WPA3 چیست و چه زمانی در شبکه‌های وای‌فای استفاده خواهد شد؟

طبق اعلام انجمن وای‌فای، WPA3 یک استاندارد امنیتی وای‌فای است که جایگزین WPA2 خواهد شد. این یکی از معدود خبرهای جالبی بود که در CES 2018 اعلام شد. ظرف چند سال وقتی روبات‌های مرتب کننده لباس و یخچال‌های هوشمند فراموش می‌شوند، WPA3 همه جا حضور خواهد داشت و کار نفوذ به وای‌فای شما را برای هکرها سخت‌تر خواهد کرد.
WPA سر نام عبارت Wi-Fi Protected Access یا دسترسی وای‌فای محافظت شده است. اگر شبکه وای‌فای خانگی خود را به کلمه عبور مجهز کرده باشید، احتمالا شبکه شما با نسخه دوم این استاندارد (WPA2) محافظت شده است. دو استاندارد قدیمی‌تر به نام‌های WPA و WEP نیز وجود دارد که دیگر امن نیستند.

WPA2 یک استاندارد امنیتی است که کنترل اوضاع را در زمانی که شما با استفاده از کلمه عبور به یک شبکه وای‌فای متصل می‌شوید به دست می‌گیرد. WPA2 با تعیین یک پروتکل مشخص می‌کند که چگونه یک روتر و دستگاه‌های کلاینت می‌توانند یک اتصال امن را با یک دیگر برقرار کنند. بر خلاف استاندارد اصلی WPA، نسخه دوم به اجرای یک سیستم کدگذاری قدرتمند AES نیاز دارد که نفوذ به آن بسیار سخت‌تر است. این کدگذاری سبب می‌شود تا یک اکسس پوینت وای‌فای (مثل یک روتر) و یک کلاینت وای‌فای (مثل یک لپتاپ یا تلفن) بتوانند به صورت بی‌سیم بدون این که ترافیک آنها در دسترس دیگران قرار بگیرد با یک دیگر ارتباط برقرار کنند.

از لحاظ فنی، WPA2 و WPA3 گواهینامه‌های سخت افزاری هستند که تولیدکنندگان دستگاه باید آن را دریافت کنند. یک تولیدکننده باید قبل از عرضه دستگاه خود تحت عنوان Wi-Fi CERTIFIED™ WPA2™ یا Wi-Fi CERTIFIED™ WPA3™ تمام ویژگی‌های امنیتی مورد نیاز را به طور کامل داشته باشد.

در حال حاضر استاندارد WPA2 نیازهای ما را به خوبی برآورده می‌سازد، اما مدت زمان زیادی از معرفی آن می‌گذرد. این استاندارد از سال 2004 آغاز شد و چهارده سال از عمر آن می‌گذرد. WPA3 قصد دارد با قابلیت‌های امنیتی بیشتر پروتکل WPA2 را ارتقا دهد.

WPA3 چه تفاوتی با WPA2 دارد

استاندارد WPA3 چهار ویژگی دارد که در WPA2 وجود نداشت. تولیدکنندگان باید به طور کامل از این چهار ویژگی پیروی کنند تا دستگاه آنها بتواند به عنوان Wi-Fi CERTIFIED™ WPA3™ وارد بازار شود. هر چند انجمن وای‌فای (گروه صنعتی که این استانداردها را تعریف می‌کند) هنوز جزئیات فنی این ویژگی‌ها را به طور دقیق توضیح نداده است، اما ما با یک طرح کلی از ویژگی‌ها آشنا هستیم.

حریم خصوصی در شبکه‌های وای‌فای عمومی

در حال حاضر، شبکه‌های وای‌فای باز (آنهایی که در فرودگاه‌ها، هتل‌ها، کافی شاپ‌ها و سایر مکان‌های عمومی وجود دارد) یک نقطه ضعف امنیتی دارند. به دلیل این که آنها باز هستند و به همه اجازه اتصال می‌دهند، ترافیک ارسال شده از طریق آنها به هیچ وجه کدگذاری شده نیست. هر چیزی که از طریق این اتصال ارسال می‌شود به شکل متن ساده خواهد بود و دیگران می‌توانند در این مسیر آن را دریافت کنند. اتصالات کدگذاری شده HTTPS در وب می‌تواند امنیت را افزایش دهد، اما مردم همچنان می‌توانند ببینند شما به کدام وبسایت متصل شده‌اید و محتوای صفحات HTTP نیز قابل مشاهده است.

WPA3 با استفاده از قابلیت رمزگذاری داده‌های فردی این مشکل را برطرف می‌کند. وقتی شما به یک شبکه وای‌فای باز متصل می‌شوید، ترافیک بین دستگاه شما و اکسس پوینت وای‌فای حتی اگر از گذرواژه در زمان اتصال استفاده نکرده باشید رمزگذاری خواهد شد. این باعث می‌شود تا شبکه‌های بی‌سیم عمومی خصوصی‌تر شود. دیگران تا زمانی که نتوانند به این داده‌های کدگذاری شده نفوذ کنند امکان دسترسی به آن را نخواهند داشت.

محافظت در برابر حملات جستجوی فراگیر

وقتی یک دستگاه به یک اکسس پوینت وای‌فای متصل می‌شود، ابتدا باید اطمینان حاصل کند که شما از یک گذرواژه صحیح برای این ارتباط استفاده کرده‌اید. در حمله 2017 معروف به KRACK attack ثابت شد این روش ارتباطی آسیب پذیر است، هر چند دستگاه‌های WPA2 موجود با به‌روزرسانی نرم افزاری می‌توانند این مشکل را برطرف کنند.

WPA3 از یک ساختار ارتباطی جدید استفاده خواهد کرد که حتی زمانی که کاربران از کلمات عبور ساده و قابل حدس استفاده می‌کنند هم از امنیت کافی برخوردار خواهد بود. به بیان دیگر، حتی اگر شما از یک کلمه عبور ضعیف هم استفاده کنید استاندارد WPA3 از شما در برابر حملات جستجوی فراگیر (brute-force) یا همان حدس زدن مکرر کلمات عبور برای پیدا کردن کلمه عبور صحیح محافظت خواهد کرد.

یک فرآیند اتصال ساده برای دستگاه‌های فاقد صفحه نمایش

امروزه ما شاهد دستگاه‌های مجهز به وای‌فای هستیم که فاقد نمایشگر هستند. هر چیزی از آمازون اکو و گوگل هوم تا پریزهای هوشمند و لامپ‌های روشنایی می‌تواند به یک شبکه وای‌فای متصل شود. اما اغلب اتصال این دستگاه‌ها به شبکه با دردسرهایی همراه است، زیرا صفحه نمایش یا صفحه کلیدی برای وارد کردن کلمه عبور ندارند. اتصال این نوع دستگاه‌ها اغلب از طریق تلفن هوشمند و با استفاده از یک اپلیکیشن برای وارد کردن گذرواژه وای‌فای شما انجام می‌شود و فرآیند آن اغلب از آنچه باید باشد سخت‌تر است.

WPA3 از قابلیتی برخوردار است که وعده می‌دهد فرآیند پیکربندی امنیتی دستگاه‌هایی که با محدودیت نمایشگر و رابط کاربری مواجه هستند را ساده می‌کند. هنوز مشخص نیست که این کار چگونه انجام می‌شود، اما باید چیزی شبیه به قابلیت Wi-Fi Protected Setup امروزی باشد که با فشردن یک دکمه روی روتر امکان اتصال به آن فراهم می‌شود. هر چند قابلیت WPS نیز مشکلات امنیتی مخصوص خود را دارد. اما باید منتظر بود و دید که چگونه این قابلیت جدید کار خواهد کرد.

امنیت بیشتر برای مراکز دولتی، دفاعی و کاربردهای صنعتی

این ویژگی آخر کاربرد چندانی برای کاربران خانگی ندارد، اما انجمن وای‌فای اعلام کرده است که WPA3 شامل یک بسته امنیتی 192 بیتی است که با بسته الگوریتم امنیت ملی تجاری (CNSA) سازگار است که برای مراکز دولتی، دفاعی و کاربردهای صنعتی در نظر گرفته شده است.

چه زمانی به این استاندارد دسترسی خواهیم داشت

طبق اعلام انجمن وای‌فای دستگاه‌هایی که از WPA3 پشتیبانی می‌کنند تا اواخر 2018 عرضه خواهند شد و شما شاهد نماد ™Wi-Fi CERTIFIED™ WPA3 روی روترهای جدید خواهید بود.

این انجمن هنوز اعلام نکرده است که آیا دستگاه‌های موجود نیز پشتیبانی از WPA3 را دریافت خواهند کرد، اما انتظار نمی‌رود که دستگاه‌های زیادی بتوانند با استفاده از به‌روزرسانی نرم افزاری از WPA3 پشتیبانی کنند. خیلی از تولیدکنندگان ترجیح خواهند داد منابع خود را صرف توسعه سخت افزارهای جدید برای پشتیبانی از این استاندارد کنند.

حتی بعد از این که روتر شما به WPA3 مجهز شد، شما به دستگاه‌های کلاینت سازگار با WPA3 نیاز خواهید داشت تا بتوانید به طور کامل از مزایای این ویژگی‌های جدید بهره‌مند شوید.

Wi-Fi WPA3 Security