های صفحه کنترلی است که میان دستکاه ها و شبکه رد و بدل می شود.

بررسی یکپارچگی ، کد احرازهویت پیام و مکانیسم های رمزنگاری برای جلوگیری از تغییرات غیرمجاز یا استراق سمع از این ارتباط استفاده می شود.

4) نظارت بر شبکه ها و تشخیص نفوذ :

اپراتورهای شبکه از سیستم محافظت و نظارت و تشخیص نفوذ برای فعالیت های مشکوک سود می برند. این سیستم ها با نظارت بر ترافیک شبکه، تجزیه و تحلیلی الگو ها و بالا بردن هشدارها هنگام شناسایی ناهنجاری ها به شناسایی و کاهش حملات یاری می رسانند.

5) پروتکل های توافقی کلیدی:

پروتکل هایی برای ایجاد کانال های ارتباطی امن بین دستگاه های تلفن همراه و شبکه معرفی نمود تا تصمینی بر آن باشد که کلید ها در محیطی امن میان طرفین درگیر، رد وبدل شود که مورد توافق قرار میگیرد.

البته این نکته ضروری است که هرچند این ارتقا ها صورت گرفته و درحال افزایش هست ولی هیچ سیستمی را نمی شود کاملا درر برابر حملات مصون دانست.

مقالات رفرنس:

1)

[1101.0552] Eavesdropping on GSM: state-of-affairs (arxiv.org)

2)

(PDF) Eavesdropping On GSM (researchgate.net)