禪

توسط محققان دانشگاه MIT

سریعترین شبکه غیرقابل ردیابی جهان طراحی شد

DSL
LAN1
LAN2
LAN3
TV

به نظر میرسد، ناشناس ماندن این روزها در کانون توجه کاربران دنیای فناوری و شرکتهای تحقیقاتی قرار گرفته است . بر همین اساس پژوهشگران موسسه MIT موفق به ابداع راهکاری در این زمینه شدهاند .

محققان موسسه MIT همراه با گروهی از محققان پلیتکنیک لوزان سوییس موفق به طراحی یک شبکه غیر قابل ردیابی شدند که در مقایسه با نمونههای مشابه نه تنها از کارایی بالاتر بلکه از سرعت بسیار سریعتری نیز برخوردار است . آلبرت کان از محققان این پروژه گفته است : «مورد استفاده اولیه این شبکه زمانی است که در نظر دارید فایلی را به صورت ناشناس به اشتراک قرار دهید . جایی که گیرنده و فرستنده به هیچ شکلی قادر به شناسایی یکدیگر نباشند .»

مطلب پیشنهادی

جدال بر سر آینده

گوگل به مبارزه با هکرهای کوانتومی آینده برخواسته است

این تیم از محققان در نظر دارند گزارش دستاورد خود را در سمپوزیم ارتقا حریم خصوصی در دنیای فناوری که همین ماه برگزار میشود، ارائه کنند . او در بخشی از صحبتهای خود آورده است: «دلیلی که

باعث شد ما دست به خلق این چنینی فناوری بزیم به مشکلاتی باز میگردد که در ارتباط با فناوریهایی همچون هانیپات وجود دارد . ما همچنین به مطالعه برنامههای کاربردی همچون توییتر پرداختیم . مکانی که شاید در نظر داشته باشید پیامهایی را بهطور ناشناس برای طیف گستردهای از کاربران ارسال کنید .»

این شبکه که Riffle نامیده میشود از تاکتیکهای رایج امنیتی استفاده میکند . اما اینکار را به شیوهای کاملا متفاوت از آن چیزی که تا پیش از این مشاهده شده است انجام میدهد . فناوری مرکزی این شبکه که mixnet نامیده میشود متشکل از مجموعهای از سرورها است که ترافیک قبل و بعد از ورود به سرور را قبل از آنکه اقدام به ارسال دادهای کند تغییر میدهد . جالب آنکه خود mixnet نیز توسط یک روتر بازگشتی پنهان میشود . اگر ترافیک از آلیس، باب و کارول باید به اولین گره شبکه و به ترتیب A,B و C برسد، سرور ممکن است ارسال بستهها را به صورت B,A و C انجام دهد . این رویکرد درهم آمیختن باعث شده است تا شبکه Riffle تبدیل به ابزار مخوفی شود . سرورهای تقسیم کننده ترافیک بهطور اتفاقی یک کارت را درآورده و بر مبنای آن عمل میکنند . در کنار تکنیک یاد شده زمانی که یک کاربر پیام یا فایلی را ارسال میکند، این محتوا به جای آنکه در یک سرور ذخیرهسازی شود در سرورهای متعددی ذخیرهسازی میشود. اینکار باعث میشود ردیابی یک پیام در عمل کار بسیار مشکلی باشد . تصویر زیر نحوه به اشتراکگذاری فایل در این شبکه را نشان میدهد .

(a) Setup: Clients share the torrent files anonymously.

(b) Request: Each client requests a file by uploading the hash of the file using Riffle.

(c) Upload: Each client uploads an encrypted file based on the requests using Riffle.

(d) Download: Each client downloads the file he or she requested using PIR.

Fig. 2. Anonymous File Sharing Protocol

هر گره قرار گرفته در این شبکه خود متشکل از یک لایه رمزنگاری شده است . حال این سوال پیش میآید که آیا Riffle غیر قابل شکستن است؟ به لحاظ فنی باید بگوییم شکستن این شبکه کار بسیار مشکلی است، اما واقعیت این است که هیچ سامانهای در جهان وجود ندارد که دست نیافتنی باشد . در بیشتر موارد اهرمهای مختلفی وجود دارند که مدیران اجرایی یک سامانه را مجبور میسازد به درخواستهایی در خصوص کشف پیامها جواب مثبت دهند . همچنین هر سامانهای آسیبپذیریهای مختلفی را در دل خود جای داده است که به افراد حرفهای اجازه میدهد از طریق این حفرهها به سامانهها وارد شوند . زمانی که یک شبکه حتا یک شبکه ناشناس جزییات مختلفی را درباره یک کاربر حتا به صورت پراکنده جمعآوری میکند، این پتانسیل را به وجود میآورد تا یک کارشناس حرفهای با چینش اطلاعات در کنار یکدیگر این توانایی را به دست آورد تا موقعیت یک کاربر را شناسایی کند .

نویسنده :
حمیدرضا_تائبی
دسته بندی:
امنیت
تاریخ انتشار :
17:02 - 03/05/1395
برچسب:
امنیت - شبکه_پنهان - MIT - mixnet - Riffle

□□□□□ منبع: https://www.shabakeh-mag.com/security/3896