رمزنگاری فرصت‌طلبانه

فایرفاکس 37 به چه ویژگی امنیتی تجهیز شده است؟

فایرفاکس از نسخه 3.5 به بعد ویژگی Private Browsing را در اختیار کاربران خود قرار داد. این ویژگی به کاربر اجازه می‌دهد که از گشت و گذار در اینترنت به شیوه امن‌تر و ناشناس‌تری استفاده کند. تاریخ‌چه، جست‌وجوها، گذرواژه‌ها، دانلودها، کوکی‌ها و محتوای کش شده در زمان خاموش کردن سیستم همگی پاک می‌شوند. این کار شانس افرادی که در صدد سرقت هویت یا دسترسی به اطلاعات شخصی هستند را کاهش می‌دهد. اما نسخه 37 به ویژگی دیگری به‌نام رمزنگاری فرصت‌طلبانه (opportunistic encryption) تجهیز شده است.

برای سایت‌هایی که از HTTPS پشتیبانی نمی‌کنند و اساس کار آن‌ها بر مبنای پروتکل ابرمتنی HTTP قرار دارد، فایرفاکس 37 گزینه پشتیبانی ساده‌تری فراهم می‌کند که رمزنگاری فرصت‌طلبانه (opportunistic encryption) یا به اختصار OE نام دارد. نسخه 37 فایرفاکس در تاریخ 31 مارس عرضه شد. با استفاده از این ویژگی پلی میان محتوای متنی غیررمزنگاری شده و محتوای کاملا رمزنگاری شده به ساده‌ترین شکل ممکن پیاده‌سازی می‌شود. اما برای کاربران عادی این ویژگی چه کاربردی دارد؟

رمزنگاری فرصت‌طلبانه به این معنی است که شما به حداقل امنیت و محافظت در مقابل نظارتی که توسط سازمان‌هایی همچون NSA روی ارتباطات انجام می‌شود، می‌رسید. البته در وقتی‌که سایت‌های مقصد از OE پشتیبانی کنند. پاتریک مک مانوس، از توسعه‌دهندگان تیم فایرفاکس، در وبلاگ شخصی خودش توضیحاتی درباره OE ارائه کرده است. او درباره این ویژگی به کار گرفته شده و تعامل آن با پروتکل HTTPS می‌نویسد: « این ویژگی از شما در برابر حمله man-in-the-middle آن‌گونه که پروتکل HTTPS این‌کار را انجام می‌دهد، محافظت نمی‌کند. اما این ویژگی مزایای خوبی برای پروتکل http:// به همراه دارد، اما به خوبی پروتکل Https نیست. زیرا تنها پروتکلی که از شما در برابر حملات فعال man-in-the middle می‌تواند محافظت کند، پروتکل HTTPS است. اگر سایت شما در ارتباط با محتوایی قرار دارد که به شما امکان مهاجرت به https را نمی‌دهد، که در بیشتر موارد در ارتباط و تعامل با محتوای ترکیب شده افراد و گروه‌های سوم شخص قرار دارد، رمزنگاری فرصت‌طلبانه مکانیزمی برای انتقال داده‌ها به شیوه رمزنگاری شده روی پروتکل http را فراهم می‌کند. کاملا روشن است، این مکانیزم جایگزین خیلی مناسب‌تری نسبت به انتقال متن‌ها به شیوه خام است.»

بر خلاف پروتکل HTTPS، رمزنگاری فرصت‌طلبانه از یک ارتباط رمزنگاری شده تصدیق هویت نشده استفاده می‌کند. به عبارت دیگر، یک سایت نیازی به گواهی امنیتی امضاء شده از منابع معتبر به شکلی که برای کارکرد پروتکل HTTPS ضروری است، نیازی ندارد. گواهی امنیتی امضاء شده یک مؤلفه کلیدی در اسکیمای امنیتی همراه با HTTPS است و آن کلیدی است که مرورگرها از آن برای اعتماد به سایت‌هایی که به آن‌ها متصل می‌شوند، استفاده می‌کنند. رمزنگاری فرصت‌طلبانه، یک رمزنگاری تعیین هویت نشده را روی TLS برای داده‌ها به شیوه دیگری غیر از یک متن ساده که باید منتقل شوند فراهم می‌کند. البته پشتیبانی فایرفاکس از این مکانیزم تنها نیمی از راه پیاده‌سازی رمزنگاری فرصت‌طلبانه است. در طرف دیگر این معادله سایت‌ها هستند. سایت‌ها برای این‌که این ویژگی به خوبی عمل کند، باید آن‌را فعال کنند. مالکان سایت‌ها به راحتی طی دو مرحله رمزنگاری فرصت‌طلبانه را می‌توانند روی

سایت‌های خود پیاده‌سازی کنند.

1- نصب یک سرور TLS بر مبنای h2 یا سرور اسپیدی روی یک پورت جداگانه، همچنین در صورت تمایل می‌توانند از یک گواهی خودامضا شده (self-signed certificate) استفاده کنند، به دلیل این‌که رمزنگاری فرصت‌طلبانه تعیین هویت نمی‌شود.

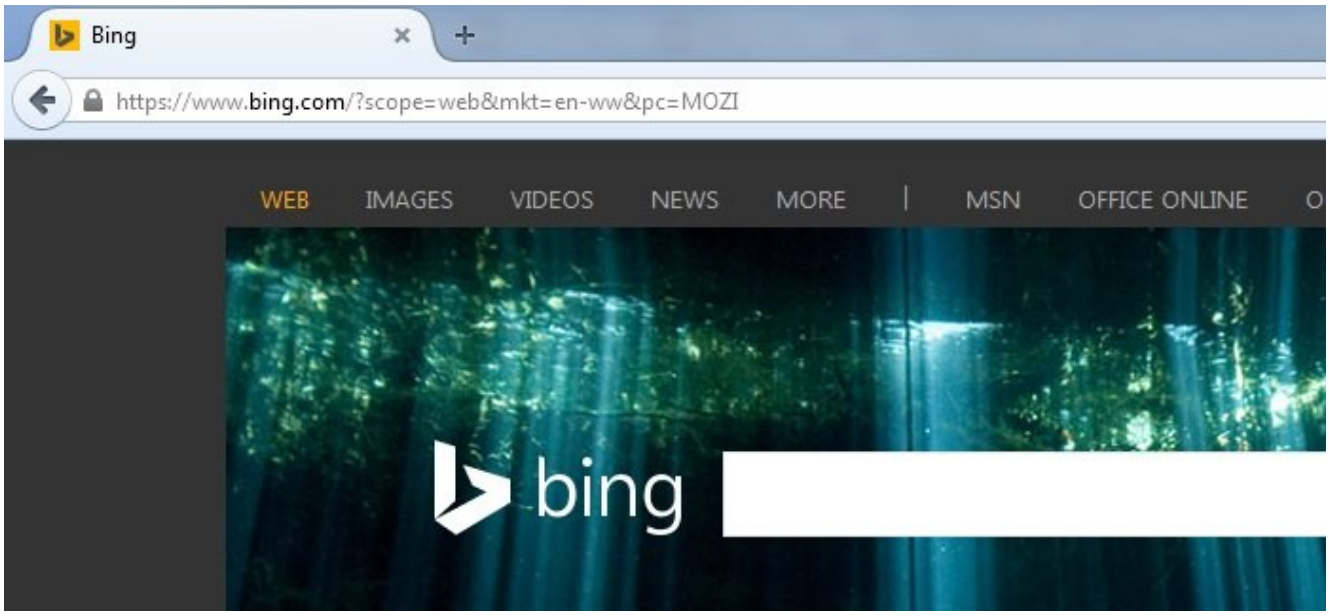
2- اضافه کردن یک سرآیند واکنش/پاسخ (Response) Alt-Svc: h2=":443 " یا اگر از سروری استفاده می‌کنید که اسپیدی روی آن فعال است، همچون ngnx می‌توانید از اسپیدی نسخه 3.1 به عنوان جایگزین دیگر استفاده کنید.

زمانی‌که مرورگر این سرآیند واکنش را مورد استفاده قرار می‌دهد، شروع به بررسی صحت این موضوع که سرویس HTTP2 روی پورت 443 قرار دارد می‌کند. زمانی‌که یک نشست با آن پورت آغاز می‌شود، شروع به مسیریابی درخواست‌هایی که به صورت عادی از پورت ساده 80 ارسال شده‌اند به داخل پورت رمزنگاری شده 430 می‌کند. به عبارت ساده‌تر، داده‌های عادی از پورت 80 به پورت 443 وارد شده و به صورت رمزنگاری شده ارسال می‌شوند. نکته جالب توجه در مورد این مکانیزیم به عدم وجود هیچ زمان تأخیری باز می‌گردد، ، به دلیل این‌که ارتباط جدید به طور کامل در پس‌زمینه و قبل از آن‌که مورد استفاده قرار گیرد منتشر شده و آماده می‌شود. اگر سرویس جایگزین (پورت 443) در دسترس نباشد یا صحت آن مورد تأیید قرار نگیرد، فایرفاکس به طور خودکار از روال عادی استفاده کرده و اقدام به ارسال داده‌ها روی پورت 80 می‌کند. این مکانیزم آماده شده و در آینده مورد استفاده قرار خواهد گرفت. اما توجه به این مسئله مهم است، در حالی‌که تراکنش‌ها به پورت متفاوتی از مبداء مسیریابی می‌شوند، اما منبع اصلی بدون تغییر می‌ماند. یعنی حتی اگر مسیریابی به پورت 443 و روی TLS انتقال یابد باز هم http://www.example.com:80 به عنوان منبع اصلی شناخته می‌شود. رمزنگاری فرصت‌طلبانه با سرورهای HTTP 1 سازگار نیست، به دلیل این‌که این پروتکل اسکیمای لازم را که به عنوان بخشی از تراکنش برای دگرگون‌سازی رویکرد Alt-Svc مورد نیاز است، حمل نمی‌کند.

همچنین، همان‌طور که پیش‌تر اشاره کردیم، هنوز هم به سرور اسپیدی SPDY یا HTTP/2 نیاز است، به گفته سایت آر اس تکنیکا، دسترسی به این سرویس‌ها ممکن است کار ساده‌ای نباشد. در نتیجه در حالی‌که رمزنگاری فرصت‌طلبانه در فایرفاکس یک شروع خوب برای کاربران به شمار می‌رود، اما این ویژگی زمانی رسما آغاز به کار خواهد کرد که مالکان سایت‌ها پشتیبانی از آن‌را آغاز کنند.

فراتر از رمزنگاری فرصت‌طلبانه

فایرفاکس به فراتر از رمزنگاری فرصت‌طلبانه روی آورده است. فایرفاکس نسخه 37 همچنین از راهکارهای جدیدی برای حفاظت در برابر گواهی امنیتی نامعتبر استفاده می‌کند. این ویژگی جدید به نام OneCLR نامیده می‌شود که به موزیلا اجازه می‌دهد، فهرستی از گواهی‌نامه‌های لغو شده را در خود مرورگر داشته باشد، به جای آن‌که به یک بانک‌اطلاعاتی آنلاین وابسته باشد. همچنین، در نسخه 37 فایرفاکس زمانی‌که از پنجره جستجوی از پیش ساخته شده مرورگر استفاده می‌کنید، فایرفاکس HTTPS را به بینگ اضافه می‌کند.



تاریخ انتشار:
22 فروردین 1394

نشانی منبع: https://www.shabakeh-mag.com/security/518