禪

آسیبپذیریهای مستتر در شبکههای فوق سریع

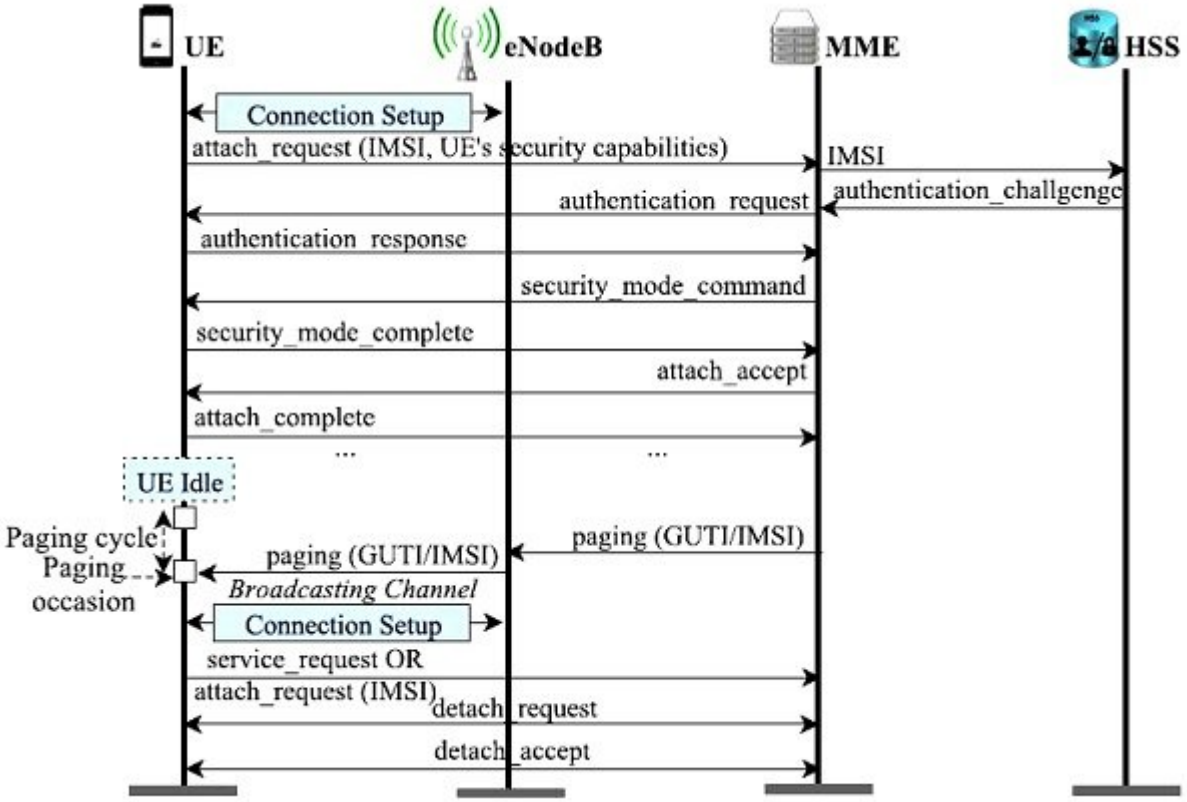
نقصهای امنیتی شبکههای 4G و 5G و مشکلات ناشی از آنها

4G
5G

در سالهای اخیر با توجه به مقبولیت شبکههای نسل چهارم LTE، شاهد رشد قابل توجه این نوع شبکهها بودهایم . نسل چهارم به سرعت جانشین نسل سوم شد و اکنون دیگر جزئی جداناپذیر در زندگی مردم، تجارت و امنیت است. به همین دلیل، این شبکهها گزینه جذابی برای هکرها و افراد بدخواه به شمار میروند . با حملات جدید کشف شده در شبکههای نسل چهارم LTE، مشخص شد هکرها قادر به جاسوسی، پیگیری کردن و شنود خواهند بود . برخی این حملات میتواند در شبکههای نسل پنجم نیز وجود داشته باشد .

حملات کشف شده در 4G LTE

محققان حوزه امنیت، مجموعهای از آسیبپذیریها را در پروتکلهای 4G LTE کشف کردهاند که خطرات بزرگی به دنبال دارد . از جمله : به سرقت بردن تماسها و پیامهای متنی کاربران، ارسال پیام اعلام خطر جعلی و جاسوسی از موقعیت مکانی دستگاه. بر اساس یکی از مقالههایی که به تازگی در دانشگاههای Purdue و Lowa منتشر شده است، جزییات 10 حمله ممکن به ترمینالهای داده و دستگاههای موبایل در شبکههای 4G LTE بررسی شده است. این حملهها ضعفهای طراحی روی سه پروتکل کلیدی را نشان میدهد که به عنوان پیوست □□□□(attach)، جدا □□□□(detach) و □□□□□□□□□(paging) شناخته میشوند. attach رویهای است که دستگاه کاربر را به شبکه متصل میکند؛ مثلا زمانی که دستگاه خاموش، روشن میشود . detach زمانی اتفاق میافتد که دستگاه خاموش میشود یا ارتباطش به علت تضعیف سیگنال با شبکه قطع میشود. paging بخشی از ایجاد تماس است؛ دستگاه را مجبور میکند تا اطلاعات سیستمی را دوباره کسب کند و همچنین برای پیغامهای اضطراری بهکار گرفته میشود . جزییات دقیق از این سه رویه را در شکل 1 مشاهده میکنید .



paging و attach و detach نمودار -1شکل

شکل ۱ (Mobility Management Entity شکل) MME . شکل شکل شکلشکل eNodB و شکلشکل شکلشکل UE شکلشکل شکلشکل شکل شکل ش

محیط تست، اجرا میشود. حملات شناسایی شده که میتواند در شبکه LTE اجرا شوند، به این صورت هستند :

1.حمله ناتوانی در همگامسازی تصدیق
Authentication Synchronization Failure))
2.حمله ردیابی Traceability))
3.حمله Numb))
4.حمله رله تصدیق Authentication Relay))
5.حمله جداسازی/ تنزل Detach/Downgrade))
6.حمله سرقت کانال صفحهبندی Paging Channel Hijacking))
7.حمله آغاز سرقت Stealthy Kicking-off))
8.حمله Panic
9.حمله کاهش انرژی Energy Depletion))
10. حمله قابلیت پیوند (linkability)

در بین حملات بالا، محققان حمله رله تصدیق را ترسناکتر میدانند که به حملهکننده اجازه میدهد با جعل شماره تلفن قربانی، به شبکه LTE وصل شود. جزییات این حمله در شکل 3 نشان داده شده است. با این حمله، هکر نه تنها توانایی خواندن پیامهای ورودی و خروجی قربانی را دارد، بلکه میتواند شخص دیگری را مجرم نشان دهد و شواهد جعلی از خود به جای بگذارد .

Malicious UE
Victim UE
IMSI, K, SQN
Malicious eNodeB
MME
HSS
S = {s|∀i ∈ I} where s = (i, K, SQN)
paging (IMSI) or detach_request
attach_request (IMSI, UE Network capabilities)
attach_request (IMSI, UE Network capabilities)
IMSI
RAND, AUTN, XRES, CK, IK (SQN = n)
authentication_request (RAND, AUTN) for SQN = n
(authentication_request (RAND, AUTN) for SQN = n
authentication_response (SRES_SQN=n)
MME waiting for response from malicious UE
authentication_response (SRES_SQN=n)
Verify: SRES_SQN=n = XRES_SQN=n
...
...
attach_complete
attach_complete

شکل **3-** حمله رله تصدیق

حمله دیگری که در این گزارش بیشتر روی آنها تأکید شده، linkability است که طی آن حملهکننده قادر به کسب اطلاعات کلی در مورد موقعیت قربانی است. در حمله panic با پخش همگانی پیامهای اضطراری ساختگی و غلط، آشفتگی و بینظمی به وجود میآید . همچنین در حمله detach هکر از حمله DoS استفاده میکند و دستگاه را آفلاین میکند . در قسمتی از مقاله نوشته شده است:«با استفاده از LTEInspector متوجه شدیم که با یک حمله، میتوان کانال paging یک دستگاه موبایلی را سرقت کرد و علاوه بر اینکه اختلالی در اطلاعرسانی (تماس، پیامکها و ...) به وجود نمیآید، میتوان پیامهای ساختگی نیز در این بین وارد کرد .»
نکته جالب توجه اینجاست که مقابله با این حملهها تنها 1300 تا 3900 دلار هزینه در پی خواهد داشت . 4G و 5G برای بهکارگیری در شهر هوشمند، آماده نیستند .
در گزارشی دیگر، شرکت Positive Technologies خبر از نقصهای امنیتی اساسی در قسمتی از هسته شبکه 4G با نام EPC(Evolved Packet Core) داده است که مربوط به بخش داده و صدا (voice) است. ممکن است اطلاعات دستگاهها جمعآوری شود یا حمله DoS اتفاق افتد .
اگر یک شهر هوشمند را در نظر بگیریم، آسیبپذیریهای کشف شده در بسیاری از بخشها وجود خواهد داشت؛ در چراغهای هوشمند ترافیک، لامپهای خیابانها، علامتهای الکترونیکی در جادهها، نمایشگر اطلاعات در ایستگاههای اتوبوس و بسیاری دیگر از عناصر شهر هوشمند که به شبکههای نسل چهارم متصل هستند. Positive Technologies این نقصها را آشکار کرده و تأکید کرده که در شبکههای نسل پنجم هم وجود خواهند

داشت.

به گفته دیمیتری کورباتوف، رئیس بخش امنیتی این شرکت، آسیبپذیریهای موجود بر اساس نقصهایی در پروتکل GTP است. GTP یک پروتکل تونلینگ بر پایه IP است که برای حمل GPRS در شبکههای نسل سوم و چهارم بهکار میرود . به عبارت دیگر، زمانی که دستگاه کاربر در شبکه 4G LTE قرار داشته باشد، نودهای EPC از یک سری پروتکل مانند GTP استفاده میکند . این پروتکل خود مجموعهای از پروتکلهای ارتباطی بر اساس IP است که GPRS یا «سرویس بسته امواج رادیویی » را حمل میکنند . این کار به کاربران اجازه میدهد تا در زمان حرکت هم ارتباطشان حفظ شود .

کورباتوف اظهار داشت که حملهکننده قادر خواهد بود ارتباط تعداد زیادی از کاربران را همزمان قطع کند؛ زیرا ارتباط چند کاربر از طریق یک تونل GTP برقرار میشود . احتمال این خطر آنقدر بالا است که نگرانی در مورد آن کاملا منطقی باشد . برای ایجاد اختلال مهارت بالا و ابزارهای خاص نیاز نیست؛ تنها یک لپتاپ، یک نرمافزار رایگان برای تست نفوذ و مهارتهای پایه برنامهنویسی کافی است . قبل از 4G LTE حملهکننده به تجهیزات و دانشی عمیق از پروتکلها نیاز داشت اما به این دلیل که 4G بر اساس مفهوم یک شبکه تمام IP ساخته شده است، اکنون ابزارهایی برای هک وجود دارند که بسیاری از کارها را خودکار انجام دادهاند و به دانش چندانی در مورد ماهیت حمله نیازی نیست .

پاول نوویکوف، رئیس هیئت تحقیقاتی در Telecom Security میگوید : «بسیاری از شهرها ترافیک جادهها را با استفاده از چراغهای ترافیکی هوشمند بهینه کردهاند که این چراغها اغلب با استفاده از فناوریهای نسل چهارم با یکدیگر در ارتباط هستند . اگر چنین شبکههایی هک شوند یا تعداد کمی از آنها دچار اختلال شوند، علاوه بر ترافیک سنگین، ممکن است شاهد پیامدهای ناگواری از جمله تصادفات جادهای باشیم . پس اپراتورهای موبایل که در شهر هوشمند نقش دارند باید توجه ویژهای به این تهدیدات داشته باشند .»

آسیبپذیریهای ذکر شده در اینترنت اشیا صنعتی (IIoT)، ماشینهای بدون سرنشین و دیگر اشیا IoT متصل به شبکههای سیار وجود دارند . با تحقیقات انجام شده توسط شرکت Erricson، تعداد دستگاههای اینترنت اشیا که به شبکههای سیار متصل هستند تا سال 2022 به 1.5 میلیارد خواهند رسید . حال فرض کنید با حمله به زیرساختها در یک شهر تعداد زیادی از این دستگاهها دچار اختلال شدهاند و این به معنای از دست دادن کنترل یک شهر هوشمند است.

اما تمام بحث در مورد دستگاههای اینترنت اشیا نیست و کاربران شبکههای موبایلی نیز در معرض خطر قرار دارند؛ حملهکننده ممکن است از اطلاعات مشترکین استفاده کند و پیامها و ایمیلهای رمز نشده را به سرقت ببرد . استراق سمع از مکالمات صوتی در LTE، جمعآوری دادههایی مثل موقعیت مکانی و جلوگیری یا قطع ارتباط ترافیک اینترنت و پیامکها که مثلا با حمله DoS انجام میشود و از جمله خطراتی است که کاربران شکههای موبایلی را تهدید میکند . حملهها میتواند توسط کارکنان داخلی یک اپراتور انجام شود یا در برخی موارد توسط خود مشترکین تلفن موبایل . همچنین حملهکنندههای خارجی میتوانند به زیرساخت اپراتور دسترسی پیدا کنند . دسترسی یافتن ممکن است از کوچکترین آسیبپذیری شبکه آغاز شود یا جستجوی ▯▯▯▯▯▯(Brute-force) برای پیدا کردن رمز بهکار گرفته شود . در حمله Brute-force تمامی حالتهای ممکن تست میشود؛ یعنی با آزمون و خطا تمام عبارات ممکن را تست میکند تا در نهایت رمز صحیح وارد شود و دسترسی پیدا کند .

برای مقابله با این خطرات، Positive Technologies پیشنهاد میدهد تحلیل دقیقی از پارامترهای امنیتی انجام شود و از ارزیابیهای صورت گرفته برای مقابله با دسترسیهای غیرمجاز استفاده شود؛ احتمالا استفاده از رمزنگاری (encryption) در بیشتر مواقع کارساز است . همچنین پیشنهاد میکند که از آخرین ورژن TSL و HTTPS برای اطمینان از عدم رمزگشایی در زمان اتصال به وبسایت استفاده شود . بهکارگیری ابزارهای خاص برای نظارت مداوم، تحلیل و فیلتر کردن پیامها در شبکه باعث افزایش امنیت شبکه و مشترکین خواهد شد. بهعلاوه خود سازمانها نیز باید احتمال هر اتفاقی را در نظر گرفته و بدون توجه به امنیت شبکه، از دستگاهها، اپلیکیشنها و سرویسهایشان در لایه امنیتی خود، محافظت کنند . خطر شبکههای 4G و 5G برای کاربران همانند دیگر شبکههای بیسیم از جمله وایفای است؛ پس کاربر به اپلیکیشنهایی با پروتکلها و کانالهای انتقال امن نیاز دارد .

سخن آخر

ضعف در پیادهسازی 4G LTE و استاندارد آن، ممکن است هر کسی را در هر کجا وسوسه کند تا به دنبال هک کردن یا نظارت و کنترل بیافتد . این در حالی است که بعضی از این افراد دانش تخصصی چندانی ندارند و این نقطهضعف استانداردها را بزرگتر نشان میدهد . با توجه به نزدیک شدن به ارائه 5G توجه به این

نقاط ضعف اهمیتی دو چندان پیدا میکند؛ زیرا با فراگیر شدن اینترنت اشیا آسیبهای ناشی از این حفرههای امنیتی همواره بیشتر و بیشتر میشود .

نویسنده :
فرشاد رضایی
منبع :
مقاله : LTEInspector: A Systematic Approach for Adversarial Testing of 4G LTE
theregister
tecore
دسته بندی:
امنیت
پرونده ویژه
تاریخ انتشار :
11:05 - 09/07/1397
برچسب:
نقص امنیتی_شبکه 4G - نقص امنیتی_شبکه5G - امنیت_شبکه 4G - امنیت UE - 4G LTE - 5G - پروتکل GTP -
شهر_هوشمند - پیادهسازی 5G - 4G LTE

نشانی
□□□□:https://www.shabakeh-mag.com/security/13072/%D9%86%D9%82%D8%B5%E2%80%8C%D9%87%D8%A7%DB%8C-%D8%A7%D9%85%D9%86%DB%8C%D8%AA%DB%8C-%D8%B4%D8%A8%DA%A9%D9%87%E2%80%8C%D9%87%D8%A7%DB%8C-4g-%D9%88-5g-%D9%88-%D9%85%D8%B4%DA%A9%D9%84%D8%A7%D8%AA-%D9%86%D8%A7%D8%B4%DB%8C-%D8%A7%D8%B2-%D8%A2%D9%86%E2%80%8C%D9%87%D8%A7