پروتکل امنیتی WPA3 چیست و چگونه امنیت شبکه وای-فای را افزایش می دهد؟ - دیجیاتو

حمید مقدسی | پنجشنبه، ۳۰ فروردین ۱۳۹۷

سالهاست که بهترین گزینه حفاظتی وای-فای شخصی در زمان تنظیم مودم یعنی WPA2 را می شناسیم. WPA2 یا «نسل دوم دسترسی حفاظت شده وای-فای» یکی از قابلیت های امنیتی استاندارد شبکه است که از روش رمزگذاری AES به واسطه رمز عبور استفاده می کند. چندی پیش نهاد مرجع این حوزه یعنی «وای-فای الاینس» (Wi-Fi Alliance) نسل سوم این فناوری یعنی پروتکل امنیتی WPA3 را معرفی کرد.

پروتکل امنیتی WPA3 در نسخه به روز شده این استاندارد است که می تواند امنیت بیشتری را فراهم آورد، موضوعی که در دنیای امروز با گسترش شبکه های وایرلس و تهدیدات امنیتی مربوط به آن، کاملاً ضروری به نظر می رسد. در این مطلب می خواهیم به بررسی ویژگی های جدید و نحوه عملکرد WPA3 بپردازیم.

WPA چگونه کار می کند؟

پروتکل امنیتی WPA از سیستم ارزیابی امنیتی «دست دهی» یا handshaking استفاده می کند. در این روش اطمینان حاصل می شود که تمامی دستگاه های حاضر در ارتباط وایرلس روی یک بستر مشترک قرار گرفته و به خوبی کار می کنند.

در WPA2 فرایند دست دهی به شکل چهار مسیره بین دو دستگاه کلاینت متصل به شبکه و دو نقطه دسترسی وایرلس (اکسس پوینت) مورد استفاده، انجام می شود. سیستم WPA2 تمام دستگاه ها بررسی کرده تا از یکسان بودن رمز عبور آنها مطمئن شود. سپس انتقال داده های رمزنگاری شده بین آنها را شروع کرده و نهایتاً پس از پایان فرایند انتقال، رمزگشایی اطلاعات در مقصد را ممکن می سازد.

مهم ترین مزیت سیستم WPA2 این است که بسیاری از انواع سرقت داده معمول را از کار انداخته یا حداقل، اجرای آنها را بسیار دشوار و پر هزینه می کند. همان طور که می دانید بسیاری از حملات هَک وای-فای از نوع «مرد میانی» (MITM) یا روش های مشابه است که تلاش می کنند اطلاعات وایرلس را در میان راه و در زمان انتقال، بدزدند. فناوری WPA2 داده ها را به گونه ای رمزنگاری می کند که حتی سرقت آنها هم سودی برای هکرها نخواهد داشت، چون توانایی رمزگشایی آنها را ندارند.

تفاوت WPA3 با WPA2 در چیست؟

پروتکل WPA2 سال های متمادی به خوبی کار کرده اما با توجه به پیشرفت تکنولوژی و روش های نوین سرقت اطلاعات ارزشمند کاربران توسط هکرها، کمی قدیمی به نظر می رسد. حالا WPA3 با افزودن چهار قابلیت جدید به فرایند رمزگذاری، امنیت آن را افزایش می دهد.

رمزگذاری بهتر برای کاربران مهمان

شبکه های وای-فای باز یا مهمان (guest) که در مراکز عمومی مانند کافی شاپ یا کتابخانه برقرار می شوند، یکی از نا امن ترین گزینه های ارتباطی هستند. در پروتکل امنیتی WPA3 رمزگذاری اطلاعات به شکل فردی و مستقل انجام می شود، یعنی ارتباط شما با یک شبکه وایرلس باز مستقیماً رمزگذاری شده خواهد بود، حتی اگر شبکه مورد نظر فاقد گزینه های امنیتی و رمز عبور باشد. این تغییر را می توان یکی از مهم ترین و ضروری ترین تغییرات دانست.

به روز رسانی فرایند دست دهی

پروتکل امنیتی WPA2 در برابر حملات در سطح سخت افزار و رمزهای عبور ضعیف، کاملاً آسیب پذیر بود. البته پسوردهای ضعیف همیشه و همه جا مشکل ساز خواهند بود. حالا برای جلوگیری از این نوع آسیب پذیری از روش جدیدی برای دست دهی استفاده می کند که در برابر تکنیک های شکستن رمز عبور یا دیگر گزینه های بروت فورس (جستجوی فراگیر) مقاومت بیشتری دارد.

ارتباط بهتر با اینترنت اشیاء

پروتکل امنیتی WPA2 برای سازگاری با دستگاه های قابل حمل معمول مانند موبایل ها و لپ تاپ ها طراحی شده بود، دستگاه هایی که نمایشگر دارند و وارد کردن رمز عبور یا دسترسی به تنظیمات وایرلس در آنها ساده است. حالا تجهیزات هوشمند متعددی را می بینیم که فاقد نمایشگر یا ابزار ورود اطلاعات هستند، یا اپلیکیشن های مربوط به آنها برای مدیریت کامل ارتباط وایرلس طراحی نشده اند.

برای ساده تر کردن این فرایندها، پروتکل امنیتی WPA3 روش های جدیدی را برای پیکربندی امنیتی شبکه بدون نیاز به نمایشگر به کار می برد. البته هنوز جزئیات بیشتری در این رابطه در دست نیست اما احتمالاً روش های جفت شدن (pairing) پیشرفته و ایمن برای این منظور به خدمت گرفته شده است.

بسته امنیتی 192 بیتی

این استاندارد امنیتی فوق پیشرفته از الگوریتم CNSA استفاده می کند که شرایط حفاظتی مورد نیاز برای فعالیت های دولتی رده بالا، نهادهای اطلاعاتی و امنیتی، و پروژه های صنعتی فوق سری را فراهم می سازد. بدین ترتیب نهادها و سازمان های فوق هم به راحتی می توانند از شبکه های وای-فای با اطمینان خاطر استفاده کنند.

شرکت های سازنده چه می کنند؟

سؤال اصلی این است که ما به عنوان مصرف کننده، چه زمانی به این استاندارد جدید دست پیدا می کنیم؟ پاسخ به این سؤال چندان ساده نیست. پروتکل امنیتی WPA3 به روز رسانی بسیار بزرگی برای دستگاه ها و تجهیزات وایرلس محسوب می شود، یعنی نمی توان صرفاً با ارتقاء فرمور یا تغییرات جزئی سخت افزاری به آن دست یافت.

شرکت های سازنده برای سازگاری با این استاندارد باید تجهیزات ارتباطی را به طور کامل از نو طراحی کرده و بسازند، تا بتوانند تمامی چهار تغییر اساسی در پروتکل امنیتی WPA3 را پیاده سازی نموده و گواهی مربوطه را دریافت کنند.

علاوه بر این، فراگیر شدن این استاندارد هم زمان زیادی را نیاز دارد. تنها یک دستگاه سازگار با WPA3 هیچ سودی ندارد، بلکه تمامی دیوایس های نهایی (موبایل، لپ تاپ و دیگر ابزارهای متصل به شبکه) و اکسس پوینت ها (مودم/روتر) باید با این پروتکل سازگاری یابند، وگرنه تغییری در فرایند ارتباط و امنیت شبکه به وجود نخواهد آمد.

با این حال به نظر می رسد در سال جاری میلادی، حضور نخستین تجهیزات شبکه مانند روترها را با پشتیبانی از WPA3 در نمایشگاه های معتبر فناوری شاهد باشیم که البته با WPA2 نیز سازگاری دارند و تا مدت ها با همین استاندارد رایج کار خواهند کرد.

دیجیاتو