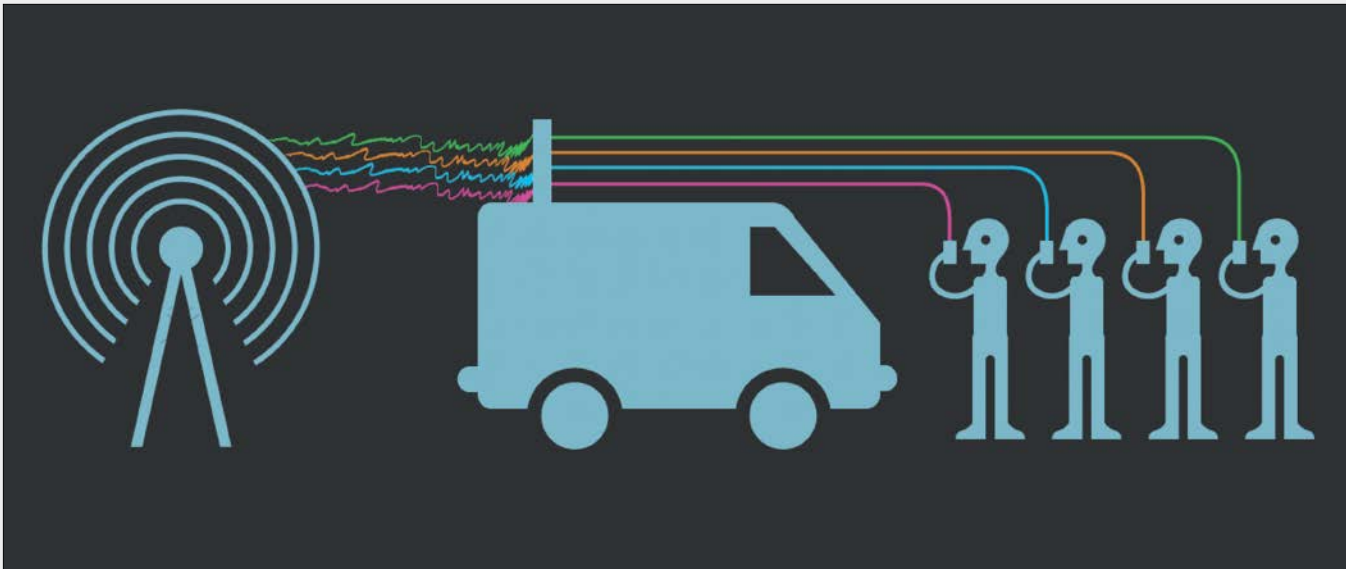




اینترنت همراه نسل ۵ هنوز امن نیست سرعت بدون امنیت؟

صالح سپهری فر

بسیاری از علاقه‌مندان به فناوری بی‌صبرانه مشتاقند که زیرساخت‌های نسل پنجم اینترنت همراه (5G) از راه پرسد تا بتوانند از مزایای آن به‌ویژه سرعت بالای آپلود و دانلود استفاده کنند. براساس اطلاعات موجود، سرعت شبکه نسل چهارم (البته در حالت ایده آل) ۱۰۰ مگابیت بر ثانیه است. این در حالی است که حداکثر سرعت شبکه نسل پنجم به حدود ۱۰۰ برابر آن یعنی ۱۰۰ گیگابیت بر ثانیه می‌رسد، اما شبکه نسل پنجم اینترنت همراه فقط به افزایش سرعت خلاصه نمی‌شود. یکی از مواردی که همواره ذهن کارشناسان حوزه ارتباطات را به خود مشغول می‌کند، امنیت است. نسل چهارم اینترنت، کاستی‌هایی در زمینه امنیت داشت. به همین دلیل، در طراحی نسل پنجم تا حد زیادی به این مساله توجه شده است. با وجود این، بررسی برخی کارشناسان گویای آن است که این نوآوری همچنان از نظر امنیت با ضعف‌های جدی روبه‌روست. اما این ضعف‌ها چه هستند؟

این مساله را یک مشکل بسیار بزرگ دانست. برای نمونه، دستگاه استرینگری می‌تواند هشت دستگاه آیفون یا پنج دوربین مداربسته را در یک منطقه جغرافیایی شناسایی کند. تا اینجا کار، شاید این داده‌ها چندان هم اهمیت نداشته باشند، اما مشکل وقتی ایجاد می‌شود که انسان بخواهد در این فرایند حضور یابد و از این داده‌ها سوءاستفاده کند. اما چطور؟

شرکت‌های مخابراتی، دستگاه‌های متصل به آن را به ۱۲ گروه مختلف تقسیم می‌کنند که البته این تقسیم‌بندی بر اساس میزان پیچیدگی و حجم داده مورد نیاز هر دستگاه است. برای نمونه یک تلفن هوشمند نمره ۱۱ یا ۱۲ می‌گیرد و یک دستگاه ساده اینترنت اشیا مثل یخچال هوشمند شاید نمره ۲ یا ۳ دریافت کند. هدف از این نمره‌دهی، تامین بهتر نیاز این دستگاه‌ها برای داده است. به این ترتیب دستگاه‌های پیچیده‌تر و دارای نمره بالاتر به شبکه نسل چهار یا پنج هدایت می‌شوند و درخواست داده دستگاه‌های با نمره پایین‌تر که نیاز به تبادل حجم زیادی از داده‌ها ندارند، به سمت شبکه نسل دوم یا سوم می‌رود.

پژوهشگران حوزه امنیت شبکه در بررسی‌های خود متوجه شدند می‌توانند از

در واقع، وجود یک وقفه زمانی در فرایند رمزنگاری سبب می‌شود امکان دخالت استرینگری فراهم شود. یک دستگاه برای اتصال به دکل مخابراتی، ابتدا حجم اندکی از داده‌ها را درباره خودش به آن منتقل می‌کند. این داده‌ها رمزگذاری شده نیستند. به همین دلیل، استرینگری می‌تواند از آن برای شناسایی و رهگیری دستگاه در منطقه‌ای مشخص استفاده کند.

آزمایش‌های صورت گرفته در این باره نشان داده از این داده‌های رمزنگاری نشده می‌توان برای تعیین نوع دستگاه (تلفن همراه، تبلت، ساعت هوشمند، حسگر و...) استفاده کرد. شناسایی سازنده دستگاه، قطعات

سخت‌افزاری موجود در آن، مدل دستگاه، سیستم‌عامل و حتی نسخه سیستم‌عامل از دیگر مواردی است که در اختیار استرینگری قرار می‌گیرد. در این صورت، در صورتی که هرکس یا دارندگان استرینگری دنبال یک هدف خاص باشند، به راحتی می‌توانند از این داده‌ها برای مقاصد خود بهره ببرند. البته این میزان از داده‌ها در مقایسه با حجم گسترده داده‌هایی که در نسل چهارم به صورت رمزگذاری نشده منتشر می‌شد، بسیار اندک است. به همین دلیل شاید نتوان

تجهیزات جاسوسی دکل نما

یکی از تجهیزات معروف در حوزه امنیت تجهیزات همراه، استرینگری (stringray) نام دارد. استرینگری یک دستگاه پیشرفته است که خود را به عنوان یک دکل مخابراتی معرفی می‌کند و به این ترتیب ضمن دستیابی به داده‌های مختلف گوشی، تبلت، خودرو، دستبند هوشمند یا هر وسیله دیگر متصل به شبکه، تا حدی می‌تواند عملکرد آن را نیز در دست بگیرد.

این دستگاه از یک سو به دکل‌های مخابراتی متصل می‌شود و از سویی دیگر، دستگاه‌های همراه (نظیر گوشی‌های همراه) را به اتصال به خود سوق می‌دهد. استرینگری نه تنها می‌تواند به داده‌های گوشی دست یابد، بلکه حتی امکان استراق‌سمع را نیز فراهم کند.

هر گوشی همراه برای اتصال به نزدیک‌ترین دکل مخابراتی، یک سری اطلاعات را به دکل می‌دهد. دستگاه‌های استرینگری خود را به عنوان دکل مخابراتی معرفی می‌کنند و به این ترتیب به این داده‌ها دست می‌یابند.

این مساله برای شبکه اینترنت همراه نسل چهارم، یک موضوع جدی بود. به همین دلیل، یکی از اولویت‌های امنیتی در طراحی شبکه نسل پنجم، برطرف کردن این نقص بود تا استرینگری دیگر نتواند از داده‌های هویتی تلفن همراه متصل شده برای شناسایی و رهگیری آن استفاده کند، اما بررسی تیم‌های امنیتی نشان می‌دهد متأسفانه شبکه اینترنت همراه نسل ۵ نتوانسته این مشکل را به‌طور کامل رفع کند. در واقع، در این شبکه نیز هنوز دستگاه‌های متصل در معرض حملات دکل‌های قلابی قرار دارند.

آیا رمزگذاری کافی است؟

یکی از بهبودهای صورت گرفته در شبکه نسل پنجم، رمزگذاری داده‌های مربوط به دستگاه است. به این ترتیب، برخلاف داده‌های دستگاه که در شبکه نسل چهارم به صورت یک فایل متنی ساده در دسترس دکل قرار می‌گرفت، در نسل پنجم از رمزنگاری استفاده می‌شود. هدف از این کار از بین بردن امکان استرینگری بود. اما ظاهراً این قابلیت، آن‌طور که باید نتوانسته از آزمایش‌ها سربلند خارج شود.

جست‌وجوی بی‌پایان

در صورتی که استرینگری بتواند دستگاه را به یک شبکه پایین‌تر ببرد، می‌تواند مانع از ورود آن به حالت «صرفه‌جویی در مصرف انرژی» شود. البته این قابلیت هدایت به شبکه‌ای پایین‌تر، به خودی خود جزو معایب شبکه اینترنت همراه نسل ۵ نیست، بلکه نحوه اجرای آن توسط اپراتورهاست که می‌تواند دردسرساز باشد.

در بررسی صورت گرفته روی ۳۰ اپراتور شبکه تلفن همراه در اروپا، آسیا و آمریکای شمالی مشخص شد ۲۱ اپراتور عملکردی داشتند که امکان این‌گونه حملات را فراهم می‌کرد و فقط ۹ اپراتور بودند که سیستم خود را به شکلی طراحی کرده‌اند که جلوی این نوع حملات را می‌گیرد. پس از این که دستگاهی به یک دکل متصل شد و تبادل داده به سرعتی تأیید رسید، منتظر پیغامی از سوی دکل می‌ماند تا دیگر به جست‌وجوی شبکه ادامه ندهد. این فرایند جست‌وجوی شبکه، انرژی بسیار بالایی مصرف می‌کند.

پژوهشگران به این نتیجه رسیدند با استرینگری می‌توان دستگاه را به ادامه این جست‌وجو سوق داد. به این ترتیب، باتری دستگاه پنج برابر سریع‌تر از حالت معمولی مصرف می‌شود. بروز این وضعیت به‌ویژه برای حسگرها و دستگاه‌های کنترلر می‌تواند بسیار خطرناک باشد.

باز هم منتظریم

پژوهش‌های انجام شده در این زمینه قرار است در تدوین نهایی استانداردهای نسل پنجم اینترنت همراه مورد بررسی قرار گیرد. این امید وجود دارد که این نواقص در این استانداردها در نظر گرفته شده و تدابیری برای رفع آنها اندیشیده شود.

هر گوشی همراه
برای اتصال به نزدیک‌ترین
دکل مخابراتی، یک سری اطلاعات
را به دکل می‌دهد. دستگاه‌های
استرینگری خود را به عنوان دکل
مخابراتی معرفی می‌کنند و به این
ترتیب به این داده‌ها دست
می‌یابند



امنیت



اگر مطالب
این صفحه را
می‌پسندید،
عدد ۷۱۸۲
را به شماره
۳۰۰۱۱۲۲۶
پیامک کنید