آشنایی با معماری USSD و راهکارهایی برای بهبود مشکلات آن

USSD چیست و خطرات امنیتی آن کدامند؟

برای کاربران ساکن در مناطق دورافتاده که از گوشی‌های غیرهوشمند استفاده می‌کنند، USSD راهکار مناسبی برای دسترسی به خدمات بانکی و پرداخت‌های بانکی است. شبیه به هر فناوری دیگری USSD دارای یکسری مشکلات امنیتی است. اگر ویژگی‌های امنیتی USSD بهبود یابند، فناوری فوق به گزینه بهتری برای اطلاع‌رسانی و انجام کارهای جدی‌تر تبدیل می‌شود. قابلیت‌های امنیتی USSD تنها زمانی بهبود پیدا می‌کنند که درک درستی از معماری، مزایا، مخاطرات و مشکلات این فناوری داشته باشیم.

ارسال پیام از طریق کد دستوری (USSD) سرنام Unstructured Supplementary Services Data، یک فناوری نشست‌محور بلادرنگ (real-time session) است که برای ارسال کدهای دستوری از سوی بانک‌ها یا شبکه‌های موبایلی با (یا بدون) اینترنت و از طریق کانال GSM استفاده می‌شود. برای خدمات بانکی که از فناوری ارسال پیام از طریق کد دستوری استفاده می‌کنند، اپراتور شبکه موبایل (MNO) سرنام Mobile Network Operator نقش رابطی میان مشتری و بانک را دارد که راهکاری سریع، ارزان و تعاملی ارائه می‌کند که به لحاظ هزینه، امنیت و مصرف کانال ارتباطی در مقایسه با سرویس پیام کوتاه مقرون به صرفه‌تر است. سرویس پیام کوتاه همیشه از کانال صوتی استفاده می‌کند، در حالی که USSD معمولا از کانال صوتی استفاده می‌کند و هر زمان کانال فوق شلوغ باشد از کانال دیگری استفاده می‌کند. USSD یک راهکار مستقل از سکو است که برای بهره‌مندی از آن نیازی نیست هیچ نرم‌افزاری توسط کاربر دانلود شود. برای کاربران ساکن در مناطق دورافتاده که از گوشی‌های غیرهوشمند استفاده می‌کنند، USSD راهکار مناسبی برای دسترسی به خدمات بانکی و پرداخت‌های بانکی است. شبیه به هر فناوری دیگری USSD دارای یکسری مشکلات امنیتی است. اگر ویژگی‌های امنیتی USSD بهبود یابند، فناوری فوق به گزینه بهتری برای اطلاع‌رسانی و انجام کارهای جدی‌تر تبدیل می‌شود. قابلیت‌های امنیتی USSD تنها زمانی بهبود پیدا می‌کنند که درک درستی از معماری، مزایا، مخاطرات و مشکلات این فناوری داشته باشیم.

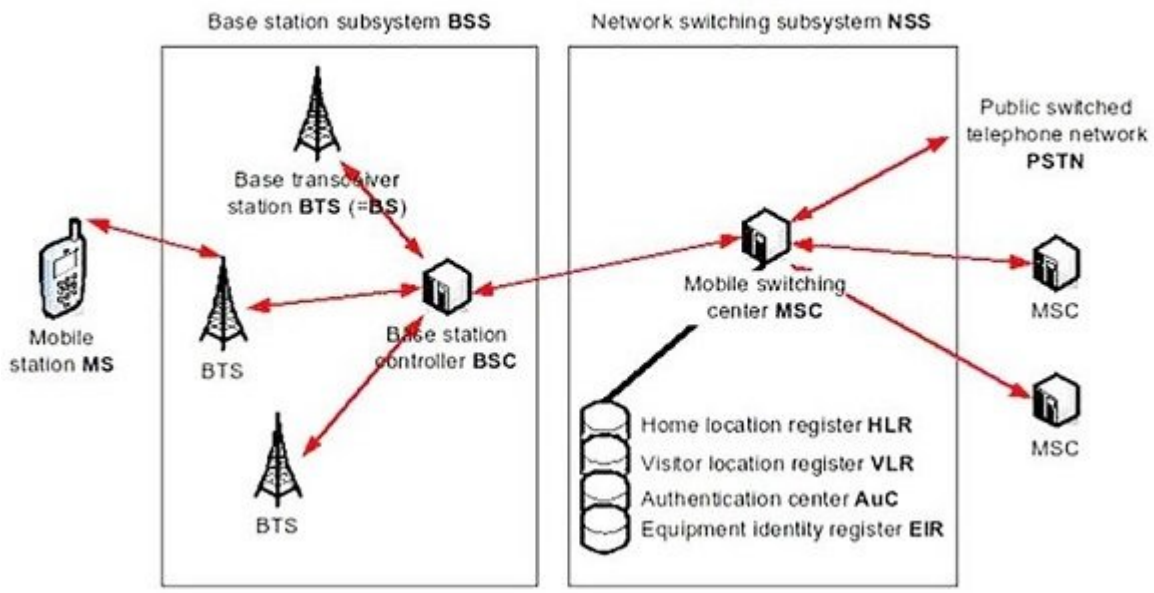
رشد روزافزون تراکنش‌های بدون پول نقد

امروزه با ظهور پروژه‌هایی همچون هند دیجیتال که راهکار تراکنش بدون پول نقد و پرداخت الکترونیک را پیشنهاد می‌دهند، ضریب نفوذ گوشی‌های هوشمند و سایر دستگاه‌های همراه در کشورهایی همچون هند رشد چشم‌گیری داشته‌اند. خبرگزاری تنسیم در خبر 31 فروردین ماه 1398 سایت خود نوشت: « هند دومین اقتصاد دیجیتال سریع جهان است. ساندار پیچای مدیرعامل گوگل در غالب پروژه‌ای به دنبال آن است تا رویای هند دیجیتال را به واقعیت تبدیل کند.»
اپراتورهای شبکه همراه از دستگاه‌های همراه برای ارائه خدمات مخابراتی رایج و گسترش نام تجاری خود استفاده می‌کنند. البته در این میان نباید از نقش اپراتورهای شبکه همراه مجازی (MVNO) سرنام Mobile Virtual Network Operator غافل شد. کاربران علاوه بر استفاده از خدمات موبایلی رایج، برای انجام تراکنش‌های مالی آنلاین و سایر

کارهای شخصی و اداری خود از گوشی‌های هوشمند استفاده می‌کنند. تراکنش‌های موبایلی به دلیل مزایای شناخته شده‌ای همچون صرفه‌جویی در وقت، سهولت استفاده و دسترس‌پذیری بالا محبوبیت زیادی نزد مردم پیدا کرده‌اند. امروزه، بانک‌ها در کشورهای مختلف جهان خدمات و تراکنش‌های مبتنی بر موبایل را ارائه می‌دهند، زیرا خدمت‌رسانی به مشتریان به شکل مطلوب‌تری انجام می‌شود، هزینه‌ها کاهش پیدا می‌کند، سهم آن‌ها در بازار رقابتی جذب مشتریان بیشتر می‌شود و به رونق برند تجاری آن‌ها کمک می‌کند. خدمات مالی مبتنی بر موبایل از طریق فناوری‌های مختلف همچون سرویس پیام کوتاه (SMS)، کدهای دستوری(USSD)، برنامه‌های مبتنی بر مرورگرها، برنامه‌های کاربردی مشتری‌محور، پاسخ صوتی تعاملی(IVR) و پروتکل دسترسی بی‌سیم (WAP) در اختیار مردم قرار می‌گیرد. در میان فناوری‌های مختلفی که به آن‌ها اشاره شد، پیام کوتاه و USSD بیشترین سهم را دارند، هرچند بیشتر موسسات مالی ترجیح می‌دهند از USSD استفاده کنند.

معماری USSD

USSD از کدهایی استفاده می‌کند که پیشوند * و پسوند # دارند. این کدها در قالب رشته‌های MMI سرنام Man Machine که بخشی از استاندارد TS 24.390 هستند توسط USSD استفاده می‌شوند. این رشته‌ها توسط ایستگاه موبایل (Mobile Station) یا ایستگاه شبکه (Network Station) مقداردهی اولیه می‌شوند. عملکرد USSD بر مبنای این رشته‌ها در یکی از دو حالت pull برای مدیریت درخواست‌های مقداردهی شده توسط ایستگاه شبکه یا حالت push برای مدیریت درخواست‌های مقداردهی شده توسط ایستگاه موبایل پیاده‌سازی می‌شود. شکل 1 معماری شبکه GSM که توسط USSD استفاده می‌شود را نشان می‌دهد.



1 - معماری شبکه GSM

ماژول‌های استفاده شده توسط USSD

برای آشنایی بهتر با USSD باید درباره ماژول‌های شبکه موبایل که نقش کلیدی در فناوری USSD دارند توضیحاتی ارائه کنیم.

Mobile Station: ایستگاه موبایل (MS) از تجهیزات موبایل (Mobile Equipment) و ماژول شناسایی مشترک (Subscriber Identity Module) تشکیل شده که مسئولیت رسیدگی به درخواست‌های ارسال یا دریافت شده را دارد.

Base Station subsystem: زیرسامانه ایستگاه پایه (BSS) مدیریت ترافیک و ارسال سیگنال میان ایستگاه موبایل و زیرسامانه راهگزینی شبکه (Network Switching Subsystem) را عهده‌دار است. این مولفه، کدگذاری کانال‌های گفتاری، تخصیص کانال‌های رادیویی به گوشی‌های همراه و انتقال و دریافت سیگنال‌ها از طریق خطوط هوایی را مدیریت می‌کند. زیرسامانه ایستگاه پایه از دو بخش BTS و BSC تشکیل شده است.

Base Transceiver Station: ایستگاه فرستنده‌گیرنده پایه (BTS) شامل ماژول‌های فرستنده و گیرنده، آنتن‌ها و تجهیزات لازم برای رمزنگاری و رمزگشایی ارتباطات کنترل‌گر ایستگاه پایه با ایستگاه فرستنده و گیرنده است. BTS برای آن‌که بتواند از فرکانس‌های متفاوت و بخش‌های مختلف سلول مخابراتی به ساده‌ترین شکل استفاده کند متشکل از چند فرستنده و گیرنده است.

Base Station Controller: کنترل‌کننده ایستگاه پایه (BSC) برای انجام درست و هوشمندانه کارها اطلاعاتی که ایستگاه فرستنده‌وگیرنده به آن نیاز دارد را در اختیارش قرار می‌دهد.

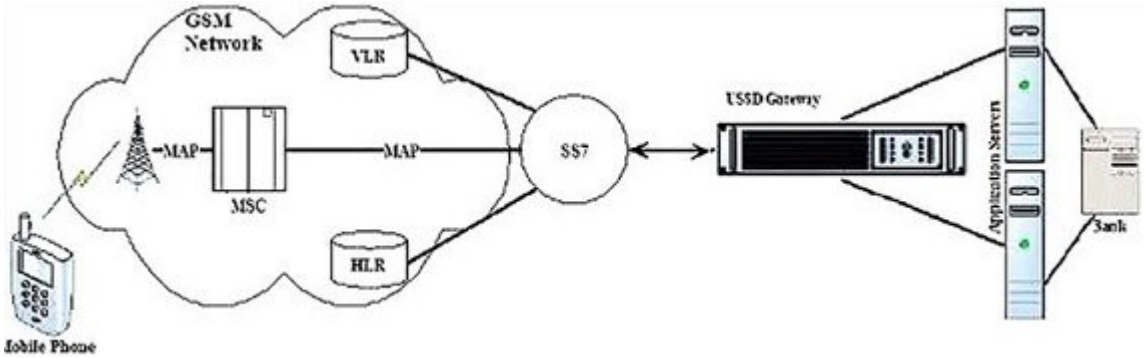
Mobile Switching Center: مرکز راهگزینی موبایل (MSC) یک یا چند کنترل‌کننده ایستگاه پایه را کنترل می‌کند. این مولفه فرآیندهای احراز هویت اولیه موبایل، تنظیمات، مسیریابی و هدایت تماس‌ها، به‌روزرسانی موقعیت مکانی در HLR، VLR، مدیریت امنیت، حسابرسی، شارژ و مدیریت سایر سرویس‌ها همچون USSD، SMS و.... را عهده‌دار است.

Home Location Register: مرکز ثبت موقعیت خانه (HLR)، اطلاعات مشترکان جدید را نگه‌داری می‌کند. این بخش، اطلاعات ثابت شناسه بین‌المللی مشترک همراه (IMSI) سرنام
IMSI International Mobile Subscriber Identity، شماره منحصر به فرد شناسایی هر مشترک در شبکه موبایلی (MSIISDN) سرنام number uniquely identifying a subscription in a mobile network و اطلاعات محرمانه مشترک که شامل کلیدهای استفاده شده در رمزگذاری و رمزگشایی مسیر میان HLR و MS است و اطلاعاتی که جنبه محرمانگی ندارند (نام و آدرس) را شامل می‌شود.

Visitor Location Register: ثبت موقعیت مکانی بازدیدکننده (VLR) با هدف کم کردن بارترافیکی HLR استفاده می‌شود و اطلاعات پویایی در ارتباط با مشترکان که جنبه محرمانگی ندارند را نگه‌داری می‌کند.

Authentication Center: مرکز احراز هویت (AC) برای بررسی صحت کاربری که تماسی برقرار کرده یا به تماسی پاسخ داده استفاده می‌شود. احراز هویت در زمان ارتباط اولیه ایستگاه موبایل و زمانی که تماسی گرفته یا دریافت شده یا در زمان به‌روزرسانی موقعیت مکانی انجام می‌شود.

Equipment Identify: ماژول ثبت شناسه تجهیزات (EI)، شماره IMEI را ذخیره کرده و زمانی‌که یک گوشی یا تبلت به سرقت می‌رود، برای بلوکه کردن شماره تلفن استفاده می‌شود.
این مولفه‌ها زمانی که USSD از کانال GSM برای ارائه خدمات بانکی استفاده می‌کند در تعامل با یکدیگر استفاده می‌شوند. شکل 2 نحوه تعامل این عناصر با یکدیگر را نشان می‌دهد.



□□□ 2- □□□□□□□□ □□ USSD □□□□□ □□□□□□□□□ □□ □□□□□ □□ GSM □□□□□ □□□□□ □□□□□

به منظور بهره‌مندی از خدمات بانکی مبتنی بر USSD، کاربر در اولین گام از ایستگاه موبایل رشته USSD MMI را دریافت می‌کند. در مرحله بعد بخش مدیریت USSD در ایستگاه موبایل نشستی ایجاد کرده و درخواست USSD که شامل رشته USSD است را ارسال می‌کند. در حالت کلی، ترتیب ارسال درخواست از مسیر MSC-> VLR->HLR->USSD Gateway عبور می‌کند که ماژول بخش کاربردی موبایل (MAP) سرنام Mobile Application Part مسئولیت هدایت درست درخواست را عهده‌دار است. بسته به نوع خدماتی که مدنظر کاربر است، درخواستUSSD توسط بخش مدیریت USSD یا یک گره خاص در مسیر انجام شده یا به گره دیگری هدایت

می‌شود. در مورد خدمات بانکی، تقریبا تمامی درخواست‌ها تنها از طریق دروازه USSD ارسال شده و مدیریت می‌شوند.
دروازه ارسال پیام از طریق کد دستوری (USSD Gateway) این امکان را برای اپراتور شبکه موبایل فراهم می‌کند تا یک منوی تعاملی به کاربر نشان دهد تا فرآیند نمایش سرویس‌های مالی به شکل ساده‌تری انجام شود. در این میان سرور برنامه کاربردی مالی که فرآیند احراز هویت، صدور مجوز و سایر مسائل امنیتی آن از طریق سرور بانک مرکزی انجام می‌شود، منوی خدمات مالی را نشان داده و گزینه‌هایی که کاربر انتخاب می‌کند را اجرا می‌کند.
رابط کاربری MAP یک لایه کاربردی ارائه می‌کند که اجازه می‌دهد فرآیند توسعه خدمات کاربردی برای شبکه GSM به شکل ساده‌ای امکان‌پذیر شود. MAP با پروتکل SS7 سرنام Signalling System 7 بسته‌بندی (کپسوله شده) شده و ارسال می‌شود.

USSD چه مزایایی دارد؟

USSD با این معماری دقیق و پیچیده چه مزایایی دارد؟ از شاخص‌ترین مزایای USSD به موارد زیر می‌توان اشاره کرد:

- برقراری و حفظ یک نشست مستقیم میان فرستنده و گیرنده با هدف انتقال سریع داده‌ها
- عدم ذخیره‌سازی اطلاعات محرمانه در گوشی‌های همراه
- پیاده‌سازی سریع و منوی کاربری ساده که فرآیند انتخاب در میان گزینه‌ها را ساده کرده و یک بازه زمانی برای خروج از گزینه‌ها را در نظر می‌گیرد.
- پشتیبانی همزمان از هر دو سرویس تماس صوتی و USSD بدون نیاز به اینترنت
- امنیت بیشتر به دلیل عدم ذخیره‌سازی اطلاعات در گوشی موبایل برعکس پیام کوتاه
- کم هزینه بودن این فناوری برای ارائه‌دهنده خدمات، زیرا فناوری فوق از پروتکل SS7 استفاده می‌کند و در نتیجه برای ارسال اعلان‌های مرتبط با خدمات جدید نیز می‌توان از آن استفاده می‌کند.
- فارغ از سکو بودن، به عبارت دقیق‌تر، USSD به مدل گوشی یا نوع سیم کارت وابسته نیست و روی همه گوشی‌هایی که از GSM پشتیبانی می‌کنند قابل استفاده است.
- با توجه به این‌که تمامی پیام‌های USSD از شبکه خانگی کاربر برای راهگزینی (مسیریابی) استفاده می‌کنند، تمام خدمات USSD در شبکه‌های خانگی بدون تحمیل هیچ‌گونه هزینه اضافی در حالت رومینگ قابل استفاده است.

چه مخاطرات امنیتی USSD را تهدید می‌کنند؟

USSD یک فناوری منحصر به فرد است که اجازه می‌دهد کاربر به ساده‌ترین شکل و به دور از هرگونه پیچیدگی از آن استفاده کند. زمانی که از خدمات همراه اول، رایتل یا خدمات بانکی استفاده می‌کنید، بدون آن‌که با مشکل خاصی روبرو شوید، قادر هستید از خدمات USSD روی سیم‌کارت دایمی یا اعتباری خود استفاده کنید. با این وجود همانند هر فناوری دیگری USSD مشکلات امنیتی خاص خود را دارد که بخشی از آن‌ها متاثر از GSM هستند که از آن جمله به موارد زیر می‌توان اشاره کرد:

- الگوریتم COMP128 که توسط سیم‌کارت و AUC برای تولید درخواست Signed RES استفاده می‌شود، شکسته شده یا به عبارت دقیق‌تر هک شده است. الگوریتم فوق هنوز هم در دستگاه‌های موبایل قدیمی استفاده شده و جایگزینی برای آن ارائه نشده است.
- مقداردهی اولیه RAND که در زمان احراز هویت اولیه با ایستگاه موبایل ارسال می‌شود قابل هک بوده و امکان پیاده‌سازی یک حمله محروم‌سازی از سرویس وجود دارد.
- کلید خصوصی Kc که الگوریتم A5 آن‌را تولید می‌کند را می‌توان با استفاده از مقادیر RAND و ki رمزگشایی کرد و به شنود سیگنالی پرداخت که میان ایستگاه موبایل و زیرسامانه ایستگاه پایه مبادله می‌شود.
- اطلاعات درخواست و انتقال شناسه بین‌المللی مشترک موبایل (IMSI) رمزنگاری و احراز هویت نمی‌شوند.
- هیچ‌گونه رمزنگاری میان مبدا و مقصد انجام نشده و رمزنگاری به کانال‌هایی که میان ایستگاه موبایل و زیرسامانه ایستگاه پایه قرار دارند محدود می‌شود.
- GSM در سرویس جهانی مخابرات همراه (UMTS) که مبتنی بر استاندارد 3G است دارای برخی محدودیت‌ها با هدف بهبود مشکلات امنیتی است که از آن جمله به موارد زیر می‌توان اشاره کرد:
- به‌کارگیری شناسه موقت برای TMSI سرنام Temporary Mobile Subscriber Identity

- احراز هویت دو طرفه کاربر و شبکه
- رمزنگاری شبکه دسترسی رادیویی
- محافظت از یکپارچگی ارسال سیگنال در برابر حملات مرد میانی

مخاطرات امنیتی USSD

در کنار مشکلات امنیتی که USSD در تعامل با شبکه GSM دارد، این فناوری خود دارای یکسری مشکلات امنیتی است که از آن جمله به موارد زیر می‌توان اشاره کرد:

- پیام‌های درخواست و پاسخ به USSD قابل دستکاری هستند که باعث شکل‌گیری یک حمله بازپخشی می‌شوند.
- تاخیری که میان پیام‌های درخواست و پاسخ USSD وجود دارند، امکان دستکاری درخواست و پاسخ را ممکن می‌کنند.
- در زمان به‌کارگیری USSD در خدمات بانک‌داری، اطلاعات حساس کاربر همچون MPIN، شماره حساب و... نشان داده می‌شود و این احتمال وجود دارد فردی که در حال تماشای تراکنش است از اطلاعات فوق بهره‌برداری غیرمجاز کند.
- از کدهای خاص USSD که کدهای کثیف (dirty USSD) نام دارند، برای تغییر پین‌کد، بازگشت به تنظیمات کارخانه یا نمایش شماره IMEI می‌توان استفاده کرد.

USSD یک فناوری انتقال پیام مبتنی بر نشست است که بیشترین زمان نشست آن 2 دقیقه است. اگر نشستی به وضعیت بیکار (idle session) وارد شود، سرور پس از 20 ثانیه به نشست پایان می‌دهد. در اغلب موارد کاربر پیش از خاتمه نشست توسط سرور به نشست پایان می‌دهد.

راهکارهایی برای بهبود مشکلات امنیتی USSD

زمانی‌که تصمیم می‌گیریم از USSD برای خدمات بانک‌داری استفاده کنیم، راهکارهای مختصری برای بهبود مشکلات امنیتی این فناوری در اختیارمان قرار دارد. از جمله راهکارهایی که قابلیت‌های امنیتی USSD را بهبود می‌بخشند به موارد زیر می‌توان اشاره کرد:
نمایش اطلاعات محرمانه در زمان استعلام وضعیت مالی: شماره حساب و پین‌موبایل به همان شکلی که هستند نشان داده می‌شوند که ناظر بر تراکنش‌ها ممکن است به سوء استفاده از اطلاعات بپردازد. برای حل این مشکل در زمان ورود پین‌موبایل توسط کاربر، باید به جای نمایش کدها، کاراکتر ستاره نشان داده شود و برای شماره حساب نیز تنها 4 رقم آخر نشان داده شود.
نمایش اطلاعات محرمانه در زمان انتقال پول توسط شناسه مبادلات پولی همراه (MMID :USSD ورودی MMID را بدون هیچ‌گونه تغییری نشان می‌دهد که اجازه می‌دهد ناظر بر اجرای تراکنش‌ها اطلاعات فوق را مشاهده کرده و از آن‌ها سوء استفاده کند. برای حل این مشکل در زمان ورود MMID توسط کاربر باید از کاراکترهای ستاره به جای کاراکترهای واقعی استفاده شود.
همچنین، در زمان درخواست نمایش MMID، اطلاعات باید پس از آن‌که شماره موبایل اعتبارسنجی شدند نشان داده شوند. بهتر است اعتبارسنجی با فاکتورهای دیگری نیز انجام شود که اگر گوشی کاربر به سرقت رفته بود، سارق به راحتی نتواند از اطلاعات
سوء استفاده کند.
تولید رمز یکبارمصرف غیرمجاز و تایید نشده: در زمان تولید رمزیکبار مصرف (OTP) علاوه بر شماره تلفن کاربر و MMID باید از جزییات دیگر کارت‌های اعتباری یا بانکی استفاده شود تا در صورت سرقت گوشی کاربر، تولید کد OTP امکان‌پذیر نشود.
ویرایش درخواست‌ها و پاسخ‌های USSD با هدف پیاده‌سازی حملات بازپخشی یا محروم‌سازی از سرویس: ورودی‌های حساس کاربر همچون پین‌موبایل، شماره تلفن، شماره حساب و MMID ممکن است با هدف پیاده‌سازی حملات محروم‌سازی از سرویس یا بازپخشی یا انتقال پول برای یک گیرنده ناشناس استفاده شوند. برای پیشگیری از وقوع این حملات باید پیام‌ها از برچسب زمانی که نقش کلید رمزنگاری را دارند استفاده کنند. برچسب زمانی می‌تواند درخواست‌ها یا پاسخ‌هایی که بازپخش شده‌اند را بی اعتبار کند.
تاخیر در پاسخ‌هایUSSD که باعث دستکاری اطلاعات می‌شوند: بستن تمامی نشست‌های باز در زمان خروج مانع از آن می‌شود تا شناسه نشست‌های باز دومرتبه استفاده شوند. همچنین باید نظارت دقیقی روی تمامی اعتبارسنجی‌ها و خطاهای داده‌ای که هم در سمت کلاینت و هم در سمت سرور رخ می‌دهد انجام شود

تاریخ انتشار:

23 مهر 1398

نشانی منبع:
https://www.shabakeh-mag.com/security/16157/ussd-%DA%86%DB%8C%D8%B3%D8%AA-%D9%88-%D8%AE%D8%B7%D8%B1%D8%A7%D8%AA-%D8%A7%D9%85%D9%86%DB%8C%D8%AA%DB%8C-%D8%A2%D9%86-%DA%A9%D8%AF%D8%A7%D9%85%D9%86%D8%AF%D8%9F