بررسی امنیت شبکه **GSM** و مشکلات آن

وحیده امانی پور
دانشکده برق دانشگاه صنعتی خواجه نصیرالدین طوسی
v_a33@yahoo.com
021-2540643

چکیده:با توجه به استفاده گسترده از سیستم GSM برای شبکه موبایل در کشورهای مختلف از جمله ایران، یکی از مباحث پر اهمیت امنیت این سیستم می باشد. امنیت سیستم خصوصی بودن اطلاعات کاربر را ضمانت کرده و از سو استفاده افراد غیر مجاز جلوگیری می کند. در این میان ضعف های امنیتی شبکه GSM موجب شده که امکان حمله به شبکه وجود داشته باشد. لذا در این مقاله به بررسی امنیت شبکه GSM ومشکلات آن پرداخته شده و در آخر پیشنهاداتی برای بهبود در این رابطه مطرح گردیده است.

کلمات کلیدی: شبکه GSM ، امنیت شبکه، حملات بر ضد امنیت شبکه.

1-مقدمه:

با توجه به افزایش ارتباطات ، شبکه های موبایل روز به روز در حال گسترش است و پیشرفتهای چشمگیری در این باره به وجود آمده است. در این راستا نسل های اول تا چهارم سیستم های موبایل به وجود آمده است. نسل دوم ، GSM (Global System for Mobile communications) ، محبوبترین سیستم تلفن موبایل در جهان است و بر اساس اخبار منتشره تا می 2001 بیش از نیم بلیون تلفن موبایل GSM در بیش از 168 کشور در حال استفاده است . در کشور ما نیز شبکه مورد استفاده بر اساس سیستم GSM است. از طرف دیگر از آنجا که سیستم موبایل از واسط هوايي برای انتقال استفاده می کند و واسط هوايي بسیار آسیب پذیر است، امنیت شبکه اهمیت دو چندانی می یابد. در مقاله حاضر به امنیت شبکه و مشکلات آن می پردازیم.

2-اهداف امنیتی **GSM** :

استفاده از مخابرات راديويي برای انتقال ، GSM را به PLMN (Public Land Mobile Network) تبدیل کرده ومنابع GSM می تواند مورد سواستفاده افراد غیر مجاز قرار گیرد. این افراد سعی می کنند خود را به عنوان مشترک مجاز جعل کنند و به استراق سمع اطلاعات متفاوتی که در مسیر راديويي رد و بدل می شود بپردازند . بنابراین ویژگی های امنیت در GSM PLMN باید برای تحقق بخشیدن به حفاظت از:

1. دسترسی به سرویس های موبایل

2. تمام گزینه های مطرح برای آشکار شدن مسیر رادیوپي بخصوص برای ضمانت خصوصی بودن اطلاعات کاربر پیاده سازی شود .

بنابراین مشخصه های امنیتی متعددی برای حفاظت از امور شخصی مشترک در GSM تعریف می شود که شامل اجـزا زیر است :

- گمنامی : تخصیص (International Mobile Subscriber Identity)IMSI :

گمنامی از ردیابی محل مشترکین موبایل که ممکن است توسط گـوش دادن بـه مبـادلات سـیگنالینگی در مـسیر رادیوپي صورت گیرند ، جلو گیری می کند .

- تصدیق تنها مشترکان ثبت شده:

در این ویژگی اجزا زمینی سیستم ضمانت می کنند که هویت مشترک موجود در طول واسـط هـوائی ، واقعـاً همـان است که در(Subscriber Identity Module) SIM کار گذاشته شده و لذا سیستم مشترک را از جهت پرداخـت هزینـه شناسایي کرده و از شبکه در برابر استفادة غیر مجاز حفاظت می شود . همچنین با از بـین بـردن امکـان جعـل هویـت کاربران مجاز توسط متجاوزان، حفاظت از مشترکان GSMPLMN را ممکن سازد. تصدیق GSM یک پروسة یک طرفه است به طور مثال Visited PLMN شناسایي نمی شود .

روال تصدیق عبارتست از :

1.ایستگاه موبایل ، IMSI را به شبکه می فرستد .

2.شبکه IMSI را دریافت کرده و Ki مطابق با آن را پیدا می کند .

3.شبکه 128 بیت شمارة رندم ، RAND ، را تولید کرده و توسط واسط هوایی به ایستگاه موبایل می فرستد .

4.ایستگاه موبایل با الگوریتم A3 و استفاده از RAND داده شده و Ki موجـود در SIM ، پاسـخ علامـت دار SRES را محاسبه می کند .

5.در همان زمان شبکه با به کارگیری الگوریتم مشابه و ورودی های یکسان SRES را محاسبه می کند .

6.ایستگاه موبایل SRES را به شبکه می فرستد .

7.شبکه SRES را از جهت اعتبار تست می کند یعنی با SRES که خود محاسبه کرده مقایسه کرده و در صورت برابر بودن آن موبایل را تصدیق می کند .

تصدیق بر پایة Ki رمزی که بین(Home Location Register) HLR و SIM مشترک تقسیم شده می باشـد . ایـن Ki هنگامی که SIM کارت شخصی می شود تولید شده و در مکان امنی روی آن نوشته می شود . همچنین یـک کپـی از کلید داخل HLR قرار می گیرد .

- حفاظت از صوت و داده سیگنالینگ در مقابل شنود با استفاده از رمز گذاری:

ارتباط رمز گذاری شده با دستور درخواست حالت رمزگـذاری از GSM آغـاز مـی شـود و بعـد از رسـیدن ایـن دسـتور ایستگاه موبایل شروع به رمزگذاری ورمزگشایي اطلاعات مـی کنـد . هـدف از ایـن کـار حفاظـت از اطلاعـات کـاربر و اطلاعات حساس در کانال سیگنالینگ (مانند شماره تلفن و TMSI) در برابر شنودکنندگان در واسط هوایي است. هـر فریم در ترافیک هوایي به وسیله یک رشته کلید متفاوت رمزگذاری می شود . الگوریتم A5 کـه بـرای رمزگـذاری داده استفاده می شود از کلید رمزگذاری Kc و شمارة فریمی که باید رمز شود استفاده می کند و لـذا بـرای هـر فـریم یـک رشته کلید متفاوت تولید می شود .

- استفاده از SIM به عنوان ماژول امنیتی:

SIM در یک کارت هوشمند پیاده سازی می شود .کارت هوشمند مانند یک میکرو کامپیوتر اسـت کـه دارای CPU ، حافظه و سیستم عامل است . به کمک برنامه ریزی حافظه rom ، کارت هوشـمند مـی توانـد اطلاعـات حـساس را بـا

بالاترین سطح امنیت در خود ذخیره کند . لذا این روش خوبی برای ذخیره TMSI, Ki و دیگر اطلاعات حساس کاربر است .

- غیر قابل استفاده بودن تلفن های موبایل بدون SIM
- عدم اجازة کپی کردن SIM در شبکه
- ذخیره مطمئن Ki
- ویژگی GSM در استفاده از سه تایي ها

3-الگوریتم ها :

3-1- A3 الگوریتم تصدیق ایستگاه موبایل :

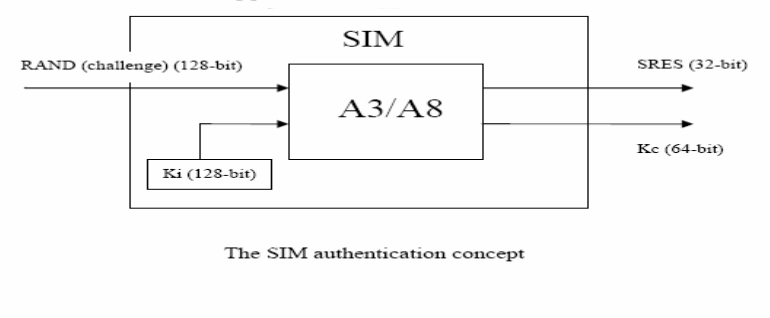
در مدل امنیتي GSM، A3 الگوریتم تصدیق است. الگوریتم A3 ، RAND را از(Mobile services Switching Center) MSC و کلید محرمانه Ki را از SIM به عنوان ورودی گرفته و 32 بیت به عنوان خروجی تولید می کند که همان پاسخ علامت دار SRES است . RAND و Ki هر دو 128 بیت طول دارند .

الگوریتم A3 را به عنوان یک تابع یک طرفه درهم (one_way hash functin) می توان در نظر گرفت . عموماً توابع یک طرفه درهم با گرفتن یک ورودی تصادفی ، یک خروجی با طول ثابت تولید می کنند . توابع درهم یک طرفه امن طوری طراحی می شوند که از نظر محاسباتی تعیین ورودی که مقدار درهم را می دهد و یا تعیین دو ورودی منحصر به فرد که منجر به دو مقدار یکسان می شود ، غیر ممکن است .

3-2- A8 الگوریتم تولید کلید رمز گذاري :

الگوریتم A8 ، الگوریتم تولید کلید فصلی در مدل امنیتی GSM است. الگوریتم A8 دو ورودی 128 بیتیRAND,Ki دارد و یک خروجی 64 بیتی تولید می کند. این خروجی کلید فصلی 64 بیتی Kc است .

هر دو الگوریتم A3 و A8 در SIM ذخیره می شود تا مانع دست زدن و خراب کردن آنها توسط افراد گردد.(شکل1) این امر موجب می شود که کارگزار بتواند مستقل از سازندگان سخت افزار و سایر کارگزاران شبکه تصمیم بگیرد که از کدام الگوریتم استفاده کند.



شکل1-الگوریتمA3/A8

3-3- الگوریتم **COMP128** :

تقریباً اکثر کارگزاران GSM در جهان از یک الگوریتم به نام COMP128 به جای الگوریتم های A3, A8 استفاده می کنند. COMP128 یک الگوریتم مرجع برای وظایفی است که توسط کنسرسیوم GSM به آن اشاره شده است.

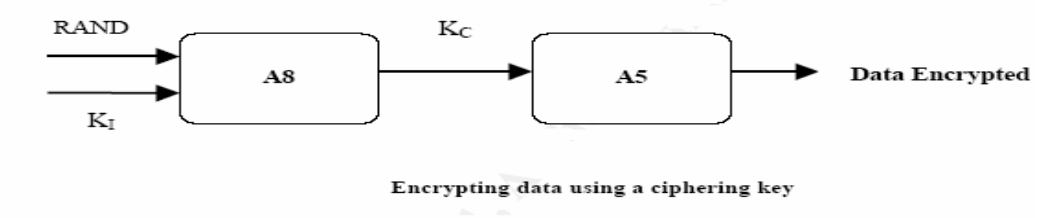
الگوریتم های دیگری نام برده شده ولی تقریبا تمام کـارگزاران بـه جـز دو اسـتثنا از COMP128 اسـتفاده مـی کننـد. COMP128 ، RAND و Ki را به عنوان ورودی گرفته و به جای 32 بیت SRES ، 128 بیت خروجی تولید مـی کنـد. 32 بیت اول از 128 بیت، پاسخ SRES را تشکیل می دهد. 64 بیت باقی مانده Kc را تـشکیل مـی دهـد. از ایـن 64 بیت 10 بیت انتهایی صفر است، لذا عملاً فضاي کلید Kc از 64 بیت به 54 بیت کاهش یافته است.

A5-4-3 الگوریتم رمز گذاری :

در حال حاضر سه امکان مختلف A5/0 (غیر رمزگذاری شده)، A5/1 ، A5/2 ، A5/3 در GSM برای امـن کـردن داده وجود دارد.به طور کلی الگوریتم های A5 بعد از A5/1 به صورت A5/X نامگذاری شده اند. اکثر الگـوریتم هـای A5/X خیلی ضعیف تر از A5/1 هستند. A5/1 دارای پیچیدگی زمانی بیش از 2^54 است. یک تخمـین از پیچیـدگی زمـانی A5/2 کمتر از 2^16 است.

الگوریتم های سری A5 درون ایستگاه پایه و ME مي باشند و درون SIM نیست زیرا آنها باید بـه انـدازه کـافی سـریع باشند و بنابراین سخت افزاری هستند.

رمز گذاری با Kc و شماره فریمي که رمزگذاری یا رمزگشایی می شود آغاز می گـردد.(شـکل2) Kc یکـسانی در طـول مکالمه استفاده می شود، اما 32 بیت شماره فریم در طول مکالمه تغییر می کند، بنابر این یک رشته کلید منحصر بـه فرد برای هر فریم تولید می شود .الگـوریتم A5/1 از سـه LSFR (Linear Shift Feedback Register) بـا طـول هـای متفاوت تشکیل شده است. LSFR ثباتی است که یک بیت خروجی را بر پایهٔ حالت قبلش و یک چند جمله ای فیدبک تولید می کند. طول مجموع LSFR ها 64 بیت است. خروجی این سه LSFR با هم XOR شده و یـک بیـت را تولیـد می کند. هر سه LSFR با کلید فصلی و شماره فریم آغازسازی می شود.



شکل2-الگوریتم A5

4- مشکلات امنیت **GSM** :

4-1- محدودیت ها و مسائل امنیت **GSM** :

- امنیت توسط ابهام : این به معنای آن است که تمام الگـوریتم هـایی کـه اسـتفاده مـی شـود بـرای عمـوم در دسترس نیست. اکثر تحلیلگران امنیت اعتقاد دارند که هر سیستمی که بـه عنـوان موضـوعی بـرای بررسـی و موشکافی بهترین مغزهای جهان نباشد ، نمی تواند امن باشد.
- تنها دسترسی امن را فراهم می کند . تمام ارتباطات بین ایـستگاه موبایـل وBTS(Base Transceiver Station) رمزگذاری می شود ولی تمام ارتباطات و سـیگنالینگ بـه طـور عمـومی بـه صـورت متنـی واضـح و آشـکار در قسمتهای ثابت شبکه انتقال داده می شود.
- بهبود بخشیدن مکانیزم های رمزگذاری مشکل است.
- دید کاربر کم است (به طور مثال نمی داند رمزگذاری شده است یا نه)
- نقص الگوریتم ها

2-4- بعضی از انواع حملات ممکن :

4-2-1- حمله **Brute-Force** بر ضد **A5** :

یک حمله brute-force زمان واقعی بر ضد امنیت سیستم GSM عملی نیست . پیچیدگی زمانی حمله 2^54 (2^64 وقتی که 10 بیت صفر نباشند) است. این احتیاج به زمان زیادی براي عملی شدن شنود مکالمات GSM به صورت زمان واقعي دارد. با این وجود می توان فریم ها را بین (Mobile station) MS و BTS ضبط کرد و سپس حمله را عملی کرد.

4-2-2- حمله **Divide-and-Conqur** بر ضد **A5** :

حمله Divide-and-Conqur برای کاهش پیچیدگی از 2^54 در حمله brute-force به 2^45 به کار می رود که تغییر نسبتاً چشم گیری است (2^9=512 برابر سریع تر). حمله Divide-and-Conqur بر پایه حمله با متن ساده معلوم می باشد. حمله کننده احتیاج دارند که 64 بیت از متن رمز و متن ساده متناظر را بداند. این شدیداً وابسته به فرمت فریم های GSM که فرستاده و دریافت می شود دارد. فریم های GSM حاوی اطلاعات ثابت زیادی هستند. 64 بیت مورد احتیاج شاید همیشه شناخته شده نباشد، اما 32 تا 48 بیت معمولاً شناخته شده اند، بعضی مواقع نیز بیشتر.به طور خلاصه حمله Divide-and-Conqur بر اساس حدس زدن محتوای دو LSFR کوچک و محاسبه کردن سومین LSFR از روی key stream معلوم انجام می شود. اگر کلاک دو رجیستر اول وابسته به رجیستر سوم نباشد، این 2^40 حمله است. اما این وابستگی پیچیدگی را از 2^40 به 2^45 افزایش می دهد.

به هر حال J.Golic حمله Divide-and-Conqur دیگری را مطرح کرد که بر پایه فرضیات مشابه قرار گرفته و به طور میانگین 2^40 پیچیدگی زمانی دارد.

4-2-3- دسترسی به شبکه سیگنالینگ :

در بالا مشخص شد که الگوریتم A5 از نظر رمز گذاری امن نیست.متاسفانه امواج هوائی بین MS و BTS تنها نقطه ضعف سیستم GSM نیست. از آنجایی که تنها انتقالات بین MS و BTS رمز گذاری می شود بعد از BTS ترافیک درون شبکه کارگزار با متن ساده انتقال می یابد. اگر حمله کننده به شبکه سیگنالینگ کارگزار دسترسی پیدا کند می تواند به تمام چیزهايي که انتقال می یابد شامل فراخوانی تلفن فعلی، KC, SRES, RAND گوش دهد. شبکه سیگنالینگ (SS7(Signaling System No.7 که در شبکه GSM کارگزار استفاده می شود اگر حمله کننده دسترسی مستقیم به آن پیدا کند کاملاً ناامن است. در سناریوی دیگر، حمله کننده می تواند به HLR یک شبکه مشخص حمله کند. اگر حمله کننده به HLR دسترسی پیدا کند می تواند Ki های تمام مشترکان آن شبکه بخصوص را بدست آورد. خوشبختانه HLR اندکی امن تر از سایر قسمت های شبکه است. بنا براین احتمال بسیار کمی دارد که نقطه ورود باشد.

دسترسی به سیگنالینگ شبکه زیاد مشکل نیست، با وجود این که BTS ها معمولاً به(BSC (Base Station Controller در طول کابل متصل اند بعضی از آنها به BSC با لینک مایکروویو وحتی لینک ماهواره ای متصل اند. این لینک با تجهیزات مناسب دسترسي نسبتاً آسانی دارند. اکثر تجهیزات موجود در بازار برای شنود GSM به نظر می رسد که از این نقطه ضعف استفاده می کنند.لینک مایکروویو می تواند رمز گذاری شود. به هر حال به سازندگان سخت افزار وابسته است و تا حدودی مانیتور آن را مشکلتر می کند.

امکان دسترسی به کابلی که BTS را ترک می کند نباید مستثنی کرد. این یک خطر واقعی است و اگر حمله با دقت انجام شود می تواند برای مدت زیادی ناشناخته بماند. امکان استراق سمع داده انتقال یافته بین BTS و BSC این

توانایی را به حمله کننده می دهد که هم فراخوانی را زیر نظر بگیرد و فراخوانی در هوا را ره گیـری کـرده و آن را رمـز گشایی کند. حال که او Kc را می داند رمزگشائی زمان واقعی مشکلی نیست.
یک رویکرد دیگر از طریق مهندسی اجتماعی است. این رویکرد نباید دست کم گرفته شـود هرچنـد بـه نظـر مـضحک بیاید. حمله کننده ممکن است خود را به شکل تعمیر کار یا مانند آن در بیاورد و وارد یـک سـاختمان مناسـب شـود و شنود کند. همچنین ممکن است به یک مهندس رشوه دهد تا این کار را برای او انجام دهد یا به او تمام Ki های تمام مشترکان یک کارگزار خاص را بدهد. این امکان بی حد و اندازه واقعی است.

4-2-3-1-لینک مایکروویو :

این حقیقت که لینک بین BS و BSC در بسیاری حالات لینک مایکروویو نقطه به نقطه اسـت یـک شـکاف آشـکار در امنیت GSM است. این لینک می تواند شنود شود زیرا داده در اینجا بدون رمز گذاری است. در زمـان طراحـی GSM انتظار بر این بود که لینک بین BS و BSC لینک های ثابتی است لذا رمز گذاری لازم نبود.

4-2-4-به دست آوردن کلید از **SIM** :

امنیت تمام مدل امنیتی GSM بر پایه Ki محرمانه است. اگر این کلید بي اعتبار شود تمام حساب ها بـی اعتبـار مـی شوند. هنگامی که حمله کننده بتواند Ki را بدست آورد نه تنها می تواند به تلفنهای مشترک گوش دهد بلکه می تواند به جای آن تلفن کند و هزینه به حساب مشترک اصلی گذاشته شود، زیرا او می تواند خود را مشترک مجاز جا بزند.اگر دو تلفن با شناسه یکسان در یک زمان روشن شود شبکه GSM به آن توجه کرده و یک سوال موقعیت از تلفن ها مـی کند. اگر که تلفن های یکسان در دو موقعیت متفاوت در یک زمان باشند، حساب آنهـا را مـی بنـدد بنـابراین از تلفـن کردن حمله کننده و مشترک مجاز جلوگیری می کند. اما اگر حمله کننده تنها علاقه داشته باشد کـه بـه تلفـن هـای مشترک گوش دهد این شیوه مناسب نیست. در این حالت حمله کننده می تواند غیر فعال بماند و تنهـا بـه تلفـن هـا گوش دهد. بنابر این برای شبکه GSM غیر قابل مشاهده می ماند.
هنگامی که فراخوانی انجام نمی شود می توان SIM را از ME جدا کرد و داخل ME دیگری گذاشت که ارتباط قبلی با آن نداشته. از آنجا که واسط SIM/ME غیر حفاظت شده است می توان SIM را به یک شبیه ساز ترمینال به جای یک ME حقیقی متصل کرد و در نتیجه پیام های بین واسط SIM/ME را استراق سمع کرد.
در آوریـل 1998 انجمـن توسـعه کارتهـای هوشـمند (SDA:Smartcard Developer Association) همـراه بـا دو پژوهشگر دانشگاه برکلی ادعا کردند که الگوریتم COMP128 ذخیره شده در SIM را شکستند. حمله آنها بر پایه حمله با چالش انتخابی قرار داشت آنها با ارسال تعداد زیادی (حدود 150 هـزار) از شـماره هـای RAND بـه مـاژول مجـاز توانـستند Ki را در عـرض چنـدین سـاعت (8 سـاعت) پیـدا کننـد. SIM در طـول یـک خواننـده کـارت هـای هوشمند(Smartcard Reader) متصل شده به یک PC در دسترس بود. Ki از SRES با آنالیز رمـز گـزاری تخمـین زده شد. خواننده کارتهای هوشمند 6/25 سوال در هر ثانیه از simcard می کرد. بنابر این حملـه کننـده نیـاز دارد کـه بـه SIM اصلی حداقل برای 8 ساعت دسترسی فیزیکی داشته باشد که به نظر غیر منطقی می آید. همچنـین آنهـا کـشف کردند که Kc تنها 54 بیت از 64 بیت را استفاده می کند و 10 بیت باقی مانده با 0 جایگزین می شـود کـه ایـن امـر کلید رمزگذاری را واقعاً ضعیف تر می کند.
دوباره این ضعف در سناریوی مهندسی اجتماعی قابل اجرا است. فردی که می توان آن را یـک فروشـنده فاسـد GSM فرض کرد می تواند به این شیوه SIM را شبیه سازی کند و سپس کارت های مشابه سازی شده را به فـرد سـومی کـه می خواهد نا شناخته بماند و نمی خواهد SIM مجاز بخرد، بفروشد. همچنین می تواند SIM مشابه سازی شـده را بـه شخص معلومی بفروشد که می خواهد تلفن های مورد نظر را شنود کند. یک کارمنـد فاسـد نیـز مـی توانـد Simcard

قربانی را در اختیار حمله کننده قرار دهد. بنابر این حمله کننده می تواند SIM را مشابه سازی کند وبعداً به تلفن های مالک آن گوش دهد. تمام این سناریو ها واقع بینانه است. ضعف پیدا شده در الگوریتم COMP128 تمام مدل امنیتی سیستم GSM را بی اعتبار می کند و بنابر این مشترکان را در یک فضای باز بدون هیچ امنیتی قرار می دهد.

4-2-5-به دست آوردن کلید از **SIM** از روی هوا :

محققان SDA و ISAAC مطمئن هستند که حمله مشابه سازی SIM یکسانی می توانند در هوا نیز اجرا شود. آنها همچنین ادعا کردند که از نظر تکنولوژی امکان ساخت ایستگاه پایه جعلی وجود دارد. این اجازه حمله man-in-the-middle را می دهد. اساساً ایستگاه پایه جعلی می تواند ایستگاه واقعی را بپوشاند و ایستگاه موبایل را مجبور کند با آن ارتباط برقرار کند.

4-2-6-به دست آوردن کلید از **AuC** :

حمله مشابه که برای بدست آوردنKi ازSimcard به کار می رود برای بدست آوردنKi از(Authentication Center) AuCبه کار می رود. AuC باید به درخواست های شبکه GSM پاسخ دهد و سه تایی های با ارزشی که در تصدیق MS استفاده می شود را به شبکه بدهد. این روال با روالی که برای دسترسی MS به Simcard استفاده می شود اساساً یکسان است. تفاوت در این است که AuC بسیار سریعتر از Simcard درخواستها را پردازش می کند زیرا باید درخواست های بسیار بیشتری را در مقایسه با یک Simcard پردازش کند. امنیت AuC در اینکه آیا حمله امکانپذیر است یانه نقش بزرگی را بازي می کند.

4-2-7-حملات پارتیشنینگ :

در می 2002 تیم تحقیقات IBM علی رغم محافظت های موجود روش جدیدی برای استخراج سریعتر کلیدهای COMP128 داخل Simcard با استفاده از کانالهای کناری کشف کردند. الگوریتم COMP128 احتیاج به مراجعه کردن به جدول های بزرگی دارد که می تواند موجب شود روی وسیله ساده ای مانند Simcard اطلاعات حساس زیادی به کانال های کناری رخنه کند. یک هکر که مالکیت یک Simcard را برای چند دقیقه دارد می تواند به آسانی تمام کلید 128 بیتی را بیرون بکشد.

5- بهبود های ممکن :

امنیت در برخی مناطق با تمهیدات نسبتاً ساده ای می تواند بهبود پیدا کند.کارگزار می تواند از یک الگوریتم امن رمز نویسی دیگر به جای A3 استفاده کند. این احتیاج به توزیع Simcard های جدید به تمام مشترکان و تجدید نرم افزار HLR دارد. این به طور موثری حمله کننده را از مشابه سازی Simcard ها (خطرناک ترین حمله) ناتوان می کند. این راه حل به آسانی اجرا می شود زیرا کارگزار شبکه می تواند خودش تغییرات را اجام دهد و احتیاج به پشتیبانی سازندگان سخت افزار یا نرم افزار و یا کنسرسیوم GSM ندارد. در حال حاضر یک الگوریتم جدید به نام COMP128-2 در دسترس است.

راه حل دیگر یک تحقق جدید A5 با رمز گذاری جدید است تا بتواند حمله BRUTE-FORCE را در هر حالت ناممکن سازد. الگوریتم جدید A5/3 برای جایگزینی با الگوریتم قدیمی A5/2 مورد توافق قرار گرفته است. این بهبود احتیاج به مساعدت و همکاری کنسرسیوم GSM و تولید کنندگان سخت افزار و نرم افزار دارد زیرا آنها باید ورژن جدیدی از سخت افزار و نرم افزار هایي که الگوریتم جدید را در بر دارند عرضه کنند.

راه حل سوم رمز گذاری ترافیک در شبکه زیرساخت کارگزار بین مولفه های شبکه است، این حمله کننـده را از شـنود شبکه زیرساخت ناتوان می سازد. این راه حل احتمالاً مـی توانـد بـدون همکـاری کنـسرسیوم GSM اجـرا شـود ولـي همچنان به مساعدت تولید کنندگان سخت افزار احتیاج دارد.

در جمع هیچکدام از بهبود هاي بالا برای اجرا زیاد سخت نیست. آنها هزینه های جدیدی را به کارگزار شـبکه تحمیـل می کنند که از نقطه نظر کارگزار شبکه جذاب نیست. بنابر این این بهبود ها تا موقعی که عموم از نا امنی شـبکه هـای GSM اطلاع پیدا نکنند و کارگزاران شبکه مجبور شوند امنیت شبکه را بهبود دهند، احتمالاً تحقق نخواهند یافت. هـر سه این بهبود ها براي امن کردن شبکه در مقابل تمام حملات که به آن آشنا شدید لازم است.

6-نتیجه گیری و پیشنهادات:

همانطور که در مقاله دیدیم ، با توجه به ضعفهای امنیتی شبکه GSM ، امکان طرح حملات مختلف بر ضد آن وجود دارد، لذا باید این ضعفها و مشکلات امنیتی بر طرف شود. البته در حال حاضر از آنجا که عموم از نا امنی شبکه اطلاع ندارند، کارگزاران شبکه در این زمینه هزینه ای نمی کنند. اما با گذشت زمان مشکلات خود را بیشتر نشان داده و روشهای جدیدتری برای حمله به شبکه مطرح خواهد شد. بنابراین پیشنهاد می شود به بررسی دقیق تر مشکلات امنیتی شبکه GSM پرداخته و راهکارهای جدیدتر وموثرتری برای بهبود ارائه شود.

7-فهرست مراجع وماخذ:

[1] مهرترا آشا ، مهندسی سیستمهای موبایل ، ترجمه جهانگیر دادخواه چیمه ، مرکز انتشارات دانشگاه علم و صنعت ایران ، تهران ،1381 .

[2] Redl Siegmund M. & Weber Matthias K. & Oliphant Malcolm W. ,An Introduction to GSM, ArtechHouse, Boston ,1995 .

[3] Mark Briceno , Ian Goldberg and David Wagner . see http://www.isaac.cs.berkeley.edu/isaac/gsm_faq.html

[4] Josyula R. Rao, Pankaj Rohatgi , Helmut Scherzer and Stefan Tinguely, Partitioning Attacks : Or How to rapidly clone some GSM card ,IEEE Symposium on Security and Privacy , Oakland , May 2002.

[5] Helena Handschuh and Pascal Paillier , Reducing the Collision Probability of Alleged Comp128 , http://www.gemplus.com/smart/r_d/publication/pdf/HP00comp.pdf , 2000 .

[6] Lauri Pesonen , GSM Inteception , http://www.dia.unisa.it/ads.ir/Corso_security/www/ORSO-9900/a5/Netsec/NETSEC.HTML , Novamber 1999

[7] Yong LI,Yin CHENG and Tie_Jun MA , Security in GSM , http://www.gsm_security.net/papers/securityingsm.pdf

[8] David Wagner, GSM Cloning , http://www.isaac.cs.berkeley.edu/isaac/gsm.html

[9] The GSM standard (An Overview of Security) , http://www.sans.org/rr/papers/58/317.pdf , SANS Institute 2001 .

[10] Paulo S. Pagliusi , A Contemporary Forward on GSM Security , http://www.isg.rhul.ac.uk , 2002 .

[11] Moe Rahnema , Overview of the GSM System and Protocol Architecture , IEEE Communications Magazine , April 1993 .