بسمه تعالی

ارزیابی امنیتی پروتکل Diameter در شبکه‌های تلکام

گزارش نتایج ارزیابی

شناسه سند ..... TR_DiameterNetworksThreats _13990119

نوع سند ..... گزارش فنی

شماره نگارش ۱/۰

تاریخ نگارش ۱۳۹۹/۰۱/۱۹

طبقه‌بندی سند ..... **عادی**

شاهرود، میدان هفت تیر، بلوار دانشگاه، دانشگاه صنعتی شاهرود، مرکز تخصصی آپا، کد پستی: ۳۶۱۹۹۹۵۱۶۱

(۰۲۳) ۲۲۰۴-۳۲۳۹ (۰۲۳) ۰۲۵۱-۳۲۳۰ cert.shahroodut.ac.ir

فهرست مطالب

۱ مقدمه ۱
۲ اصول و روش‌ها ۱
۳ نمای کلی تهدیدات Diameter ۳
۴ منشاء آسیب‌پذیری ۵
۵ حمله منع سرویس ۶
۶ افشای موقعیت مکانی مشترکان ۸
۷ افشای اطلاعات مشترکان ۸
۸ افشای اطلاعات شبکه ۹
۹ جمع‌بندی ۹
۱۰ اقدامات پیشنهادی به اپراتورها ۹
۱۱ مراجع ۱۰

۱ مقدمه

امروزه تصور زندگی بدون ارتباطات از راه دور مشکل است؛ با توجه به اینکه اینترنت اشیاء به طور گسترده در فرآیندهای صنعتی و و زیرساخت‌های شهری گسترش می‌یابد، اختلال در شبکه موبایل می‌تواند آن‌ها را فلج کند؛ و علاوه بر وقفه‌های اتفاقی در خانه‌های هوشمند یا دستگاه‌های اتومبیل، باعث وقایع بحرانی مانند افت ترافیک، قطع برق و در نهایت نارضایتی مشتریان اپراتورها شود.

سرویس 4G یا همان LTE علاوه بر سرعت بالا دارای خطرات امنیتی زیادی است. در واقع LTE نسخه جدیدتر شبکه تلفن همراه پس از GSM است، که بسیاری از مشکلات GSM در آن بهبود یافته‌اند. در هر حال نقاط ضعف امنیتی زیادی در شبکه‌های LTE توسط محققان در سال‌های اخیر کشف شده است؛ این ضعف‌ها به مهاجمان امکان می‌دهد به اطلاعات مشترکان دسترسی پیدا کرده، آن‌ها را تغییر دهند یا کاربران را به سایت‌های مخرب یا فیشینگ هدایت کنند.

شبکه‌های 4G از پروتکل Diameter signaling[۱] استفاده می‌کنند، که مانند SS7 (پروتکل سیگنالینگ[۲] سیستم) حاوی نقص‌های امنیتی هستند. این پروتکل برای تأیید اعتبار و مجوز پیام‌ها و توزیع اطلاعات در شبکه‌های 4G استفاده می‌شود. در واقع آسیب‌پذیری‌ها در پروتکل Diameter به مهاجمان اجازه می‌دهد حملاتی را تقریباً در همان محدوده روی مشترکین و اپراتورهای موبایل مانند شبکه‌های نسل قبلی اعمال کنند. با توجه به اینکه مردم نسبت به گذشته بیشتر به شبکه‌ها وابسته هستند، امنیت سایبری قوی برای همه اپراتورهای تلفن همراه بسیار مهم است. در این مقاله وضعیت فعلی حفاظت شبکه‌های موبایلی و پیامدهای امنیت شبکه‌های نوظهور 5G را مورد بررسی قرار می‌دهیم.

۲ اصول و روش‌ها

پروتکل سیگنالینگ سیستم (SS7) برای تبادل داده بین دستگاه‌های شبکه در شبکه‌های ارتباطی استفاده می‌شود. هنگامی که استاندارد SS7 تدوین شد، فقط اپراتورهای خط ثابت به این شبکه دسترسی داشتند؛

---

[۱] پروتکل Diameter، پروتکلی به منظور احراز هویت، مجوز کنترل دسترسی و حسابداری (AAA) برای شبکه‌های رایانه‌ای است. این پروتکل، تکامل یافته‌ی پروتکل RADIUS و متعلق به پروتکل‌های لایه اپلیکیشن در مجموعه پروتکل اینترنت است.

[۲] پروتکل signaling نوعی پروتکل است که برای تلفیق داده‌های سیگنالینگ استفاده می‌شود. همچنین برای شناسایی وضعیت اتصال بین تلفن‌ها یا پایانه‌های VOIP (تلفن IP یا رایانه‌های شخصی یا واحدهایVoWLA) نیز استفاده می‌شود.

بنابراین امنیت آن از اهمیت زیادی برخوردار نبود. اما امروزه این شبکه منزوی نیست و به مهاجمان امکان می‌دهد از نقص‌های آن سوءاستفاده کرده، تماس و پیام کوتاه را قطع کند، سیستم پرداخت را دور بزند، از حساب‌های موبایلی سرقت کند و یا بر عملکرد شبکه تلفن همراه تاثیر بگذارد.

اگرچه امروزه شبکه‌های 4G جدید از پروتکل Diameter signaling استفاده می‌کنند، اما مسائل امنیتی SS7 همچنان پابرجاست؛ زیرا اپراتورهای تلفن همراه باید از پشتیبانی 2G و 3G و تعامل بین نسل‌های مختلف شبکه اطمینان حاصل کنند. علاوه بر این، تحقیقات نشان می‌دهد پروتکل Diameter مستعد تهدیدهای مشابه است. امروزه اپراتورهای تلفن همراه مسائل امنیتی SS7 را جدی‌تر تلقی کرده و تکنیک‌های محافظتی را پیاده‌سازی می‌کنند.

برای ارزیابی امنیت SS7، پروتکل Diameter و شبکه‌های GTP، کارشناسان اقدامات مهاجمانی که از شبکه خانگی یا خارجی استفاده می‌کنند را شبیه‌سازی می‌کنند. در صورتی که اپراتور اقدامات حفاظتی مناسب را انجام ندهد، مهاجمان می‌توانند درخواست‌های پروتکل لایه اپلیکیشن را به شبکه اپراتور بفرستند و گستره وسیعی از تهدیدات را هدایت کنند.

شبکه‌های سیگنالینگ، اپراتورهای شبکه تلفن همراه (MNO) در سراسر جهان را متحد می‌کند و افراد، مشاغل و دستگاه‌های هوشمند IoT را به یک اکوسیستم یکپارچه موبایل پیوند می‌دهند. این اکوسیستم برای حفظ ارتباطات مطمئن و ایمن، به عملکرد ارائه‌دهندگان خدمات بستگی دارد. با این حال، نقص‌های اساسی در پروتکل‌های سیگنالینگ (SS7، Diameter، GTP) و خطاهای پیکربندی تجهیزات شبکه، آن‌ها را در معرض تهدیدهای شدید امنیتی زیر قرار می‌دهد:

- حمله منع سرویس شبکه (DoS)
- نقض حریم خصوصی: شنود تماس صوتی، پیام کوتاه و داده‌ها، ردیابی موقعیت مشترکان
- کلاه‌برداری سیگنالینگ

علاوه بر این، همگرایی نسل‌های مختلف تکنولوژی (مانند 3G، 4G و حتی 5G به طور بالقوه) آسیب‌پذیری‌های جدید و حمله‌هایی با استفاده از چند پروتکل را به ارمغان می‌آورد.

با وجود اقدامات حفاظتی کافی، همه شبکه‌ها در معرض آسیب‌پذیری‌های ناشی از تنظیم نادرست تجهیزات یا نقص‌های موجود در ساختار SS7 که با ابزارهای موجود قابل حل نیستند، وجود دارند. برای حل این مسئله، رویکرد جامعی که ترکیبی از تحلیل امنیتی، ایستایی وضعیت شبکه، نظارت منظم بر ترافیک سیگنالینگ و تشخیص به موقع فعالیت‌های غیرمجاز است، امنیت بیشتری در برابر مجرمان ایجاد خواهد کرد.

سطح آگاهی اپراتورها از امنیت SS7 رو به افزایش است، به همین دلیل آن‌ها تکنیک‌های محافظتی را اجرا می‌کنند. در سال ۲۰۱۵، شبکه‌ها مستعد انواع تهدیدات بودند؛ اما طی سال‌های اخیر روند مثبتی در امنیت

این شبکه‌ها مشاهده شده است. این گزارش نتایج ارزیابی‌های امنیتی انجام شده در طول دوره زمانی ۲۰۱۸-۲۰۱۹ از طرف ۲۸ اپراتور مخابراتی در اروپا، آسیا، آفریقا و آمریکای جنوبی را نشان می‌دهد. همچنین به بررسی وضعیت شبکه‌های Diameter می‌پردازد.

۳ نمای کلی تهدیدات Diameter

در دو سال گذشته پیشرفت زیادی در امنیت شبکه‌های Diameter اتفاق نیفتاده است. بزرگترین تهدید (که در تمام شبکه‌های تلفن همراه مورد آزمایش شناسایی شده است) حمله منع سرویس[۳] بود.

این حملات بر کاربران شبکه‌های 4G و 5G تاثیر می‌گذارد. اولین نسل شبکه‌های 5G (5G غیر مستقل) مبتنی بر هسته‌ی شبکه LTE است درنتیجه 5G کلیه آسیب‌پذیری‌های موجود در LTE را به ارث می‌برد. مانند ردیابی موقعیت مکانی کاربر، به دست آوردن اطلاعات حساس و در برخی موارد انتقال مشترکان به شبکه‌های 3G و ناامن کردن این شبکه‌ها. سایر آسیب‌پذیری‌های موجود در پروتکل Diameter به این معناست که عاملان خارجی می‌توانند مکان مشترکان را ردیابی کرده و اطلاعات حساس مشترک را که می‌توانند از آن برای شنود تماس صوتی استفاده کنند، بدست آورند و از محدودیت‌های موجود در خدمات تلفن همراه استفاده کنند. بنابراین اولین قدم محافظت از مشترکان 5G باید بهبود امنیت شبکه‌های 4G باشد.

به طور کلی تهدیداتی که با استفاده از بهره‌برداری از نقص‌های امنیتی در شبکه‌های تلفن همراه اتفاق می‌افتند شامل موارد زیر است:

- افشای اطلاعات مشترکان
- افشای اطلاعات شبکه
- شنود ترافیک مشترکان
- کلاه‌برداری
- حمله منع سرویس
- افشای موقعیت مکانی مشترکان

میزان برخی از این تهدیدات در سال‌های اخیر در جدول شماره ۱ بررسی شده است:

[۳] denial of service

تهدیدات	۲۰۱۷	۲۰۱۸	۲۰۱۹
افشای اطلاعات مشترکان	۱۰۰٪	۱۰۰٪	۱۰۰٪
افشای موقعیت مکانی مشترکان	۱۰۰٪	۱۰۰٪	۷۵٪
حمله منع سرویس	۱۰۰٪	۱۰۰٪	۱۰۰٪
افشای اطلاعات شبکه	۷۵٪	۱۰۰٪	۱۰۰٪

جدول شماره ۱ : درصد شبکه‌های Diameter آسیب‌دیده توسط یک تهدید خاص

افشای اطلاعات مشترکان به معنای نشت IMSI[۴]، افشای موقعیت مکانی مشترکان یا سایر داده‌ها مانند مانده حساب یا مشخصات پروفایل مشترکان است. افشای اطلاعات شبکه ناشی از نشت داده‌های پیکربندی شبکه SS7 است. روش‌های خاص شنود ترافیک مشترکان به مهاجم امکان می‌دهد تا در تماس‌های تلفنی اختلال ایجاد کرده یا آن‌ها را به تماس دیگری هدایت کند و همچنین پیام‌های کوتاه کاربر را شنود کند.

همه تهدیدات ذکر شده خطرات مالی و اعتباری برای اپراتورها به وجود می‌آورند. کلاه‌برداری، شنود ترافیک و حمله منع سرویس به طور مستقیم بر مشترکان تاثیر گذاشته و ممکن است منجر به خسارات مالی قابل توجه، نقض حریم خصوصی و اختلال در دسترس بودن مشترکان شود. طبق تحقیقات در سال ۲۰۱۸، یک سوم شبکه‌ها در برابر کلاه‌برداری‌ها آسیب‌پذیر بوده‌اند. مهاجمان می‌توانند به منظور استفاده رایگان از خدمات ارتباطی در شبکه‌های Diameter، محدودیت‌ها را بردارند. در گزارش امسال آمار مربوط به کلاه‌برداری حذف شده است زیرا تقریباً همه شبکه‌های آزمایش‌شده از مکانیزم‌هایی که با استفاده از روش‌های شناخته شده مورد حمله قرار می‌گیرند، پشتیبانی نمی‌کنند یا این آزمایشات خارج از محدوده آزمایش می‌باشد. در این نمونه‌ها هنگامی که آزمایشات مربوط به کلاه‌برداری انجام شد، مهاجمان قادر به دور زدن محدودیت‌های مربوط به اپراتور هستند و از خدمات حتی زمانی که چنین خدماتی در برنامه نرخ مشترکان گنجانده نشده است، استفاده می‌کنند.

روش‌هایی برای جلوگیری از شنود پیام کوتاه در شبکه‌های Diameter وجود دارد؛ اما پیاده‌سازی آن‌ها در آزمایشات مشکل است. اکثر اپراتورها هنوز پیام‌های کوتاه را از طریق 4G انتقال نمی‌دهند. درعوض، دستگاه‌های مشترکان به شبکه 3G تغییر می‌یابد و به مسائل امنیتی SS7 آسیب‌پذیر می‌شوند. در سال

[۴] یک شماره شناسایی منحصر به فرد جهانی است که درون سیم‌کارت ذخیره می‌شود. این شماره ۱۵ رقمی به منظور شناسایی دستگاه در سامانه جهانی ارتباطات (GSM) استفاده می‌شود.

۲۰۱۹، ۸۶ درصد از شبکه‌های SS7 به شنود پیام کوتاه آسیب‌پذیر بوده‌اند. همچنین تنها یکی از سه فناوری موجود برای انتقال پیام‌های کوتاه در شبکه‌های 4G از پروتکل Diameter استفاده می‌کند.

شبکه‌های 4G از پروتکل SIP[۵] برای تماس‌های صوتی استفاده می‌کنند. این تماس‌ها می‌توانند در ۵۸ درصد از شبکه‌های آزمایش شده SS7 شنود شوند.

۴ منشاء آسیب‌پذیری

ارزیابی امنیتی خارجی، نقص‌های ساختاری را در Diameter آشکار کرده است. شبکه‌ها مکان واقعی مشترکان را بررسی نمی‌کنند یا شبکه مبداء پیام‌های سیگنالینگ برای مشترکان را تایید نمی‌کند.

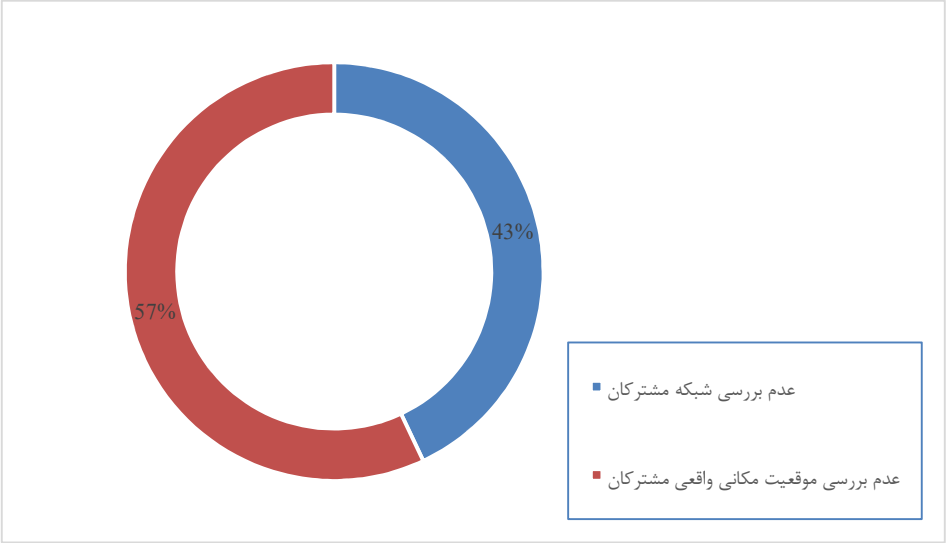
شبکه‌های اپراتور می‌توانند پیام‌های سیگنالینگ را به مشترکان رومینگ[۶] (پیام‌های سیگنالینگ نسل دوم GSMA) ارسال کنند. اگر آدرس مبداء و IMSI مشترکان با همان اپراتور مطابقت داشته باشند، بنابراین آن شبکه، شبکهٔ خانگی مشترک مورد نظر است. با این حال آدرس منبع می‌تواند در طول انتقال اصلاح شود، بنابراین می‌توان با اطمینان تشخیص داد که ترافیک سیگنالینگ فقط در صورتی که ترافیک از یک شبکه خارجی به مشترکین خود اپراتور ارسال شود، جعلی است.

خطا در تشخیص موقعیت مکانی واقعی مشترکین مربوط به پیام‌های سیگنالینگ نسل سوم GSMA است که از شبکه رومینگ به شبکه‌های خانگی اپراتور فرستاده می‌شوند. از آنجایی که در هر شبکه‌ای مشترک رومینگ می‌تواند چنین درخواست‌هایی را به شبکه خانگی مشترک ارسال کند، تعیین مجاز بودن پیام فقط بر اساس پارامترهای آن غیرممکن است؛ به همین دلیل اپراتورها باید بررسی کنند که آیا مشترک در واقع در شبکه در حال رومینگ است و درخواست‌های جدید را در برابر داده‌های موقعیت مکانی قبلی ارجاع می‌دهد یا خیر. حملات پیشخوان که از این نقص‌ها بهره‌برداری می‌کنند، نیاز به نظارت مداوم و تحلیل دقیق ترافیک سیگنالینگ دارند. در شکل شماره ۱ حملات موفقی که از آسیب‌پذیری‌های عدم بررسی شبکه و موقعیت مکانی مشترکان استفاده می‌کنند، بررسی شده است.

---

[۵] یک پروتکل سیگنالینگ ارتباطی است که به صورت گسترده برای کنترل session های ارتباطات چندرسانه‌ای مورد استفاده قرار می‌گیرد. از SIP در کنترل ارتباطاتی همچون انتقال صدا و ویدئو بر روی شبکه‌های IP استفاده می‌شود. پروتکل SIP کنترل شروع، تغییر و پایان session را انجام می‌دهد.

[۶] راهی برای دریافت اطلاعات و سیگنال در خارج از کشور یا در مناطقی که اپراتور پوشش دهی ندارد.



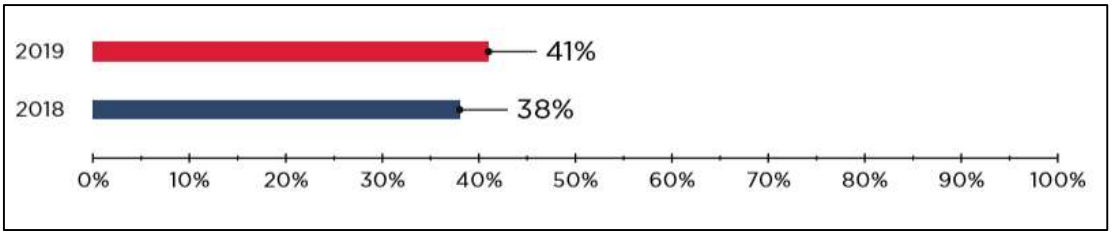
شکل شماره ۱ : آسیب‌پذیری‌هایی که باعث حمله می‌شوند (درصد حملات موفق)

۵ حمله منع سرویس

هنگام انتخاب یک اپراتور موبایل، مشترکان به مسائلی به جز قیمت فکر می‌کنند. آن‌ها 4G را با استاندارد خاصی از خدمات با کیفیت و پهنای باند بالا مرتبط می‌کنند. تحقیقات در مورد Diameter نشان می‌دهد بزرگترین تهدید برای کاربران 4G حمله منع سرویس است؛ اکثر این شبکه‌ها مستعد حملات منع سرویس بوده و شبکه‌های 5G نیز از این حملات مصون نیستند. اختلال عملکرد در شبکه‌های 4G ممکن است باعث رویگردانی مشترکان شود. مصرف‌کننده‌های اصلی سرویس‌های ارتباطی دیگر افراد نیستند، بلکه دستگاه‌های اینترنت اشیاء هستند. این دستگاه‌ها به خرابی در شبکه‌های موبایل حساس هستند: سیستم هشدار که در حین شرایط ضروری فعال نمی‌شود، سنسورهای صنعتی که آفلاین می‌شوند، سیستم‌های شهر هوشمند که دیگر نمی‌توانند ارتباط برقرار کنند؛ همه این موارد عواقب بالقوه بسیار بیشتری از کاهش سرعت اینترنت برای کاربران خانگی دارد.

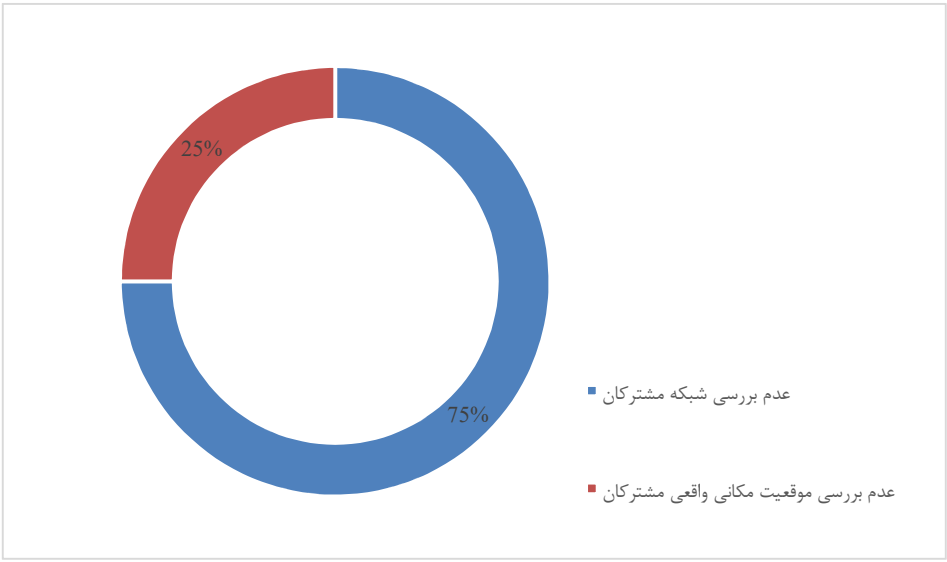
در این گزارش حمله منع سرویس فقط در مشترکان شخصی در نظر گرفته می‌شود؛ زیرا تنها تعداد اندکی از اپراتورها می‌توانند عناصر شبکه‌ای که منجر به اختلال در عملکرد شبکه تلفن همراه می‌شوند را مورد آزمایش قرار دهند. نرخ پایین موفقیت مهاجمان به این معنا نیست که اپراتورها تلاش می‌کنند که از خود محافظت کنند؛ زیرا آن‌ها چنین عملکردی را در شبکه‌های خود نداشتند. بسیاری از روش‌های ارائه شده در شبکه‌هایی که فاقد سازوکارهای مدرن هستند بی‌استفاده خواهند بود؛ مانند پیامک در MME و صوت در LTE (VoLTE). در شبکه‌هایی که از VoLTE برای تماس‌های صوتی استفاده می‌کنند، آزمایش‌کنندگان می‌توانند مشترکان را به 3G انتقال داده و خدمات را کاهش دهند. و حتی در شبکه‌هایی بدون این عملکرد،

دستگاه‌های اپراتور ممکن است پیام‌های دریافتی را به طور نادرست دستکاری کنند. شکل شماره ۲ درصد حملات موفقیت‌آمیز منع سرویس را نشان می‌دهد.



شکل شماره ۲ : درصد حملات موفقیت‌آمیز DoS

حملات آزمایشی باعث شده است ایجاد اتصالات کاهش یافته یا بطور قابل توجه‌ای کندتر شود، که این امر مشترکان را از استفاده از اینترنت بازمی‌دارد. در بعضی موارد، دستگاه مشترکان مجدداً در حالت 3G متصل می‌شود. امروزه اپراتورها اقداماتی را انجام می‌دهند که خطر افشای اطلاعات شبکه و مشترکان را کاهش می‌دهد، زیرا این داده‌ها مبنای حملات بعدی هستند. در حقیقت، دفاع در برابر چنین حملاتی چندان سخت نیست و بازار امنیت اطلاعات راه‌حلهایی را برای حفاظت اطلاعات ارائه می‌دهد. هنوز صد درصد شبکه‌ها نسبت به آن‌ها آسیب‌پذیر هستند و این نشان‌دهنده ناکارآمدی راه‌حل‌های فعلی است. در شکل شماره ۳ حملات موفق منع سرویس که از آسیب‌پذیری‌های عدم بررسی شبکه و موقعیت مکانی مشترکان استفاده می‌کنند، بررسی شده است.



شکل شماره ۳ : آسیب‌پذیری‌هایی که باعث حملات منع سرویس می‌شوند (درصد حملات موفق)

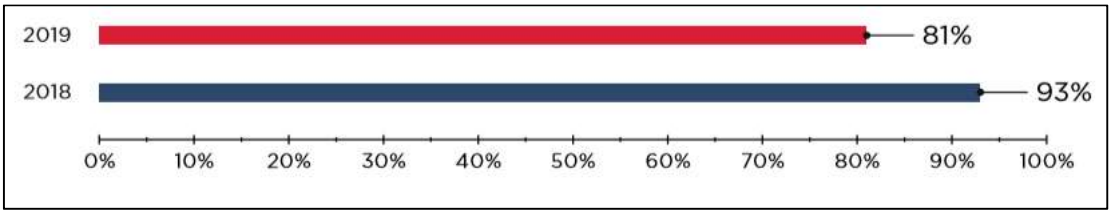
۶ افشای موقعیت مکانی مشترکان

موقعیت مکانی مشترکان می‌تواند در ۸۹ درصد نمونه‌ها ردیابی شود. بدین منظور از جعل هویت کاربر رومینگ برای ارسال پیام سیگنالینگ با درخواست موقعیت مکانی مشترکان استفاده می‌شود. همانطور که در بخش چهارم گزارش ذکر شد، شبکه‌ها فقط در صورتی که پیام، خطاب به مشترک آن کاربر رومینگ باشد، باید پاسخی را برگردانند. اما تعیین این امر غیرممکن است؛ زیرا کاری که اپراتور می‌تواند انجام دهد، مسدود کردن پیام‌هایی است که از یک شبکه خارجی به مشترکان اپراتور ارسال می‌شود. متاسفانه اپراتورها نمی‌توانند این بررسی‌ها را انجام دهند. فقط یک شبکه با وجود پیکربندی eGLR (ثبت موقعیت مکانی Gateway) در لبه شبکه، به چنین پیام‌هایی پاسخ نمی‌دهد.

۷ افشای اطلاعات مشترکان

مهاجمان می‌توانند از پروفایل‌های مشترکان استفاده‌های زیادی کنند؛ مانند به دست آوردن شماره موبایل، وضعیت دستگاه موبایل و پیکربندی APN (نقطه دسترسی). همچنین پروفایل مشترکان پارامترهای صورتحساب و محدودیت‌های خدمات تلفن همراه را ذخیره می‌کند. این اطلاعات توسط مهاجمان به منظور اهداف کلاه‌برداری قابل تغییر است.

علاوه بر این یک مهاجم می‌تواند به کلیدهای احراز هویت مشترکان دسترسی پیدا کرده و از آن‌ها برای ایجاد یک ایستگاه پایه استفاده کند. یک ایستگاه پایه جعلی به مهاجمان امکان می‌دهد که IMSIهای مشترکان را به دست آورده، تماس‌های صوتی خروجی را شنود کرده و حملات منع سرویس را انجام دهند. در شکل شماره ۴ میزان حملاتی که از افشای اطلاعات پروفایل مشترکان استفاده می‌کنند بررسی شده است.



شکل شماره ۴ : درصد حملات موفقیت‌آمیز که با استفاده از اطلاعات از پروفایل مشترکان انجام شده است.

در بیشتر نمونه‌ها، آزمایش‌کنندگان با موفقیت به پروفایل‌های مشترکان دسترسی پیدا کردند. همان طور که گفته شد، دلیل این مسئله این است که شبکه‌های اپراتور از دریافت موقعیت مکانی واقعی مشترک در هنگام دریافت ترافیک سیگنالینگ از یک شبکه خارجی غفلت می‌کنند. با این حال، راه دیگری برای تشخیص یک پیام جعلی از پیام صحیح وجود ندارد. فیلتر کردن صحیح پیام‌های دریافتی، از جمله ارجاع متقابل موقعیت

مکانی مشترکان، می‌تواند از افشای اطلاعات شبکه اپراتور و مشترکان جلوگیری کند؛ این به نوبه خود، مانع از حملات پیچیده‌تر می‌شود.

۸ افشای اطلاعات شبکه

مهاجمان برای انجام حملات پیچیده‌تر، نیاز به اطلاعاتی در مورد شبکه اپراتور دارند. به طور مثال برای ایجاد حمله منع سرویس، مهاجمان باید آدرس عناصر شبکه را بدانند. کلیه حملات مورد آزمایش در آزمایش‌های خارجی در به دست آوردن اطلاعات در مورد تجهیزات شبکه موفقیت‌آمیز بودند. تفکیک کردن پیام‌های جعلی استفاده شده در حملات از پیام صحیح بسیار دشوار است. فیلتر کردن چنین پیام‌هایی نیاز به این مسئله دارد که اپراتور موقعیت مکانی مشترکان را تایید کرده و هر پیام دریافت شده را با پیام‌های قبلی به منظور تعیین اینکه آیا مشترک در واقع در شبکه‌ای است که درخواست از آن منشا گرفته است یا خیر، ارجاع متقابل دهد. امروزه تجهیزات اپراتورها اجازه انجام چنین تحلیلی از ترافیک را نمی‌دهد.

۹ جمع‌بندی

پروتکل Diameter آسیب‌پذیری‌هایی دارد که به مهاجمان اجازه می‌دهد موقعیت مکانی مشترکان را ردیابی کنند، اطلاعات حساس شبکه اپراتور و مشترکان را به دست آورند و محدودیت‌های اپراتور در استفاده از خدمات موبایلی را دور بزنند. بعضی از روش‌ها، باعث می‌شوند که مشترکان به 3G ناامن متصل شوند.

کلیه شبکه‌های آزمایش شده نسبت به حمله منع سرویس آسیب‌پذیر بوده‌اند، که تهدید مستقیمی برای دستگاه‌های IoT است.

شبکه‌های 5G در حال حاضر ساختار غیر مستقلی دارند، که مبتنی بر 4G است. بنابراین مشترکانی که بهبود امنیت را از مزایای شبکه 5G به شمار می‌آورند، هنوز هم در برابر تهدیدات مربوط به شبکه‌های 4G آسیب‌پذیر هستند.

۱۰ اقدامات پیشنهادی به اپراتورها

امنیت باید در طول طراحی شبکه اولویت باشد. این مسئله اکنون بیش از هر زمان دیگری واقعیت دارد، زیرا اپراتورها شروع به مقابله با ساخت شبکه‌های 5G می‌کنند. تلاش برای اجرای امنیت در مراحل بعدی ممکن است هزینه‌های بیشتری داشته باشد: در بهترین حالت، اپراتورها به احتمال زیاد نیاز به خرید تجهیزات

اضافی دارند، در بدترین حالت، ممکن است اپراتورها با آسیب‌پذیری‌های امنیتی دراز مدت که بعداً برطرف نمی‌شوند درگیر شوند.

ترافیک سیگنالینگ باید هنگام عبور از لبه شبکه کنترل و تحلیل شود. این خطرات تهدیدات و خطاهای پیکربندی را شناسایی می‌کند، این نظارت‌ها با رهنمودهای GSMA تقویت می‌شود. برای اجرای این امر، اپراتورها باید از سیستم‌های شناسایی تهدید ویژه استفاده کنند که بتوانند ترافیک سیگنال را در زمان واقعی تحلیل کرده و فعالیت غیرمجاز را توسط میزبان‌های خارجی تشخیص دهند. این راه‌حل‌ها بدون تأثیرگذاری بر عملکرد شبکه یا در دسترس بودن مشترکان، پیام‌های غیرمجاز را مسدود می‌کنند. آن‌ها همچنین برای افزایش کارآیی می‌توانند اطلاعات را به سایر سیستم‌های محافظت انتقال دهند.

۱۱ مراجع

[1] https://positive-tech.com/research/diameter-2020/

[2] https://positive-tech.com/research/ss7-vulnerability-2018/

[3] https://positive-tech.com/products/signalling-firewall/

[4] https://positive-tech.com/services/express-monitoring/

[5] https://positive-tech.com/storage/services/express-monitoring/PT-AG-Express-Monitoring-eng.pdf