بررسی آسیب‌پذیری‌های امنیتی USSD

محسن تورانی

toorani@ieee.org

چکیده: GSM، پرکاربردترین شبکه تلفن همراه در جهان است. داده سرویس تکمیلی ساخت نیافته (USSD)، یک سرویس انتقال داده در GSM است که برای انتقال متن بین یک کاربر و برنامه مورد استفاده قرار می‌گیرد. USSD، یک سرویس نشست گرا است و این امکان را برای مشترکین فراهم می‌آورد تا بتوانند رده سرویسهایشان را تغییر دهند، سرویسهای پیشرفته را از اپراتور تقاضا نمایند یا یک دستور پرداخت را با استفاده از تلفن همراهشان به انجام رسانند. از آنجا که USSD یکی از سرویسهای مورد استفاده در تجارت سیار است و از آنجا که نگرانیهای امنیتی مهمترین مانع در توسعه تجارت و پرداختهای سیار بوده است، بررسی آسیب‌پذیریهای امنیتی این سرویس، امری ضروری است. در این مقاله، به معرفی اجمالی USSD و بررسی آسیپ‌پذیریهای امنیتی آن می‌پردازیم.

واژه های کلیدی: USSD، امنیت تلفن همراه، GSM، تجارت سیار، آسیب‌پذیریهای امنیتی.

۱- مقدمه

استفاده از تلفن همراه در میان جوامع بشری با رشد و استقبال روز افزونی مواجه شده است. در انتهای سال ۲۰۰۷، تعداد مشترکین تلفن همراه در جهان از مرز ۳/۳۳ میلیارد نفر گذشت که از این میان، ۲/۸۸ میلیارد نفر مشترکین شبکه GSM[1] (با احتساب نسخ ارتقا یافته‌اش) بوده‌اند. این در حالی است که تعداد مشترکین UMTS[2] فقط ۱۹۶ میلیون نفر بوده است [۱]. بسته به اینکه چه کانالی برای عرضه محصولات و خدمات در شبکه تلفن همراه مورد استفاده قرار می‌گیرد، ملاحظات امنیتی و تجاری متفاوتی برای برنامه‌های کاربردی لازم است. USSD[3] یک سرویس GSM است که می‌تواند برای ارسال متن بین یک کاربر و یک برنامه مورد استفاده قرار گیرد و مشخصات آن در [۲] بیان شده است. USSD یک سرویس نشست گرا است و همانند SMS[4] مبتنی بر قابلیتهای GSM در انتقال اطلاعات بر روی کانال سیگنالینگ است. USSD یکی از مسیرهای دسترسی در خدمات تجارت سیار است و از نظر اقبال و استفاده عمومی در رتبه دوم (پس از SMS) قرار دارد [۳]. USSD همچنین کاربرد ویژه‌ای در خدمات ارزش افزوده و خدمات پیش پرداخت[5] GSM دارد. با این وجود، این سرویس با مشکلات امنیتی متعددی مواجه است که این موضوع در این مقاله مورد توجه قرار خواهد گرفت.

۲- مروری بر USSD

USSD یک سرویس ارائه شده توسط GSM است؛ بدین معنا که سایر شبکه‌های تلفن همراه غیر GSM، USSD را پشتیبانی نمی‌کنند. USSD یک سرویس نشست گرا است و برخلاف SMS، مبتنی بر ویژگی ذخیره و ارسال نمی‌باشد. این امر، USSD را به مراتب ساده‌تر و سریعتر از SMS می‌سازد. اما به دلیل آنکه USSD خصوصیت ذخیره و ارسال را ندارد، اگر پوشش شبکه از بین برود، تعامل با کاربر قطع خواهد شد. USSD همچنین دارای قابلیت تلاش مجدد برای ارسال نمی‌باشد، ضمن آنکه تضمینی نیز برای تحویل پیام ارائه نمی‌دهد اما اگر اشکالی پیش بیاید، به فرستنده گزارش خواهد شد. اصلی ترین مزیت USSD آن است که اجازه ارتباط خیلی سریع بین کاربر و کاربرد را ممکن می‌سازد. بسیاری از کاربردهایی که توسط USSD امکان پذیر شده‌اند، مبتنی بر منو می‌باشند و مشتمل بر خدماتی نظیر پیش پرداخت سیار و چت می‌باشند. هیچ منوی خاصی در تلفن برای دریافت یا ارسال USSD لازم نیست و کاربر می‌تواند مستقیما از صفحه اولیه تلفن، دستورات USSD را وارد کند. USSD بر خلاف SMS، ارتباط بین تلفن همراه با تلفن همراه را فراهم نمی‌آورد.

سرویس USSD در GSM از طریق دروازه USSD[6] فراهم می‌آید. این دروازه، پیامهای USSD را از شبکه سیگنالینگ به کاربردهای خدماتی و بالعکس هدایت می‌کند. یکی از ویژگیهایی که دروازه USSD را از سایر انواع دروازه متمایز می‌نماید، آن است که دروازه USSD می‌بایست بداند که هر نشست متعلق به کدام کاربر است. کاربران برای دسترسی به سرویسهای USSD احتیاج به دسترسی به یک گوشی با منوی خاص ندارند و می‌توانند فرامین USSD را مستقیماً از صفحه اصلی گوشی موبایل خود

[1] Global System for Mobile Communications

[2] Universal Mobile Telecommunications System

[3] Unstructured Supplementary Service Data

[4] Short Message Service

[5] Pre-paid

[6] USSD Gateway

مجموعه مقالات کنفرانس بین المللی شهروند الکترونیک و تلفن همراه (International Conference on eCitizen & Cell phone 2010)، تهران، ۱۳۸۹.
http://www.civilica.com/Paper-ICECC01-ICECC01_058.html

وارد نمایند. فرامین USSD به HLR[1] شبکه خانگی کاربر ارسال خواهند شد. بدین ترتیب کاربران خواهند توانست در زمان رومینگ نیز مانند زمانی که در شبکه خانگی خود به سر می‌برند، از خدمات مبتنی بر USSD استفاده کنند. USSD بر روی تمام گوشیهای GSM موجود کار می‌کند. هم STK[2] و هم WAP[3]، USSD را پشتیبانی می‌نمایند. البته با وجود آنکه USSD در تئوری می‌تواند با STK کار کند و حتی ETSI نیز یک توصیه برای نحوه استفاده از آن دارد، اما عملا انواع کمی از گوشیها از آن پشتیبانی می‌کنند. نکته دیگر آنکه هنوز برخی اپراتورها، قابلیت محاسبه هزینه خدمات USSD را ندارند.

USSD در عمل، برای مبادله پیامهای متنی بین یک کاربر و برنامه مورد استفاده قرار می‌گیرد. USSD را بیشتر باید به عنوان یک عامل تصور نمود تا یک کاربرد، چرا که این USSD است که سایر کاربردها را قادر به فعالیت می‌سازد. USSD یک روش ایده‌آل برای مشترکین فراهم می‌آورد تا بدان وسیله بتوانند رده سرویسهایشان را تغییر دهند، سرویسهای پیشرفته را تقاضا نمایند یا یک دستور پرداخت را با استفاده از تلفن همراهشان به انجام رسانند. USSD همچنین می‌تواند به عنوان حامل WAP، در خدمات مبتنی بر منو نظیر اخبار، وضعیت هوا و قیمت سهام، خدمات محتوایی مبتنی بر موقعیت و کاربردهای مبتنی بر SAT[4] مورد استفاده قرار گیرد. برای دست یافتن به این مهم، ترتیب عملیات از این قرار است:

- مشترک یک پیام USSD آغاز شونده از موبایل می‌فرستد.
- پیام USSD مطابق توصیه‌های GSM به HLR شبکه خانگی مشترک هدایت می‌شود.
- HLR، پیام USSD را به دروازه USSD هدایت می‌کند.
- دروازه USSD، پیام را با استفاده از TCP/IP که برای یکپارچه سازی با سکوهای[5] کامپیوتری تجاری مناسب‌تر است، به کاربردهای بیرونی مخابره می‌نماید.
- سیستم بیرونی پیام را تفسیر می‌نماید و عمل مقتضی را که در پیام به آن اشاره شده، به انجام می‌رساند.
- در طی زمان وقفه، سیستم بیرونی، دریافت موفقیت آمیز پیام را از طریق دروازه USSD به موبایل اعلام وصول می‌نماید. سیستم بیرونی بعداً به طور غیرهمزمان می‌تواند اطلاعات اضافی را (مثلا از طریق یک SMS) برای مشترک موبایل ارسال دارد.

یک ارتباط USSD به دو صورت برقرار می‌شود: در صورت اول، کاربر نشست را آغاز می‌کند که چنین قابلیتی بر روی همه تلفنهای همراه GSM وجود دارد. در صورت دوم، یک برنامه ارتباط را با تلفن همراه آغاز می‌کند که این قابلیت در اکثر گوشیها پیاده‌سازی شده، ولی عملکرد بسیار متفاوتی در انواع مختلف دارد. فاز یک USSD که در GSM 02.90 توصیف شده، فقط عملیات آغاز شونده از گوشی را پشتیبانی می‌کند (عملیات Pull). فاز دوم USSD که در GSM 03.90 مشخص شده، عملیات آغاز شونده از شبکه را نیز پشتیبانی می‌نماید (عملیات Pull و Push)، ضمن آنکه از عملیات منویی نیز پشتیبانی می‌نماید. خدمات فاز ۱ و ۲ USSD می‌توانند به طور همزمان با تماس تلفنی[6] و یا مستقل از تماس تلفنی[7] باشند که در حالت اول از کانال FACCH[8] و در حالت دوم از کانال SDCCH[9] استفاده می‌شود. پیامهای USSD مبتنی بر تماس، برای استفاده در کاربردهای تجاری چندان جالب به نظر نمی‌رسند چرا که به ندرت پیش می‌آید که کاربر در ضمن تماس تلفنی به استفاده از USSD بپردازد. با این وجود، احتمال آنکه کاربر در حین تماس یک پیام USSD را از شبکه دریافت دارد، وجود دارد.

پیامهای USSD هم از نظر طول و هم از نظر محتوا بسیار انعطاف پذیر می‌باشند. USSD از ارقام 9-0 و کلیدهای * و # استفاده می‌نماید. کدهای دسترسی به سرویس و نام سرویسها از طریق برنامه ریزی هوایی بر روی گوشیها قابل دانلود می‌باشند. این امر کار را برای کاربران تازه وارد راحت‌تر خواهد کرد. وارد کردن یک رشته عددی برای کاربر بسیار ساده‌تر از شکل‌دهی یک پیام کوتاه است. رشته‌ها ممکن است تحت کلیدهای شماره‌گیری کوتاه، بر روی گوشی ذخیره شده باشند. طول پیامهای USSD می‌تواند تا ۱۸۲ کاراکتر باشد که حد بیان شده وابسته به لایه پروتکل مورد استفاده قرار گرفته است. نرخ داده کانال FACCH حدود ۱۴۰ بایت در ثانیه است در حالی که نرخ داده کانال SDCCH حدود ۸۳ بایت در ثانیه است. بنابراین هر پیام USSD در زیر دو ثانیه قابل ارسال است. پس از وارد نمودن کد USSD بر روی گوشی، پاسخ اپراتور GSM پس از چند ثانیه بر روی گوشی نمایان خواهد شد.

---

[1] Home Location Register

[2] SIM Toolkit

[3] Wireless Application Protocol

[4] SIM Application Toolkit

[5] Platforms

[6] Call Related USSD Service

[7] Call Independent USSD Service

[8] Fast Associated Control Channel

[9] Stand Alone Dedicated Control Channel

USSD یک واسط TCP/IP ساده برای کاربردهای خارجی که چیزی از شبکه SS7 نمی‌دانند، ارائه می‌دهد. مسیریابی کاربردها با استفاده از یک کد سرویس ساده – که در پیام USSD لحاظ می‌شود – انجام می‌شود. تفسیر کد سرویس توسط پیکربندی دروازه USSD و توسط اقدامات کاربرد خارجی مرتبط با آن کد سرویس انجام می‌شود. کاربردهای خارجی می‌توانند بر روی هر ماشینی که به یک شبکه TCP/IP دسترسی داشته باشد موجود باشند.

۳- مشکلات امنیتی USSD

همانگونه که در قسمت قبل به آن اشاره شد، USSD یک تکنولوژی مفید و پر استفاده در GSM است. با این وجود USSD به اندازه‌ای امن نیست که به عنوان حاملی امن برای تراکنش‌های مالی مورد استفاده قرار گیرد. در کل مشکلات امنیتی USSD را می‌توان به دو دسته تقسیم نمود:

۱- مشکلات امنیتی که USSD به عنوان یک روش انتقال داده در GSM, از شبکه سیار مورد استفاده به ارث برده است. این قبیل مشکلات امنیتی به تمام روشهای انتقال داده‌ای که از GSM استفاده می‌نمایند، سرایت خواهد نمود که این موضوع در بخش (۳-۱) مورد توجه قرار خواهد گرفت.

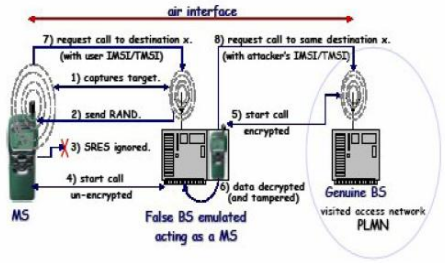
۲- تعدادی آسیب‌پذیری اضافه خاص USSD که در بخش (۳-۲) به آن اشاره خواهد شد.

۳-۱- مشکلات امنیتی مشترک با سایر سرویسها

همانگونه که بیان شد، USSD یک سرویس فراهم آمده توسط GSM است و در بسیاری از شبکه‌های سیار، چنین قابلیتی وجود ندارد. علیرغم آنکه GSM با هدف ایجاد یک سیستم سیار امن طراحی شده و احراز اصالت کاربر و رمزنگاری مبادلات هوایی را مدنظر قرار داده بود، در برابر بسیاری از حملات که هر کدام بخشی از شبکه را هدف قرار می‌دهند, به شدت آسیب پذیر است. محرمانگی پیام، جامعیت[1]، احراز اصالت، عدم انکار[2]، کنترل دسترسی[3] و در دسترس بودن[4] از مهمترین سرویس‌های امنیتی هستند که باید توسط یک شبکه امن تامین شوند [۴] اما GSM در تامین این سرویس‌ها با مشکل جدی مواجه است [۵].

همانگونه که ذکر شد، USSD برای تبادل اطلاعات از کانال سیگنالینگ GSM استفاده می‌نماید. در واقع کلیه مشکلات امنیتی GSM به تمام سرویس‌ها و مسیرهای انتقال داده GSM و از جمله USSD قابل اعمال می‌باشند، چرا که حملات ذکر شده کلیه داده‌ها و اطلاعات سیگنالینگ مبادله شده را هدف قرار می‌دهند. بیان اصول امنیتی و مکانیزمهای امنیتی GSM در این مقال نمی‌گنجد. با این وجود در ادامه، به برخی از مهمترین مشکلات امنیتی GSM اشاره خواهد شد [۵].

۱- استفاده از پروتکل احراز اصالت یک سویه و امکان حمله مرد میانی[5]: به این معنی که کاربر باید اصالت خود را به شبکه ثابت کند و شبکه اصالت خود را به کاربر اثبات نمی‌نماید. این امر منجر به امکان انجام حمله مرد میانی از طریق اعمال BTS قلابی[6] می‌شود. در این حمله، حمله‌گر با قرار دادن یک ایستگاه فرستنده-گیرنده که کد شبکه موبایل واقعی را دارد، خود را به عنوان ایستگاه فرستنده- گیرنده پایه واقعی جا می‌زند و به عنوان واسطه‌ای بین کاربر و شبکه واقعی قرار گرفته، مبادرت به شنود و یا حتی تغییر پیامها و مکالمات کاربر می‌نماید. فرآیند این امر در شکل (۱) نشان داده شده است. سناریوهای متعددی جهت سوء استفاده از این نقطه ضعف قابل طرح و اجرا است که جهت اختصار به آنها نمی‌پردازیم.



شکل ۱- ایستگاه پایه قلابی [۶]

۲- اشکال در پیاده‌سازی الگوریتمهای A3/A8: با وجود آنکه طراحی GSM به اپراتور اجازه می‌دهد تا هر الگوریتمی را که می‌خواهد برای توابع A3 و A8 انتخاب کند، بسیاری از اپراتورها از همان الگوریتم موسوم به COMP128 (یا COMP128-1) که توسط انجمن GSM و به صورت مخفیانه طراحی شده بود،

[1] Integrity
[2] Non-repudiation
[3] Access Control
[4] Availability

[5] Man-in-the-middle attack
[6] False BTS (Base Transceiver Station)

استفاده می‌نمایند. ساختار COMP128-1 در نهایت به کمک مهندسی معکوس و اسناد لو رفته GSM مشخص و اشکالات امنیتی فراوانی در آن کشف شد. این الگوریتم علاوه بر اینکه امکان نشت کلید سری Ki را فراهم می‌کند (مخصوصا هنگامی‌که چالشهای تصادفی خاصی به آن اعمال شود)، ۱۰ بیت سمت راست کلید جلسه ۶۴ بیتی Kc تولید شده را تعمدا برابر صفر قرار می‌دهد که این امر منجر به کاهش فضای کلید الگوریتم رمز مورد استفاده خواهد شد و این امر مستقل از نوع الگوریتم رمزنگاری مورد استفاده، الگوریتم رمزنگاری را حدود ۱۰۲۴ مرتبه ضعیفتر و شکست پذیرتر خواهد نمود. برخی از اپراتورهای GSM, به سوی پیاده‌سازی جدیدتری از A3/A8، یعنی یک الگوریتم جدید و محرمانه، موسوم به COMP128-2 گام برداشته‌اند که به جز به ارث بردن یکی از ضعفهای عمده COMP128-1 یعنی فضای کلید کاهش یافته، اشکال امنیتی دیگری تاکنون در خصوص آن گزارش نشده است. از چندی پیش, الگوریتم COMP128-3 نیز پیشنهاد شده که مشابه COMP128-2 است؛ با این تفاوت که در آن، Kc به صورت کامل (۶۴ بیتی) تولید می‌شود و این امر، امکان بهره‌برداری از حداکثر قدرت الگوریتم رمزنگاری مورد استفاده را فراهم می‌آورد.

۳- حمله به سیم کارت و کپی سیم کارت[1]: یکی از خطرناک‌ترین انواع حملات، استخراج کلید سری Ki از سیم کارت مشترک است. برای اولین بار انجمن توسعه دهندگان کارت هوشمند و گروه تحقیقاتی ISAAC، اشکال عمده‌ای در الگوریتم COMP128-1 کشف نمودند که به طور موثری آنها را قادر می‌ساخت با ارسال تعداد زیادی چالش به سیم کارت، کلید سری Ki را در حدود زمان هشت ساعت استخراج نمایند. پس از آن, حملات دیگری مبنی بر ارسال چالشهای انتخابی به سیم کارت نیز پیشنهاد شدند که قادر به استخراج کلید سری در مدت زمانی به مراتب کمتر بودند. سرانجام در سال ۲۰۰۲, یک تیم تحقیقاتی از شرکت IBM روش جدیدی مبتنی بر استفاده از کانالهای جانبی[2] کشف نمودند که به وسیله آن، هکری که سیم کارت مشترک را فقط به مدت یک دقیقه در اختیار داشته باشد، قادر به استخراج کلید سری (Ki) وی خواهد بود. او به کمک عدد به دست آمده خواهد توانست سیم کارتی مشابه سیم کارت مشترک هدف تولید نموده و از آن سوء استفاده نماید. البته مشکل کوچکی نیز در استفاده از سیم کارتهای کپی شده وجود دارد و آن اینکه GSM در هر لحظه فقط به یک مشترک اجازه دستیابی به شبکه را می‌دهد. بنابراین اگر حمله‌گر و مشترک اصلی در یک زمان تلاش کنند تا به شبکه دسترسی پیدا کنند، شبکه خواهد فهمید که دو سیم کارت مشابه در دو موقعیت متفاوت وجود دارند و بلافاصله حساب مربوطه را مسدود و دسترسی هر دوی آنها را ممنوع خواهد ساخت.

۴- خطر استخراج کلید سری بدون تماس فیزیکی با سیم کارت: حمله‌گر می‌تواند از نقطه ضعف COMP128-1 استفاده نموده، حتی بدون در اختیار گرفتن سیم کارت مشترک مربوطه و از طریق ارتباطات رادیویی و ارسال چالشهای متعدد و دریافت پاسخ از مشترکی که TMSI یا IMSI او مشخص شده، اقدام به محاسبه کلید Ki وی نموده، یک کپی از سیم کارت او تهیه نموده و مبادرت به برقراری و یا دریافت تماسها و داده‌ها, با استفاده از حساب کاربری مشترک هدف قرار گرفته شده بنماید. البته استخراج کلید بدین طریق، چند ساعت به طول خواهد انجامید.

۵- ضعف شدید الگوریتمهای رمزنگاری مورد استفاده: باور عمومی بر این است که الگوریتم A5/2 با حدود 2^{16} گام در زمان واقعی[3] قابل شکست می‌باشد. در کاراترین حمله انجام شده بر این الگوریتم، احتیاج به کمتر از یک ثانیه مکالمه رمز شده با A5/2 می‌باشد تا در مدت زمانی کمتر از یک ثانیه، کلید رمز با استفاده از یک کامپیوتر معمولی استخراج شود [۷]. الگوریتم رمز A5/1 نیز که در ابتدا برای استفاده در اروپا طراحی شده بود, به دلیل مخفی‌کاری و مکتوم ماندن اشتباهات به درستی طراحی نشد و با حداکثر 2^{40} گام قابل شکست می‌باشد. مولفین [۸] از رخنه‌های ظریف موجود در ساختار فیدبک رجیسترها در A5/1 استفاده نموده و با فرض استفاده از COMP128-1 در پیاده‌سازی A3/A8، حمله‌ای را پیشنهاد داده‌اند که مبتنی بر یک مرحله پیش پردازش با 2^{48} عملیات می‌باشد و با استفاده از نتایج ذخیره شده این پیش پردازش، حمله به A5/1 بر روی یک کامپیوتر شخصی در زمان واقعی و به دو صورت زیر قابل انجام خواهد بود: در حالت اول به خروجی الگوریتم A5/1 در دو دقیقه اول مکالمه احتیاج است تا کلید Kc در کمتر از یک ثانیه استخراج شود و در حالت دوم، به خروجی الگوریتم A5/1 برای مدت دو ثانیه از مکالمه احتیاج است تا کلید Kc در زمان حدود دو دقیقه استخراج شود. تفاوت بین این دو حالت تنها در موازنه بین حافظه مصرفی و زمان می‌باشد.

[1] SIM Card Cloning

[2] Side-Channel attack

[3] Real-time

۶- کوتاه بودن دامنه حفاظت و مشکلات امنیتی ستون فقرات GSM: احراز اصالت و محرمانگی در GSM صرفاً ارتباط بین MS و BTS سرویس دهنده را حفاظت می‌کند، در حالی‌که کلیه مبادلات بین سایر اجزا به صورت معمولی و رمز نشده انجام می‌شود. این در حالی است که ارتباط بین BTS ها با یکدیگر و یا شبکه معمولاً از طریق لینکهای مایکروویو -که به راحتی قابل شنود می‌باشند- انجام می‌شود. لذا نفوذگر با نفوذ به قسمت ثابت GSM خواهد توانست به اهداف خود دست یابد. سیستمهای سیار در اصل از سیستم سیگنالینگ شماره ۷ (SS7[1]) به منظور ارتباط بین شبکه‌ها و برای فعالیتهایی نظیر احراز اصالت، به روز رسانی موقعیت، سرویس‌های تکمیلی و کنترل تماسها استفاده می‌نمایند، در حالی که امنیت SS7 به نوبه خود جای بحث دارد. بزرگترین آسیب‌پذیری SS7 ناشی از تعدد و پیچیدگی واسطهای بین موجودیتهای مستقل در آن است. همچنین استفاده از اتصالات داخلی شبکه و اینترنت به طور نمایی در حال رشد می‌باشد که زمینه‌ساز آسیب‌پذیری‌های مضاعفی خواهد بود. مشکل سیستمهای SS7 عمومی این است که پیامها به صورت غیرقابل کنترلی قابل تغییر، تزریق و یا حتی حذف می‌باشند. این امر، این امکان را فراهم می‌آورد تا حمله‌کننده با تولید پیامهای SS7 و اعمال آنها به شبکه، قادر به در هم گسیختن سرویس‌ها و حتی برقراری تراکنشهایی باشد.

۷- معلوم نبودن وضعیت رمزنگاری برای کاربر: کاربر اطلاعی از فعال بودن یا نبودن رمزنگاری ندارد و اختیار این امر با شبکه است و لذا یک BTS قلابی می‌تواند حالت بدون رمزنگاری را انتخاب نموده و مشترک شبکه را مجبور به ارسال داده‌ها در حالت آشکار و بدون رمزنگاری نماید.

۸- ضعف در حفظ گمنامی کاربران: در GSM این قاعده پیش‌بینی شده که اگر مشترک برای بار اول وارد شبکه شود و یا به هر دلیلی جدول نگاشت بین IMSI و TMSI در شبکه از بین برود، شبکه از مشترک تقاضای اعلام IMSI را بنماید. چون این اعلام در حالت آشکار و بدون رمزنگاری خواهد بود، حمله‌گر می‌تواند از این امر سوء استفاده کند.

۹- امکان حمله اختلال در سرویس[2]: حمله‌کننده می‌تواند به طور مکرر با مشخصات مختلف با شبکه ارتباط برقرار نموده و تقاضای تخصیص کانال نماید و بدین نحو تمام کانالهای خالی یک سلول را اشغال نموده، مانع ارتباط سایر مشترکین با شبکه شود.

این حمله از آن جهت امکان پذیر است که در پروتکل برپایی ارتباط، هیچ مکانیزمی برای احراز اصالت کاربر و حفظ جامعیت اطلاعات سیگنالینگ در نظر گرفته نشده است. این حمله, هزینه‌ای برای حمله‌کننده در بر نخواهد داشت، ضمن آنکه شبکه نیز نخواهد توانست وقوع چنین حمله‌ای را تشخیص دهد.

۱۰- عدم حفظ جامعیت اطلاعات: علیرغم آنکه معماری امنیتی GSM احراز اصالت و محرمانگی را مدنظر قرار داده است، ملاحظه‌ای برای حفظ جامعیت اطلاعات صورت نگرفته است [۹]. بنابراین گیرنده نمی‌تواند مطمئن باشد که داده‌های دریافت شده همان داده‌های ارسال شده هستند.

۱۱- امکان استفاده از حملات تکرار[3]: حمله‌کننده می‌تواند از اطلاعات مبادله شده قبلی بین کاربر و شبکه سوء استفاده نماید. به عنوان مثال, پروتکل چالش-پاسخ احراز اصالت در برگیرنده مهر زمانی نمی‌باشد. بنابراین چنانچه یک BTS قلابی به طرز موفقیت آمیزی خود را به عنوان BTS واقعی جا بزند, قادر به حفظ کلید جلسه خواهد بود که برای مدت احتمالا مدیدی به او اجازه رمزگشایی داده‌هایی را خواهد داد که با استفاده از این کلید، رمز می‌شوند. نمونه دیگری از حمله تکرار مبتنی بر استفاده مجدد از بردار احراز اصالت است که ممکن است چندین بار توسط شبکه مورد استفاده قرار بگیرد.

۱۲- افزایش افزونگی[4] به دلیل انجام کدینگ قبل از رمزنگاری: در GSM، کدینگ تصحیح خطا قبل از انجام عمل رمزنگاری صورت می‌پذیرد که این امر باعث افزایش همبستگی پیام شده و انجام حمله به الگوریتمهای رمزنگاری را تسهیل می‌نماید.

موارد ذکر شده صرفا به تعدادی از مهمترین مشکلات امنیتی GSM اشاره دارند. سناریوهای متعددی برای سوء استفاده عملی از این اشکالات قابل طرح و اجرا است که یکی از آنها در بخش بعد مورد توجه قرار خواهد گرفت. موارد ذکر شده به خوبی بیانگر این نکته است که GSM فاقد ویژگیهای یک شبکه امن است و این نا امنی را به طور ذاتی به USSD انتقال داده است.

۳-۲- مشکلات امنیتی خاص USSD

همانگونه که ذکر شد، USSD تعدادی آسیب‌پذیری اضافه و مختص به خود نیز دارد. بسیاری از مشکلات امنیتی USSD، مشابه SMS می‌باشد. اما USSD از برخی جهات امن‌تر از SMS

[1] Signaling System #7

[2] Denial of Service attack (DoS attack)

[3] Replay attack

[4] Redundancy

می‌باشد. به عنوان مثال، یکی از آسیب‌پذیریهای اضافه‌ای که SMS دارد، مربوط به خاصیت ذخیره پیامها بر روی مرکز SMS[1] و همچنین تلفن همراه کاربر می‌باشد که با دسترسی به مرکز SMS و یا سرقت گوشی، اطلاعات شخصی کاربر در معرض تهدید قرار خواهد گرفت. اما در USSD، اطلاعات مبادله شده به صورت ثابت در مرکز USSD ذخیره نمی‌شود بنابراین چنانچه نفوذگر قادر به دسترسی به اطلاعات مرکز USSD باشد، فقط قادر به شنود اطلاعات از آن لحظه به بعد خواهد بود و به پیامهای مبادله شده قبلی دسترسی نخواهد داشت. در خصوص ذخیره اطلاعات بر روی گوشی کاربر نیز این آسیب‌پذیری در USSD وجود دارد ولی از آسیب‌پذیری مشابه در SMS خفیف‌تر است. بدین معنا که در USSD نیز امکان و قابلیت ذخیره موقت رشته‌های USSD بر روی گوشی تلفن همراه وجود دارد. این رشته‌ها ممکن است حاوی اطلاعات حساب بانکی و PIN مخصوص برای دسترسی به این حساب باشد که در صورت سرقت گوشی می‌توانند مورد سوء استفاده قرار گیرند که این ویژگی مشابه داستان سرقت کارت بانکی ATM به همراه یادداشت حاوی PIN کاربر است. همانگونه که ذکر شد، پیامهای USSD را می‌توان مستقیما از صفحه اصلی وارد نمود، مشابه حالتی که برای شماره‌گیری معمولی مورد استفاده قرار می‌گیرد. بنابراین دسترسی به پیامهای قبلی USSD معمولا با فشردن دکمه تکرار در گوشیها میسر است که در صورت سرقت گوشی این امر می‌تواند مورد سوء استفاده قرار گیرد. با این وجود معمولا در گوشیها با تعویض سیم کارت، شماره‌های قبلی وارد شده و از جمله رشته‌های USSD از حافظه دستگاه پاک شده و قابل دسترسی نمی‌باشند. بر خلاف SMS که معمولا حتی با وجود تعویض سیم کارت، پیامهای کوتاه ذخیره شده بر روی گوشی توسط سایر استفاده کنندگان از آن گوشی، قابل مشاهده است. اگر چه USSD نسبت به SMS از امنیت بالاتری برخوردار است، ولی این برتری در برابر مشکلات امنیتی متعددی که USSD به عنوان یک روش انتقال داده در GSM با آنها مواجه است، ناچیز است.

یکی دیگر از مشکلات امنیتی USSD، مربوط به قابلیت رومینگ است که از آن به عنوان مزیتی برای استفاده از USSD در سایر شبکه‌ها و کشورها ذکر می‌شود. به عنوان مثال معمولا در تبلیغات عامیانه، استفاده از یک سیستم پرداخت سیار مبتنی بر USSD در سایر کشورها -که امنیت آن مبتنی بر امنیت فراهم آمده توسط GSM و PIN کاربر است- به عنوان مزیتی برای این سیستم پرداخت سیار ذکر می‌شود، حال آنکه این مزیت چیزی به جز یک آسیب‌پذیری و تهدید امنیتی بزرگ نیست؛ چرا که محتویات USSD یک کاربر در حال رومینگ می‌بایست به HLR شبکه خانگی وی منتقل شود که این اطلاعات از شبکه‌های مختلف و حتی گاهی اینترنت عبور می‌کنند و این امر می‌تواند حساب بانکی کاربر در حال رومینگ را در معرض آسیب‌پذیری‌ها و حملات مختلف قرار دهد.

۴- ارزیابی امنیت USSD

مشکلات امنیتی USSD در بخش قبل مورد توجه قرار گرفتند. USSD را از نقطه نظر کاربردهای مالی و تجاری نمی‌توان یک کانال مطمئن و امن تلقی نمود چرا که به طور طبیعی در آن مکانیزمی برای رمزنگاری داده ها و یا بررسی جامعیت پیام در نظر گرفته نشده است. با این وجود USSD (پس از SMS) پر کاربردترین روش دسترسی در میان روشهای موجود تجارت سیار است [۳]. همین عدم توجه کافی به مقوله امنیت در تجارت و پرداخت سیار مهمترین مانع در رسیدن حجم تجارت سیار به پیش‌بینی‌های انجام شده است. براساس تحقیقات انجام شده توسط فورستر، نگرانیهای امنیتی مانع اصلی برای حدود ۵۲ درصد کاربرانی است که هیچ نوع تراکنش تجاری با تلفنهای همراه انجام نمی‌دهند [۱۰]. برای درک بهتر از آسیب‌پذیری امنیتی USSD در ادامه به بیان سناریویی برای سوء استفاده از یک روش پرداخت سیار مبتنی بر امنیت شبکه تلفن همراه و استفاده از PIN کاربر خواهیم پرداخت با این توضیح که بیشتر سیستمهای موجود پرداخت سیار مبتنی بر چنین پیش فرضهایی می‌باشند. در ابتدا لازم است که ساختار یک پیام USSD را مورد توجه قرار دهیم. فرمت پیامهای USSD را می‌توان به صورت زیر خلاصه نمود [۲]:

- نشان ستاره (*) برای جدا کردن پارامترها از یکدیگر مورد استفاده قرار می‌گیرد.
- یک کد سرویس ۲ یا ۳ رقمی وارد می‌شود.
- اطلاعات تکمیلی با طول دلخواه و متغیر را می‌توان وارد نمود. به عنوان نمونه یک PIN را به عنوان معیاری از امنیت می‌توان وارد نمود.
- کلید # درخواست را پایان می‌بخشد.

این رشته پیام سپس از طریق شبکه به HLR خانگی مشترک ارسال می‌شود. همانطور که می‌دانیم مبادلات بر روی ستون فقرات شبکه GSM رمز نمی‌شود و بررسی جامعیت نیز بر روی آن انجام نمی‌پذیرد. این امر USSD را در برابر حملات مختلف آسیب‌پذیر

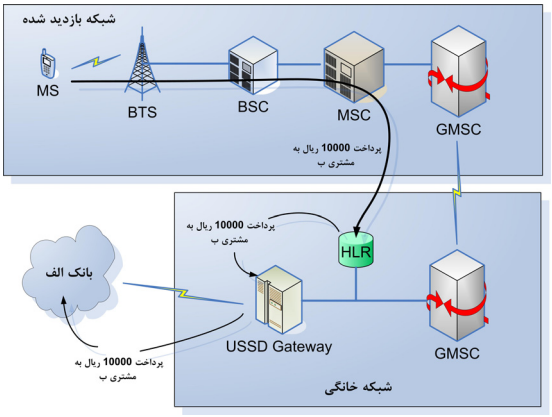
[1] SMS Center

می‌سازد. بنابراین حمله‌گر به راحتی می‌تواند به تغییر، حذف و یا حتی ایجاد پیامهای جعلی بر روی شبکه بپردازد. چنانچه USSD در کاربردهایی نظیر درخواست تغییر سرویس مورد استفاده قرار گیرد، این امر ممکن است مشکل چندانی ایجاد نکند. اما اگر USSD برای یک تراکنش مالی مورد استفاده قرار گیرد، وضع فرق خواهد کرد. به منظور توضیح بیشتر، در ادامه به بیان یک سناریوی حمله می‌پردازیم. فرض کنید مشتری بانک الف -که قبلا طبق توافقی در بانک مزبور به عنوان یک مشتری سرویس بانکداری سیار ثبت نام کرده است- در حال رومینگ در اروپا باشد. بانک الف از طریق یک کاربرد مبتنی بر USSD امکان پرداخت از طریق کارت اعتباری به هر کارت اعتباری دیگر را برای مشتری مزبور فراهم می‌آورد. مشتری بانک الف نیازمند پرداخت مبلغی به مشتری ب می‌شود. او همانطور که در شکل (۲) نشان داده شده است، دستور پرداخت زیر را از طریق USSD برای بانک الف ارسال می‌نماید:

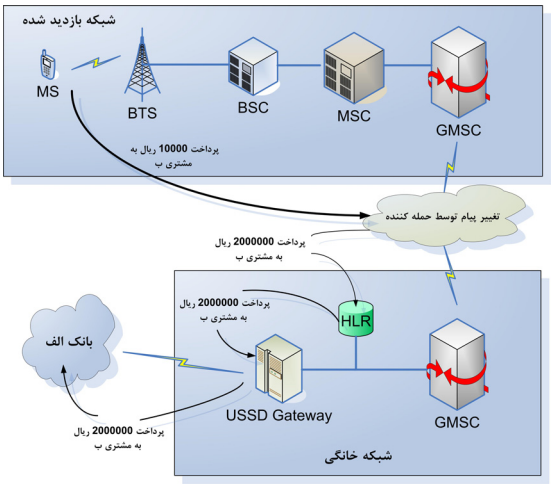
*184*1234*1*10000*0101852414007*+989122597712#

که در آن، 184 کد سرویس، 1234 PIN مشترک الف، 1 مشخص کننده نوع حسابی که برداشت باید از آن صورت پذیرد، 10000 مبلغی (حسب پول رایج محلی) که باید پرداخت شود، 0101852414007 شماره حسابی که برداشت باید از آن صورت گیرد، 989122597712+ شماره تلفنی که تاییدیه پرداخت باید برای آن ارسال شود و # خاتمه دهنده درخواست می‌باشد.

از طرفی، مشتری ب که دچار مشکل مالی بزرگی شده است، دوستانی در یک اتحادیه کلاهبرداری دارد و به آنها می‌گوید که مشتری الف به زودی مبلغی را از طریق کاربرد بانکداری سیار به وی پرداخت خواهد کرد و ممکن است از آنها بخواهد برای پرداخت بدهی وی تا جایی که ممکن است برایش سرقت کنند. اتحادیه مزبور به فن‌آوری لازم برای ایجاد وقفه و تغییر در تراکنش مجهز است. از آنجا که هیچگونه رمزنگاری و بررسی جامعیت بر روی پیامها در حین انتقال بر روی ستون فقرات شبکه موبایل انجام نمی‌شود، انجام چنین حمله‌ای امکان‌پذیر است. حمله‌کننده قادر به تغییر مبلغ پرداخت و حتی حسابی که پول می‌بایست به آن پرداخت شود، می‌باشد. شکل (۳) فرآیند این حمله را نشان می‌دهد. از سناریوی بیان شده مشخص می‌شود که به منظور منطقی بودن انجام تراکنشهای مالی از طریق USSD می‌بایست امکان رمزنگاری و بررسی جامعیت پیام به نحوی در این کانال لحاظ گردد. USSD به تنهایی قادر به فراهم آوردن این سرویس بر روی خودش نیست. لذا برای امنیت بخشی به این سرویس، کاربرد یا فن‌آوری دیگری مورد نیاز است.



شکل ۲- روند استفاده از USSD در یک تراکنش مالی نوعی



شکل ۳- فرآیند ایجاد وقفه و تغییر پیام USSD در یک تراکنش مالی

۵- نتیجه‌گیری

در این مقاله، داده سرویس تکمیلی ساخت نیافته (USSD)، به عنوان یک سرویس نشست گرا و پرکاربرد ارائه شده توسط شبکه تلفن همراه GSM مورد بررسی قرار گرفت و مزایا و معایب فراهم آمده توسط این سرویس معرفی شدند. همچنین مشکلات و آسیب‌پذیریهای امنیتی مرتبط با آن مورد بررسی قرار گرفتند و مشخص شد که USSD از امنیت کافی برای انجام تراکنشهای مالی برخوردار نمی‌باشد و بنابراین نباید به تنهایی برای این منظور مورد استفاده قرار گیرد.

مراجع

[1] GSM World News – Statistics: http://www.gsmworld.com/news/statistics/pdf/gsma_stats_q4_07.pdf.

[2] "European Telecommunications Standards Institute. Digital cellular Telecommunications system (Phase 2); Unstructured Supplementary Service Data (USSD); Stage 1. GSM 02.90 version 4.1.1. ETSI September 1997."

[3] A. Sarajlic and D. Omerasevic, "Access Channels in m-Commerce Services," in *29th International Conference on Information Technology Interfaces (ITI'07)*, Croatia.

[4] W. Stallings, *Network Security Essentials: Applications and Standards*: Prentice Hall, 2000.

[5] M. Toorani and A. Beheshti, "Solutions to the GSM Security Weaknesses," in *2nd IEEE International Conference on Next Generation Mobile Applications, Services, and Technologies (NGMAST'08),*, University of Glamorgan, Cardiff, UK, pp. 576-581.

[6] S. M. Siddique and M. Amir, "GSM Security Issues and Challenges," in *Seventh IEEE International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD'06)*, pp. 413-418.

[7] E. Barkan, E. Biham, and N. Keller, "Instant Ciphertext-Only Cryptanalysis of GSM Encrypted Communication," in *CRYPTO 2003*, pp. 600-616.

[8] A. Biryukov, A. Shamir, and D. Wagner, "Real Time Cryptanalysis of A5/1 on a PC," in *FSE 2000*, pp. 1-18.

[9] P. Chandra, *Bulletproof Wireless Security: GSM, UMTS, 802.11 and Ad hoc Security*: Elsevier, 2005.

[10] M. Khosrow-Pour, *Encyclopedia of E-Commerce, E-Government, and Mobile Commerce*: Idea group publication, 2006.