محققان می‌گویند رمزنگاری HTTPS آنقدرها که به نظر می‌رسد امن نیست - دیجیاتو

شایان ضیایی | شنبه، ۲۶ مهر ۱۳۹۹

متد رمزنگاری HTTPS به افزوده شدن انبوهی از قفل‌های سبز رنگ به صفحات وب و البته محافظت از اطلاعات درون آن‌ها منجر شده است. تمام سایت‌های محبوبی که به صورت روزانه به آن‌ها سر می‌زنید به احتمال زیاد از یک خط دفاعی به نام «امنیت لایه انتقال» یا «TLS» برخوردار هستند که اطلاعات را میان مرورگر شما و وب سروری که با آن در ارتباط هستید رمزنگاری می‌کند تا از برنامه‌های سفرتان، رمزهای عبور و سرچ‌هایتان در گوگل در برابر مهاجمین محافظت شود. اما یافته‌های جدید محققان دانشگاه کا فوسکاری ونیز نشان می‌دهد که شمار غافلگیرکننده‌ای از سایت‌های رمزنگاری شده، این ارتباطات را در معرض حمله هکرها قرار داده‌اند.

با تحلیل ۱۰ هزار سایت HTPPS برتر -براساس رده‌بندی کمپانی آماری الکسا که متعلق به آمازون است- محققان دریافته‌اند که ۵.۵ درصد از آن‌ها از آسیب‌پذیری‌های TLS رنج می‌برند. این نواقص ناشی از ترکیبی از مشکلاتی است که هنگام تعبیه رمزنگاری TLS در سایت بروز کرده‌اند و ضمنا برخی از باگ‌های از پیش شناسایی شده TLS نیز برطرف نشده‌اند. اما بدترین نکته اینست که علی‌رغم وجود این نواقص و آسیب‌پذیری‌ها، علامت قفل سبز رنگ همچنان کنار آدرس سایت‌ها به نمایش در می‌آمده است.

ریکاردو فوکاردی، محقق امنیت شبکه و رمزنگاری در دانشگاه کا فوسکاری ونیز که هم‌موسس شرکت Cryptosense نیز بوده می‌گوید: «ما در مقاله فرض را بر این گذاشتیم که مرورگر کاملا به روز است، اما چیزهایی یافتیم که مرورگر قادر به شناسایی‌شان نبود. این‌ها نواقصی هستند که برطرف نشده‌اند و حتی مورد توجه هم قرار نگرفته‌اند. ما می‌خواستیم این مشکلات را در سایت‌های مبتنی بر TLS بیابیم که هنوز هیچ اطلاعاتی راجع به نواقص به کاربران نداده‌اند».

محققان که یافته‌های کامل خود را در گردهمایی IEEE در زمینه امنیت و حریم شخصی طی ماه مه آتی منتشر خواهند کرد، تکنیکی برای تحلیل TLS توسعه داده‌اند و ضمنا از ادبیات رمزنگاری از پیش موجود برای شناسایی مشکلات TLS در ۱۰ هزار سایت برتر استفاده کرده‌اند. و براساس یافته‌ها، آسیب‌پذیری‌ها در چند بخش دسته‌بندی شده‌اند.

برخی از نواقص ریسک خاصی به همراه دارند، اما هکر نمی‌تواند به صورت کامل بر آن‌ها متکی باشد. این بدان خاطر است که این نواقص یک کوئری واحد را برای چندین مرتبه به جریان می‌اندازند و اطلاعات به صورت بسیار قطره‌ای قابل استخراج خواهد بود. این باگ‌ها می‌توانند به هکر در رمزگشایی چیزی مانند کوکی نشست کمک کنند، چرا که کوکی‌ها احتمالا همراه با هر کوئری در سایت ارسال شوند، اما در زمینه‌هایی مانند استخراج رمز عبور چندان کارآمد نیستند.

باگ‌های موجود در دسته‌بندی بعدی اما اندکی شیطانی‌تر ظاهر می‌شود. آسیب‌پذیری‌های این دسته‌بندی، کانال‌های رمزنگاری ضعیف‌تری میان مرورگر و وب سرور دارند و به مهاجم اجازه می‌دهد تا تمام ترافیکی که میان این دو در جریان است را رمزگشایی کنند. بدتر از همه نیز، کانال‌هایی را داریم که نه‌تنها به هکرها اجازه می‌دهد تمام ترافیک را رمزگشایی کنند، بلکه امکان دستکاری ترافیک را نیز مهیا می‌سازند. این‌ها در واقع فونداسیونی برای «حملات مرد میانی» به حساب می‌آیند که رمزنگاری HTTPS اصلا برای مقابله با همان‌ها توسعه یافته بود.

نواقصی که محققان یافته‌اند در عمل لزوما آسیب‌پذیری‌هایی حیاتی به حساب نمی‌آیند. این را کن وایت، مهندس امنیت و مدیر پروژه Open Crypto Audit می‌گوید. اکثر این نواقص را می‌توان مورد سوء استفاده قرار داد، اما از آن‌جایی که نیاز تلاش فراوان هستند شاید به مذاق هکرها خوش نیایند. اما وایت در هر صورت تاکید می‌کند که این یافته‌ها بسیار مهم تلقی شده و می‌توانند بخش از یک تلاش بزرگ‌تر برای تمیز کردن وب باشند.

ديجياتو