پرسه در دالان‌های تاریک

» نویسنده: اندرو کانینگهام
» منبع: آرس تکنیکا
» ترجمه: احمد شریف‌پور

من و خانواده‌ام تقریباً از سال ۱۹۹۸ آنلاین بوده‌ایم. اما من در ابتدای کار چندان به امنیت در فضای آنلاین توجه نمی‌کردم. البته، کامپیوتر متصل به اینترنت (که در آن زمان یک سلرون ۴۳۳ مگاهرتزی بود) همیشه آخرین نسخه مرورگر اینترنت اکسپلورر را اجرا می‌کرد و من هم سعی می‌کردم برای همه کارهایم از یک گذرواژه استفاده نکنم. اما توجهی به این‌که ترافیک وب من به کجا می‌رفت نداشتم یا توجه نمی‌کردم که در حرکت به سرور اینترنتی و بازگشت چه مسیری را طی می‌کند. من همان زمان هم (از طریق یکی از اساتیدم) می‌دانستم که استفاده از ایمیل مانند این است که سرت را از پنجره بیرون کنی و داد بزنی! امنیت و حریم خصوصی چندانی وجود ندارد. اما از چیزهایی که می‌دانستم به درستی استفاده نمی‌کردم.

چنین رویکردی در گذشته خطرناک بود و اکنون نیز با درنظر گرفتن مجموعه ابزارهای پیچیده و پیشرفته هک که امروزه به‌صورت آماده موجود است، این رویکرد خطرناک‌تر هم شده است. خوشبختانه وضعیت امنیت خود اینترنت هم کم‌وبیش بهتر شده است. در این مقاله که نخستین بخش از مجموعه‌ای پنج قسمتی است، قصد داریم درباره امن نگاه داشتن خودتان و کسب‌وکارتان در روی وب صحبت کنیم. حتی اگر می‌دانید در گوشه‌های خلوت اینترنت چه خطراتی در کمین شما است، ممکن است یکی از آشنایان شما با این موضوع آشنا نباشد. بنابراین به این مطلب و قسمت‌های بعدی آن به چشم یک راهنمای سریع و دم‌دست برای کسانی که چندان با امنیت در فضای آنلاین آشنا نیستند، نگاه کنید. کسانی که برای این موضوع اهمیت بیشتری قائل هستند، بهتر است برای آشنایی با مباحث پیچیده‌تر به قسمت‌های بعدی این مقالات هم توجه کنند. مطلب حاضر را با برخی اطلاعات پایه درمورد رمزنگاری در اینترنت و نحوه استفاده از آن برای محافظت از اطلاعات شخصی‌تان شروع می‌کنیم. پس از آن به بدافزارها، امنیت برنامک‌های موبایل و موضوعات دیگر خواهیم پرداخت.

SSL و TLS، شنل‌های امنیتی نامریی

معمول‌ترین شیوه رمزنگاری در وب، چیزی است که بیشتر کاربران حتی متوجه آن هم نمی‌شوند. پروتکل امن انتقال ابرمتن HTTPS (سرنام HyperText Transfer Protocol Secure) ترافیک معمول وب که به‌صورت http است را به کمک امنیت لایه انتقال TLS (سرنام Transport Layer Security) یا لایه سوکت‌های امن SSL (سرنام Secure Sockets Layer) رمزنگاری می‌کند. TLS جدیدتر است و بیشتر در سایت‌های مدرن مورد استفاده قرار می‌گیرد. اما از آنجا که این دو به لحاظ عملکرد یکسان هستند، متخصصان امنیتی به‌صورت یکجا و با نام SSL/TLS از آن یاد می‌کنند. جدیدترین نسخه SSL نسخه ۳ و جدیدترین نسخه TLS نسخه ۱ است. پروتکل HTTPS به‌طور معمول هنگام انتقال داده‌های حساس یا شخصی مورد استفاده قرار می‌گیرد. نام کاربری و کلمه عبور، اطلاعات مالی و اطلاعات ردوبدل شده میان سرور و کلاینت‌های ایمیل به‌طور معمول با این پروتکل جابه‌جا می‌شوند. صفحات معمول وب اغلب از این سیستم استفاده نمی‌کنند، اگرچه در سایت‌هایی نظیر ویکی‌پدیا هم میزان استفاده از نسخه HTTPS کم‌کم در حال رشد است.

شکل ۱ مسئله فقط همان S است. یک اتصال https امنیت ارتباط میان مرورگر شما و سرور سایت را تأمین می‌کند.

HTTPS اتصالی رمزنگاری‌شده و امن را میان مرورگر شما و سرورهای سایتی که به آن متصل می‌شوید برقرار می‌کند. داده‌ها قبل از ارسال به سمت سرور رمزنگاری می‌شوند و این داده‌ها تنها زمانی رمزگشایی می‌شوند که به‌صورت کامل و صحیح به سرور رسیده باشند. همین امر در مورد داده‌هایی که از سرور برای مرورگر شما فرستاده می‌شوند هم صادق است. در رمزنگاری استاندارد «متقارن» کلید واحدی برای رمزنگاری و رمزگشایی مورد استفاده قرار می‌گیرد. در مقابل در رمزنگاری «کلید عمومی نامتقارن» از کلیدی همگانی که در دسترس عموم قرار دارد برای رمزنگاری استفاده می‌شود. اما محتوای رمزنگاری شده بدون حضور کلید خصوصی دومی (که البته به لحاظ ریاضی به اولی مربوط است) قابل رمزگشایی نخواهد بود. پروتکل https ترکیبی از این دو روش را برای ممانعت از دسترسی و رمزگشایی غیرمجاز داده‌ها به کار می‌گیرد. یکی دیگر از بخش‌های حیاتی این پروتکل شامل کنترل هویت سرور و کلید عمومی آن است تا مشخص شود آیا این سرور و اطلاعات واقعاً به شخص یا سازمانی که ادعا می‌کند مربوط است یا خیر. اگر کسی سروری جعلی یا آلوده به راه انداخته باشد (که به‌اصطلاح آن را فرد وسطی یا man in the middle می‌نامند)، رمزنگاری ارتباطات در عمل هیچ فایده‌ای نخواهد داشت. برای این که هویت سرور تأیید و مشخص شود به یک کلید عمومی نیاز است که توسط یک مقام مجاز امنیتی به‌صورت دیجیتال امضا شده باشد. این مقامات مسئول را به‌اصطلاح CA (سرنام Certificate Authority) می‌نامند. این CAها سازمان‌های حقوقی شناخته شده‌ای هستند که به‌طور معمول با نرخ‌های گزاف به متقاضیان

شکل ۲ بیشتر مرورگرها می‌توانند همه اطلاعات مورد نیاز درباره مجوز امضا شده یک سایت را به شما نشان دهند.

یک گواهی‌نامه امضا شده می‌دهند تا به کمک آن هویت و صحت اعتبار سرورهای‌شان را به مرورگرها اثبات کنند.

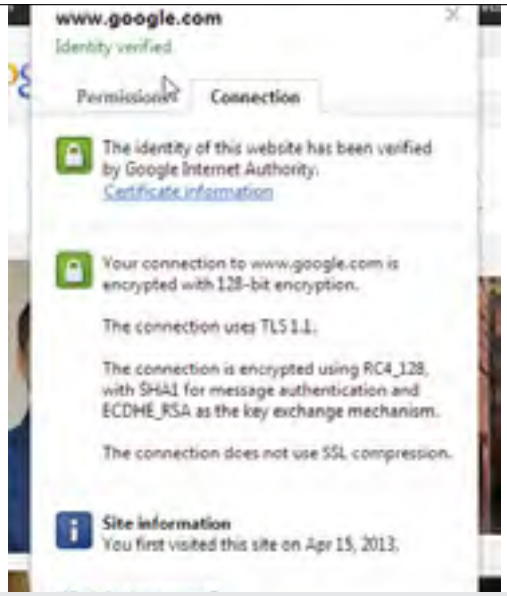
مدیران سرورها بدون این گواهی‌نامه‌های امضا شده نیز می‌توانند ترافیک سرورشان را رمزنگاری کنند، اما این گواهی‌نامه‌های «خود امضا» روش مطمئنی برای اعتبارسنجی هویت سایت‌ها نیستند و به‌سادگی ممکن است جعل شوند. بیشتر مرورگرها و برنامه‌ها طوری طراحی شده‌اند که به این گواهی‌نامه‌ها اعتماد نکنند. دلیل اصلی همان‌طور که پیش‌تر گفته شد این است که جعل‌کردن آن‌ها ساده‌تر است. مرورگرها درچنین شرایطی پیام‌های خطای ترسناکی را به نمایش در می‌آورند که به کاربران هشدار می‌دهد به این سایت‌ها اعتماد نکنند. این سایت‌ها ناامن هستند و تجربه کاربری بدی را به ارمغان می‌آورند. اما گواهی‌نامه‌های امضا شده هم محدودیت‌ها و ضعف‌های خود را دارند. یک CA تنها به اندازه سیاست‌های امنیتی‌اش قابل اعتماد است. اگر خود CA مورد نفوذ قرار بگیرد، تمام گواهی‌نامه‌هایی که تا زمان نفوذ

شکل ۳ گواهی‌نامه‌های خود امضا در برابر نفوذ و جعل آسیب‌پذیرتر هستند.

صادر کرده است را نیز باید بی‌اعتبار و از دست رفته تلقی کرد. البته این خود می‌تواند موضع مقاله‌ای جداگانه باشد.

بـا توجه به این موضوع که تقریباً تمـام این فرآیند رمزنگاری از کنترل کاربر خارج است، بهترین کاری که می‌توانید برای حفظ امنیت خود درهنگام انتقال داده‌های در دنیای آنلاین می‌توان انجام دهید این است که دقت کنید که کدام سایت‌ها از HTTPS و کدام‌ها از HTTP استفاده می‌کنند. بیشتر مرورگرها برای نشـان دادن امن بودن سایت از یک تصویر کوچک (شکل یک قفل) در نوار آدرس استفاده می‌کنند. این آیکون‌ها هم ممکن است جعل شوند، به همین دلیل در متن آدرس به دنبال کلمه https بگردید.

اگر لازم باشد می‌توانید از مرورگرتان بخواهید که اطلاعات جامعی را در ارتباط با گواهی‌نامه و الگوریتم رمزنگاری مورد استفاده سایت به شما ارائه کند. ما در این اسکرین‌شات‌ها از کروم گوگل استفاده کرده‌ایم، اما تقریباً همه مرورگرها می‌توانند همین کار را انجام دهند.(شکل ٤)



مرورگر کروم امکان مشـاهده دیدی کلی از سیسـتم رمزنگاری که برای حفظ امنیت شما مورد استفاده قرار گرفته است را به‌سادگی فراهم می‌آورد.

شکل ۴

با کلیک روی همان آیکون قفل می‌توانید اطلاعات رمزنگاری و گواهی‌نامه مربـوط به سـایت موردنظـر را ببینید. در ایـن نمونه گواهی‌نامه توسـط VeriSign امضا شـده است و اتصال از TLS 1.1 با رمزنگاری ۱۲۸ بیتی RC4 استفاده می‌کند. کلیک روی لینک اطلاعات گواهی‌نامه، اطلاعات بیشتری را در مورد خود گواهی‌نامه به شـما نشـان خواهد داد. مثلاً این که تاریخ انقضای گواهی‌نامه چه زمانی است و به چه شخصیت حقیقی یا حقوقی تعلق دارد.

رمزنگاری‌هـای SSL و TLS عالی و بی‌نقص هسـتند و اسـتفاده از این پروتکل‌ها بیشـتر و بیشـتر رایج می‌شـوند. اما حقیقتی که باید به آن توجه کرد این اسـت که این پروتکل‌ها تنها ارتباط کامپیوتر شما و یک سایت واحد را حفاظت می‌کنند. بسیاری از سایت‌ها هنوز از http قدیمی و ناامن استفاده می‌کننـد. اگر می‌خواهید از «تمام» ترافیک وب‌تان به صورت یک‌جا محافظت کنیـد (به‌خصوص زمانی که از یک محل عمومی یـا وای‌فای باز همگانی به اینترنت وصل شده‌اید) به‌احتمال زیاد تنها گزینه شبکه خصوصی مجازی یا VPN (سرنام Virtual Private Network) است.

استفاده از VPN برای حفاظت کامل

چندین نوع مختلف از سرورهای VPN وجود دارد، اما بیشتر آن‌ها از یک روش واحد استفاده می‌کنند: کامپیوتر شما به یک سرور VPN متصل می‌شود و تمام ترافیک میان شما و سـرور به‌صورت رمزنگاری شده در می‌آید. به VPN به چشـم یک تونل امن نگاه کنید که داده‌های شما را از سایت داده‌های موجود در شبکه جدا می‌کند. این اتصال همچنین تمام ترافیک شما را (نه فقط بخشی از آن را با سـایت‌های https) رمزنگاری می‌کند. تمام ارتباطات شما توسط سرور رمزگشایی شده و از طریق شبکه سرور (که معمولاً امن فرض می‌شـود) به‌سوی مقصد فرستاده می‌شـود. داده‌های برگشتی نیز به همین ترتیب در سرور رمزنگاری شده و برای سیستم شما ارسال می‌شود.

نقطـه ضعف VPN این اسـت که برقـراری اتصال آن بـه عهده کاربر اسـت. در حالـی کـه TLS و SSL کم و بیش شـفاف (پنهان از دیـد کاربر و بدون نیاز به انجام عملی از سـوی او) هسـتند، کاربر باید هر بار به‌شخصه اتصـال VPN را برقـرار کند. البتـه، نمونه‌های خودکارتـری از VPN مانند Microsoft Direct Access نیـز وجود دارند، اما میزان اسـتفاده از آن‌ها به نسـبت کمتر است. نکته دیگر این‌که شـما باید دسترسی به یک سرور VPN را به نوعی تهیه کنید. ممکن است کارفرمای شما چنین امکانی را برای انجام امور شـرکت دراختیار شما بگذارد، اما برای استفاده از این سیستم در امور غیرکاری (یا زمانی که نمی‌خواهید کارفرما از همه فعالیت شـما روی وب را ببیند) باید به فکر راه‌حل دیگری باشید.

اگر شـما به سـرور اختصاصی خودتـان نیاز داریـد، می‌توانید از نرم‌افزارهای آزادی مانند OpenVpn اسـتفاده کنیـد. برای کاربران مک، سیستم VPN از طریق بسته ۲۰ دلاری OS X Server قابل تهیه است. برخی از روترهـای رده بالای بـازار یا فرم‌ویرهای طرف سـوم نیز می‌توانند قابلیت‌های سـاده VPN را بدون نیاز به سخت‌افزار اختصاصی دراختیار

شکل ۵ سیستم‌عامل OSX Server با یک سرویس VPN ابتدایی عرضه می‌شود که ممکن است برای کاربران خانگی یا کسب‌وکارهای کوچک مناسب باشد. اما OpenVPN قدرتمندتر است و روی پلتفرم‌های بیشتری کار می‌کند.

کاربر قرار دهند. OpenVpn به‌طور معمول به‌عنوان ستون فقرات بسیاری از سرویس‌های VPN دیگر (که در بخش‌های بعدی از آن‌ها صحبت خواهیم کرد) مورد استفاده قرار می‌گیرد.

اگر نخواهید هزینه و دردسر تهیه و نگه‌داری سخت‌افزارهای مورد نیاز را تقبل کنید، این روش (استفاده از VPN روی روتر) امن‌ترین روش موجود است چراکه داده‌ها تنها در شبکه شما بدون رمزنگاری خواهند بود و به‌محض خروج از روتر به‌صورت رمزنگاری شده برای سرور VPN ارسال می‌شوند. اما این روش برای همه کار نخواهد کرد. همچنین مجبور خواهید بود که تنظیمات صحیح Port Frwarding را روی روترتان اعمال کنید تا بتواند با سرور VPN ارتباط برقرار کند. انجام این تنظیمات کاری است که روال در روترهای مختلف با هم متفاوت است. کسانی که با تجهیزات معمول و برای استفاده‌های معمولی به اینترنت متصل می‌شوند، مجبور خواهند بود که بعضی وقت‌ها با آدرس‌های IP سروکار داشته باشند و این آدرس‌ها هم گه‌گاه تغییر می‌کنند.

کار درچنین شرایطی نیازمند دستکاری تنظیمات سرور VPN یا استفاده از سیستمی پویا برای DNS نظیر DynDNS است. البته، همه این‌ها به شرطی است که ISP مورد استفاده اجازه برقراری اتصال VPN را بدهد. هر دوی این مشکلات را می‌توان با خرید یک اتصال رده تجاری از ISP برطرف کرد. اما چنین روشی به تبع هزینه بیشتری را به همراه خواهد داشت. همانند بسیاری از خدمات فناوری، سرورهای VPN هم می‌توانند برون‌سپاری شوند. سرویس‌های پولی فراوانی برای VPN در دسترس هستند که مزیات استفاده از آن‌ها واضح است. نیازی نیست سرور خودتان را راه‌اندازی کنید، زمان خرابی و عدم پاسخ‌گویی کمتری (به واسطه قطع برق، خرابی شبکه یا به‌روزرسانی سیستم‌ها) خواهید داشت. بیشتر این سرویس‌های VPN علاوه‌بر امنیت به حفظ حریم‌خصوصی شما نیز کمک خواهند کرد، چراکه می‌توانند ترافیک شما را حتی از ISPاتان مخفی کنند یا حتی طوری وانمود کنند که انگار شما از کشور دیگری به اینترنت متصل شده‌اید.

در تناقضی آشکار، مهم‌ترین ضعف این سرویس‌ها امنیت آن‌ها است! این سرویس‌ها تنها به اندازه افرادی که آن‌ها را عرضه می‌کنند اعتبار داشته و قابل اعتماد هستند، چراکه تمام ترافیک شما از سرورهای آن‌ها گذشته و در ماشین‌های آن‌ها رمزگشایی می‌شود.

پیتر اکرسلی مدیر پروژه‌های فناوری بنیاد پیشتازان الکترونیک (Electronic Frontier Foundation) می‌گوید: «این مشکل ذاتی تمام سرویس‌های VPN است. کاربر مجبور است به شرکت عرضه‌کننده VPN کاملاً اعتماد کند. حتی اگر برای همه‌چیز از HTTPS/TLS استفاده کنید، خدمات‌دهنده VPN شما می‌تواند آدرس IP شما را ثبت کرده، درخواست‌های DNSتان را ببیند و بفهمد به کدام سرورها متصل شده‌اید. اگر نخواهید یا نتوانید از HTTPS/TLS استفاده کنید، باید در زمینه محتوای ترافیک‌تان هم به خدمات‌دهنده VPN اعتماد کنید.»

او ادامه می‌دهد: «همچنین سؤالی که مطرح می‌شود این است که آیا تضمینی وجود دارد که فراهم‌کنندگان VPN به سیاست‌های حریم‌شخصی که قول داده‌اند وفادار بمانند؟ یافتن پاسخ این سؤال برای یک فراهم‌کننده خاص نه تنها نیازمند کسب اطلاعات درباره شرکت ارائه‌کننده و قابل اعتماد بودن آن‌ها است، بلکه در بسیاری موارد نیازمند کسب اطلاع از قوانین در زمینه‌های مختلف قضایی است.»

برای نگاه دقیق‌تر به عرضه‌کنندگان مختلف VPN اکرسلی مطالعه فهرست زیر از TorrentFreak را پیشنهاد می‌کند:

https://torrentfreak.com/which-vpn-providers-really-take-anonymity-seriously-111007/

این سایت تعدادی از این شرکت‌ها را براساس میزان ثبت داده‌ها و سیاست‌های حفظ حریم‌خصوصی، فهرست کرده است. البته، به‌طور معمول بررسی ترافیک شما و دسترسی به اطلاعات‌تان یا فروش این اطلاعات به دیگران جزء سیاست‌های این شرکت‌ها نیست، زیرا در چنین صورتی به سرعت مشتریان خود را از دست خواهند داد، اما به هر حال این موضوعی است که باید مراقبش باشید و البته از کنترل شما خارج است. اما یقین بدانید که هیچ خدمات‌دهنده‌ای نمی‌تواند به اندازه سروری که خودتان راه‌اندازی می‌کنید امن باشد، اما به هر حال استفاده از وی‌پن‌های شرکت‌های دیگر هم از استفاده بدون ملاحظه از وای‌فای‌های باز یا اینترنت در مکان‌های عمومی بهتر است. درنهایت در نظر داشته باشید که جدا از نیات و مقاصد ارائه‌کنندگان سرویس‌های VPN هر کدام از آن‌ها هم ممکن است مانند هر شبکه و سیستم دیگری مورد نفوذ قرار گرفته و باعث لو رفتن اطلاعات شما شوند.

قدم اول تنها قدم لازم نیست

استفاده از فناوری‌هایی مانند TLS و VPN برای حفظ امنیت شما در فضای وب ضروری است. بهترین قدمی که می‌توانید برای محافظت از خودتان بردارید شناخت این فناوری‌ها است. اطمینان حاصل کنید که سایت‌هایی که داده‌های ارزشمندتان (نظیر شماره کارت‌های اعتباری، آدرس و گذرواژه‌ها) را در آن‌ها ذخیره می‌کنید از گواهی‌نامه‌های امضا شده معتبر و نوعی از رمزنگاری SSL یا TLS استفاده می‌کنند. اگر به‌صورت معمول با اطلاعات حساس و مهم آن هم در شبکه‌های عمومی سروکار دارید، حتم استفاده از VPN را برای حفظ امنیت داده‌های‌تان در برابر کاربران مشکوک یا نفوذهای احتمالی به این شبکه‌ها مدنظر داشته باشید. حتی اگر این تنها کاری باشد که انجام می‌دهید، باز هم وضعیت بسیار بهتر از حالتی است که من استفاده از اینترنت را شروع کردم!

در بخش بعدی این مجموعه به موضوع بدافزارهای وب خواهیم پرداخت.