فصلنامه علمی تخصصی ایده های نو در علوم، مهندسی و فناوری ، دوره ۷، شماره ۱، بهار ۱۴۰۲، ص ۱۰-۱
ISSN: 2588-3984
http://www.Tajournals.com

عنوان مقاله: بررسی روش‌های حمله به شبکه Tor
دوره ۷/ شماره ۱ / بهار ۱۴۰۲/ ص ۱۰ – ۱

بررسی روش‌های حمله به شبکه Tor

اصغر اخلاق‌عالی۱ و کورش داداشتبار احمدی ۲
۱دانش آموخته کارشناسی ارشد برق – مخابرات امن و رمزنگاری دانشگاه صنعتی مالک اشتر واحد تهران
Akhlaghale1370@gmail.com
۲استادیار دانشکده برق و کامپیوتر دانشگاه صنعتی مالک اشتر واحد تهران
Dadashtabar@mut.ac.ir

چکیده

در سال‌های اخیر، مفهوم حریم خصوصی در اینترنت به عنوان نگرانی افراد در خصوص مانیتورینگ و نظارت بر ارتباطات دیجیتالی آن‌ها، توجه بیشتری را به خود جلب کرده است. برای حفظ ناشناسی و حفاظت از حریم خصوصی و سلامت کامل ارتباطات، ابزارهای قابل اطمینانی مانند Tor[1] طراحی و پیاده‌سازی شده است. Tor به کاربران این امکان را می‌دهد تا به صورت ناشناس در اینترنت از طریق یک شبکه از رله‌ها مرور کنند، اما کاربران با استفاده از این ابزار همچنان ممکن است در برابر حملات کورلیشن ترافیکی آسیب‌پذیر باشند که توسط دشمنانی که رله‌های Tor را نظارت می‌کنند و فایل‌های لاگ Tor را تجزیه و تحلیل می‌کنند، انجام می‌شود.

هدف این تحقیق، بهبود درک تهدید حملات کورلیشن ترافیکی بر روی کاربران Tor با توسعه مدل تهدیدی از چنین دشمنانی است. این مدل شیوه‌ها و روش‌های مختلفی را در نظر می‌گیرد که یک دشمن برای انجام حملات کورلیشن ترافیکی روی کاربران Tor ممکن است به کار ببرد. برای ارزیابی عملکرد روش‌های مختلف کورلیشن، از ابزار شبیه‌ساز Shadow برای شبیه‌سازی شبکه Tor در مقیاس کوچکتر استفاده شده است. عملکرد روش‌های مختلف با در نظر گرفتن مدل‌های مختلف کلاینت، ارزیابی شده و نتایج برای تعیین روش مناسب‌تر برای دشمن مورد استفاده قرار گرفته‌اند.

کلمات کلیدی: دارک وب، دیپ وب، تور، حمله، همبستگی

[1] The Onion Router

مقدمه

ما در عصر اطلاعات زندگی می‌کنیم که در آن هر شخصی که به اینترنت متصل است، تمام اطلاعات جهان را در دستان خود دارد. در حالی که اینترنت امکان اشتراک‌گذاری اطلاعات را گسترش داده است، اما بسیاری از کاربران را نگران کرده که اطلاعات خصوصی آنها، از جمله فعالیت وب‌گردی، بدون اجازه و اطلاع‌شان ردیابی شود. با افزایش نگرانی‌ها در مورد حریم خصوصی و امنیت، کاربران اینترنت به دنبال راه‌هایی برای ناشناس کردن ترافیک شبکه خود هستند. ذکر Tor به سال ۱۹۹۵ بر می‌گردد [۱]، زمانی که دفتر تحقیقات نیروی دریایی ایالات متحده[۲] به همراه آژانس پروژه‌های تحقیقاتی پیشرفته دفاعی[۳](DARPA) روی توسعه نوع جدیدی از فناوری کار کردند که ردیابی ترافیک به آنها را دشوار می‌کرد. این ایده مبتنی بر عبور ترافیک از طریق گره-های تصادفی قبل از رسیدن به مقصد بود. هدف از این کار ایجاد سردرگمی در مورد اینکه فرستنده و مقصد مورد نظر چه کسی است، و از این طریق شناسایی مقصد نهایی ارتباط را دشوار می‌کرد. هدف از توسعه این فناوری در ابتدا تقویت حریم خصوصی نبود، بلکه ایجاد امکان برای افراد جاسوس جهت برقراری ارتباط ناشناس بدون ترس از دستگیری بود. Tor بزرگترین شبکه ارتباطی در وب تاریک است که از آن برای گمنام‌سازی (پنهان‌سازی) ارتباط بین کاربر و سرور استفاده می‌شود. تاکنون تحقیقات بسیاری آسیب‌پذیری‌های شبکه تور را مورد بررسی قرار داده‌اند و کارایی و موفقیت آن را به چالش کشیده‌اند. سرویس مخفی (HS) [۴] یک سرویس شبکه است که مکان سرورهای آن توسط شبکه Tor مخفی می‌شود. با ظهور سرویس‌های مخفی Tor، امکان راه‌اندازی سایت‌هایی که قابل ردیابی نباشند فراهم گردید و در واقع گمنام‌سازی دو طرفه گردید. این سایت‌ها محل مناسبی برای انجام کسب و کارهای غیره قانونی تبهکارانه است که یکی از نیازهای اصلی سازمان‌های قانونی، شناسایی و در واقع غیرگمنام‌سازی این سایت‌ها است. با وجود اینکه هدف اصلی راه‌اندازی سرویس‌های مخفی گمنام‌سازی است، اما مانند هر سرویس امنیتی دیگری آنها نیز آسیب‌پذیری‌هایی دارند. سرویس‌های مخفی Tor به طور فزاینده‌ای با حملات غیرگمنام‌سازی مورد حمله قرار می‌گیرد. با گذشت زمان، حملات پیچیده‌تر و مؤثرتر شده‌اند و نیاز به حملات ترکیبی افزایش یافته است که می‌تواند در لایه شبکه، لایه پروتکل یا لایه برنامه انجام شود.

فضای وب

امروزه بدون اغراق تمامی اطلاعاتی که بیشتر افراد کسب می‌کنند با واسطهٔ یا بدون واسطهٔ از طریق اینترنت وموتورهای جستجو می‌باشد. اما این چیزی که در دسترس کاربران قرار دارد تنها ۴٪ [۲] تمام اطلاعات می‌باشد که به اصطلاح وب آشکار[۵]گفته می-شود. وبقیه اطلاعات که در دسترس موتور جستجو قرار ندارد واین موتورها نمی‌توانند آنها را کاوش کنند وب عمیق[۶]نام دارد. وب عمیق یا به تشخیص موتورهای جستجو کاوش نمی‌شود مانند مشخصات شخصی، نام وشماره تلفن ویا توسط برنامه نویسان برای انجام کارهای مخفی مورد استفاده قرار می‌گیرد که در این صورت به آن وب تاریک می‌گویند.

نیمی از فعالیت‌هایی که در وب تاریک اتفاق می‌افتد غیر قانونی است مانند: خرید و فروش مواد مخدر و اسلحه، خرید و فروش برده های جنسی و حتی آزار جسمی و جنسی انسان‌ها به صورت آنلاین که در این بُعد از اینترنت بدون جا گذاشتن ردی از افراد صورت می‌پذیرد. البته در بعضی مواقع این وب تاریک کاربردی نیز می‌باشد به عنوان مثال: فعالان خبرنگاری و فعالان سیاسی در کشورهایی که تحت سانسور شدید اینترنتی قراردارند می‌توانند بدون جا گذاشتن هیچ رد پایی از خود از این روش بهره‌مند شوند. این بُعد از اینترنت در ابتدا توسط نیروی دریایی ایالات متحده آمریکا مورد استفاده قرار گرفت [۳].

در اغلب موارد شبکه دارک وب با دیپ وب همسان شمرده می‌شود اما در حقیقت این دو شبکه با هم تفاوت دارند و هر دو در یک موضوع و زمینه خاصی فعالیت نمی‌کنند. به طور خلاصه وب‌عمیق به تمام وبسایت‌هایی گفته می‌شود که از طریق موتورهای

[2] US Office of Naval Research
[3] Defense Advanced Research Projects Agency
[4] Hidden Service
[5] surface web
[6] Deep Web

فصلنامه علمی تخصصی ایده های نو در علوم، مهندسی و فناوری ، دوره ۷، شماره ۱، بهار ۱۴۰۲، ص ۱۰-۱
ISSN: 2588-3984
http://www.Tajournals.com

جستجوگر نمی‌توان به آن‌ها دسترسی پیدا کرد به بیان دیگر وبسایت‌هایی که موتورهای جستجو قادر به بایگانی کردن صفحاتشان نیستند در دسته وب عمیق قرار می‌گیرند. بنابراین دارک وب را در حقیقت باید زیر مجموعه‌ای از وب عمیق دانست. اما دارک وب به طور کل از نظر تکنیک‌های ارائه شده در این شبکه با وب عمیق متفاوت است، در اینجا منظور از تکنیک‌ها مجموعه‌ای از محصولات و خدمات می‌باشد که برای همه کاربران اینترنت مورد استفاده قرار نمی‌گیرد و فقط بخشی از کاربران خواهان دستیابی به این محصولات و خدمات هستند که برای مثال می‌توان به وبسایت‌های خرید و فروش مواد مخدر، شرطبندی‌های غیر قانونی، وبسایت‌های کودک آزاری، خرید و فروش سلاح‌های گرم و سرد و ... اشاره کرد. پس در واقع وبسایت‌های حاوی خدمات و محصولات غیر مجاز در دیپ وب را با نام دارک وب معرفی می‌کنند [۲].

شبکه دیپ وب در کشورهای تمامیت‌خواه معمولا برای دسترسی آزاد و بدون مشکل به شبکه جهانی وب و همچنین به منظور شناسایی نشدن مورد استفاده قرار می‌گیرد ولی این موضوع بدین معنا نیست که این شبکه فقط در چنین جوامعی مورد استفاده قرار می‌گیرد، بلکه در کشورهای دموکراتیک نیز این شبکه حتی از جوامع توتالیته هم بیشتر کاربرد دارد که یکی از مهمترین دلایل استفاده از این سرویس در چنین کشورهایی، افشاگری‌های مختلف در خصوص شنود و زیر پا گذاشتن حریم خصوصی کاربران توسط دولت‌ها است [۴].

با توجه به توضیحات داده شده در خصوص وب عمیق و وب تاریک به این نتیجه خواهیم رسید که استفاده از هر کدام نیاز به سواد مخصوص خود را دارد. در میان این حجم افسار گسیخته اطلاعات و دسترسی به اینترنت شاید طوری هدایت شویم که تبدیل به یک ابزار برای بازی دارک وبی‌ها باشیم حتی بدون اینکه اطلاعی از آن داشته باشیم. این روزها جرائم به سمت سایبری شدن می-رود چنانچه جنگ‌ها هم به این سو رفته به همین منظور داشتن سواد دیجیتال برای هر رده سنی و شغلی بسیار مهم است.

شکل ۱: تقسیم بندی فضای وب

معرفی شبکه Tor

Tor یک سرویس ارتباطی ناشناس با تأخیر کم است که در برابر حملات اولیه تجزیه و تحلیل ترافیک محافظت می‌کند [۳].

هدف از توسعه TOR

هدف اولیه از توسعه Tor ایجاد یک شبکه با تأخیر کم بود که بتواند ارتباط آنلاین را ناشناس کند. و برای محافظت از ارتباطات از پروتکل نوع TCP استفاده می‌شود. هنگام برقراری ارتباط با استفاده از پروتکل‌های TCP/IP، بسته حاوی داده‌ها، آدرس‌های IP و پورت‌های مبدا و مقصد است [۵]. و حتی اگر داده‌ها رمزگذاری شده باشند، مهاجم همچنان می‌تواند تشخیص دهد که هر دو طرف ارتباط چه کسانی هستند و بر اساس تجزیه و تحلیل ترافیک، می‌تواند اطلاعات بیشتری مانند ماهیت ارتباط را بدست آورد. هدف اصلی Tor جلوگیری از این اتفاق است. علاوه بر آن، توسعه دهندگان Tor برخی از اهداف طراحی را در مقاله ۲۰۰۴ [۳] خود پیشنهاد کردند برخی از این اهداف عبارت‌اند از:

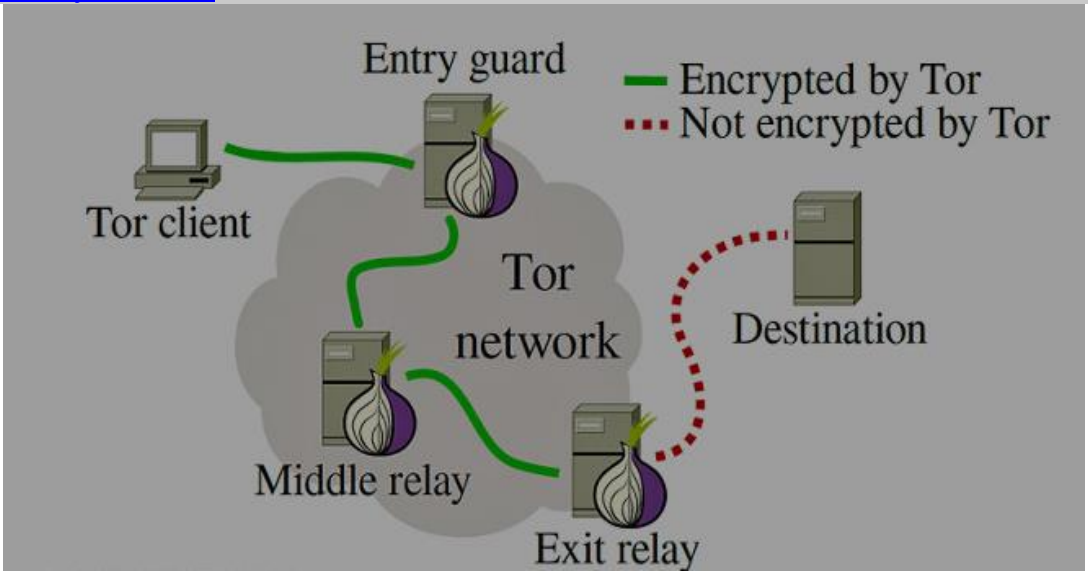
- قابلیت استقرار: از آنجایی که طراحی Tor وابسته به داوطلبانی است که رله‌های فردی را اجرا می‌کنند، نباید گران باشد و باید نصب و راه‌اندازی آن آسان باشد. Tor نباید از اپراتورهای رله بخواهد که هویت خود را اعلام کنند.
- قابلیت استفاده: در شبکه Tor هرچه تعداد کاربران و اپراتورهای رله بیشتر باشد ایمن‌تر می‌شود. بنابراین برای Tor ضروری است که کاربر پسند باشد، زیرا یک سیستمی که سطح کاربری سختی دارد کاربران کمتر از آن استفاده می‌کنند. یعنی باید این قابلیت را داشته باشد که هر کاربر Tor بتواند با هر سیستم عامل استانداردی به راحتی از آن استفاده کند.
- انعطاف‌پذیری: پروتکلی که در شبکه برای برقراری ارتباط استفاده می‌شود باید به خوبی مشخص و منعطف باشد، بنابراین می‌توان آن را در تحقیقات دیگر در مورد شبکه‌های ناشناس با تأخیر کم به کار برد.
- طراحی ساده: طراحی پروتکل باید به راحتی قابل درک باشد. و باید از ویژگی‌های اثبات نشده و پیچیده در طراحی پروتکل وجود نداشته باشد.

Tor شبکه‌ای است که امکان مخفی‌سازی هویت کاربران را در فضای اینترنت فراهم می‌کند و از دسترسی سیستم‌های نظارتی، مکان‌یاب و غیره به حریم خصوصی کاربران جلوگیری می‌کند، برای اتصال به این شبکه امنیتی نیاز به نسخه‌ای خاص و تغییریافته از مرورگر فایرفاکس است که تحت‌عنوان توربروزر[7]شناخته می‌شود.

نحوه کارکرد Tor بدین صورت است که با مفهومی تحت‌عنوان اونیون روتر (مسیر پوست‌پیازی) ابتدا اطلاعات کاربر رمزنگاری می‌شود سپس در بین رِله‌های مختلفی که در شبکه Tor وجود دارد جابجا می‌شود. همچنین رمزنگاری چندلایه باعث می‌شود هویت کاربر مخفی بماند، برای درک بهتر سازوکار Tor، همان‌طور که در شکل ۲ ملاحظه می‌کنید، مشابه لایه‌های مختلف یک پیاز عمل می‌کند:

[7] Tor Browser

فصلنامه علمی تخصصی ایده های نو در علوم، مهندسی و فناوری ، دوره ۷، شماره ۱، بهار ۱۴۰۲، ص ۱۰-۱
ISSN: 2588-3984
http://www.Tajournals.com



شکل ۲: شبکه Tor

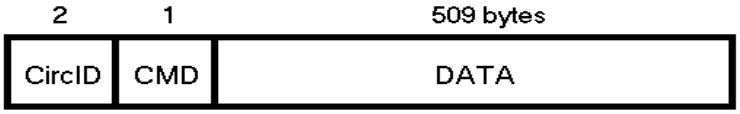
پروتکل Tor

Tor یک شبکه همپوشانی است، به این معنی که ORها با هم یک شبکه مجازی ایجاد می‌کنند که بر روی یک شبکه فیزیکی دیگر، در این مورد، اینترنت ساخته شده است [۶]. ORهای فردی با استفاده از پروتکل TLS [۷] با یکدیگر ارتباط برقرار می‌کنند. هر کلاینت یک پروکسی به نام onion proxy (OP) اجرا می‌کند که اتصالات به ORها را مدیریت می‌کند و با استفاده از پروتکل SOCKS4 با برنامه‌های کاربردی کاربر ارتباط برقرار می‌کند. سرورهای دایرکتوری رله‌هایی هستند که اطلاعات مربوط به شبکه را نگه می‌دارند و آن را در اختیار OPها و سایر OR ها قرار می‌دهند تا بتوانند به هم متصل شوند و یک مسیر معتبر از طریق شبکه ایجاد کنند.

سلول‌ها

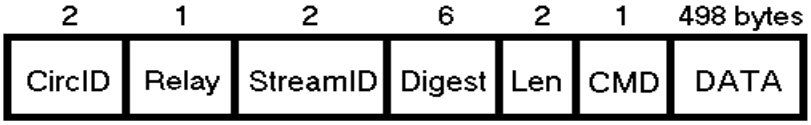
در پروتکل Tor سلول‌ها به عنوان یک واحد ارتباطی تعریف می‌شوند. هدف اولیه از ارسال داده‌ها از طریق سلول‌ها جلوگیری از حملات اولیه تجزیه و تحلیل ترافیک است. توسعه دهندگان پروژه Tor تغییراتی را از نسخه ۱ پروتکل Tor انجام دادند، اما هسته اصلی طراحی ثابت ماند. علاوه بر این، پروتکل‌های Tor جدید با پروتکل‌های قدیمی سازگار هستند.

در نسخه ۲ یا بالاتر، در ادامه فیلد فرمان یک فیلد طول بار سلور را مشخص می‌کند [۳]. در Tor، هر ترافیکی که بین دو وسیله ارتباطی (بین دو اونیون روتر یا بین یک اونیون پروکسی و یک اونیون روتر) وجود دارد همیشه به سلول‌هایی با اندازه ثابت (۵۱۲ بایت) تقسیم می‌شود تا تجزیه و تحلیل ترافیک سخت‌تر شود [۷]. این واحدهای ارتباطی از یک هدر و یک بار تشکیل شده‌اند. هدر حاوی یک شناسه مدار (circID) است که مشخص می‌کند سلول به کدام مدار اشاره دارد و یک شناسه فرمان (CMD) که نحوه تفسیر سلول را توضیح می‌دهد. با توجه به مقدار شناسه فرمان، یک سلول را می‌توان به عنوان یک سلول کنترل (شکل ۳) یا به عنوان یک سلول رله (شکل ۴) تفسیر کرد.



شکل ۳: سلول کنترل

سلول‌های کنترل عمدتاً برای راه‌اندازی مدارهای جدید و از بین بردن مدارهای موجود استفاده می‌شوند. ایجاد یک مدار همیشه به تبادل دو سلول کنترل نیاز دارد. اول از همه، یک سلول ایجاد می‌کند که به روتر پیاز اطلاع می‌دهد که یک مدار جدید قصد دارد آن را به عنوان یکی از سه جهش خود اضافه کند.



شکل ۴: سلول رله

با توجه به سلول‌های رله، از آنها برای حمل داده‌های جریان سرتاسر استفاده می‌شود. در مقایسه با سلول‌های کنترلی، سلول‌های رله دارای یک هدر اضافی (به نام هدر رله) هستند که در جلوی بلوک بارگذاری (به نام رله بارگذاری) قرار دارد. این هدر حاوی اطلاعات مفیدی در مورد سلول است، مانند فیلد streamID که نشان می‌دهد سلول به کدام جریان تعلق دارد (بسیاری از جریان‌ها را می‌توان در یک مدار مالتی پلکس کرد). فیلد دایجست حاوی نتیجه جمع کنترلی و فیلد لن که اندازه بار رله را در خود دارد و در نهایت، فیلد فرمان رله که وظیفه اختصاص داده شده به سلول را مشخص می‌کند. فیلد فرمان می‌تواند مقادیر زیادی داشته باشد:

- شروع: برای باز کردن یک رشته جدید.
- پایان: برای بستن یک رشته به طور کامل.
- اتصال: برای اطلاع دادن به پروکسی پیاز هنگام برقراری جریان.
- Extend: برای گسترش مدار توسط یک پرش.
- Extended: برای تصدیق گسترش مدار.
- داده: برای حمل برخی از داده‌ها

Entry Node/Guard: این رله‌ای در شبکه Tor است که کاربر مستقیماً به آن متصل می‌شود و از این رو، آدرس پروتکل اینترنت (IP) کلاینت را می‌داند. بنابراین، در حمله اولیه Tor یا گره‌های ورودی موجود را به خطر می‌انداختند یا گره‌های مخربی را به عنوان گره‌های ورودی نصب می‌کردند تا کاربر آن را به عنوان گره ورودی انتخاب کند و به واسطه آن او را غیرگمنام کنند. یکی دیگر از ویژگی‌های مهم گره‌های ورودی با معرفی گره‌های نگهبان به وجود آمد. از آنجایی که Tor اغلب مدارهای جدیدی را ایجاد می‌کند، همیشه این شانس وجود دارد که یک گره کنترل شده توسط دشمن را به عنوان گره ورودی انتخاب کند. شبکه Tor گره‌های محافظ را برای کاهش احتمال این اتفاق معرفی کرد. اکنون، OP ها مجموعه کوچکی از گره‌های قابل اعتماد را به عنوان گره‌های نگهبان انتخاب می‌کنند و تنها از یکی از این گره‌ها به عنوان گره ورودی برای همه مدارها استفاده می‌کنند تا زمانی که آنها (OPs) مجموعه متفاوتی از گره‌ها را به عنوان محافظ انتخاب کنند. DS ها پس از در نظر گرفتن پهنای باند، زمان آپدیت و زمان آن در شبکه Tor، یک پرچم نگهبان را به یک گره اختصاص می‌دهند. شرط لازم برای اینکه یک گره در شبکه به عنوان گره نگهبان انتخاب شود این است که هشت روز از زمان پیوستنش به شبکه Tor بگذرد [۸].

Introduction Points: اینها گره‌های تصادفی هستند که توسط HS برای ثبت خدمات خود در شبکه Tor انتخاب می‌شوند. برای جلوگیری از هرگونه تأثیر حملات احتمالی انکار سرویس (DOS) علیه یک نقطه شروع، HS معمولاً چندین مورد از آنها را انتخاب می‌کند. سپس HS این نقاط معرفی انتخاب شده و کلید عمومی خود را در فهرست راهنمای سرویس‌های مخفی (HSDirs) تبلیغ می‌کند. نقاط معرفی آدرسIP HS را نمی‌دانند زیرا از طریق یک مدار کامل Tor متشکل از چندین رله میانی به HS متصل می‌شوند.

انوع حملات انجام شده به Tor

بررسی‌های زیادی در مورد حملات انجام شده به Tor صورت گرفته است که به دنبال غیرگمنام‌سازی ارتباط برقرار شده از طریق شبکه Tor می‌باشد. اکثر این حملات براساس تجزیه و تحلیل ترافیک می‌باشند. چنین حملاتی برای اینکه مشخص کنند که آیا کاربر از شبکه Tor استفاده می‌کند یا خیر میزان شباهت بین ترافیک ارسالی از سمت کاربر به ورودی مقصد را تجزیه و تحلیل می‌کنند [۴].

حملات غیرگمنام‌سازی[8]
حملات اختلال شبکه[9]
حملات سانسور
حملات عمومی
حملات تایید ترافیک
حملات همبستگی
حملات زمان‌بندی
حملات واترمارکینگ

شبیه سازی شبکه Tor

وقتی نوبت به انجام تحقیقات روی شبکه Tor می‌رسد، یک رویکرد آشکار اعمال مستقیم تغییرات ناشی از موضوع تحقیق در شبکه زنده Tor است. با این حال، کار مستقیم روی شبکه Tor زنده توصیه نمی‌شود زیرا ممکن است به طور ناخواسته به عملکرد و ناشناس بودن کاربران زنده آسیب برساند. بنابراین، یک رویکرد بهتر شامل استفاده از ابزارهای آزمایشی برای ساخت شبکه‌های خصوصی Tor در مقیاس کوچک است [۹].

Shadow یک شبیه ساز رویداد گسسته است که برای اجرای برنامه‌های واقعی مانند Tor بر روی یک ماشین طراحی شده است. به گفته توسعه‌دهنده آن، دقت شبیه‌سازی را با کارایی و کنترل شبیه‌سازی ترکیب می‌کند و بهترین هر دو رویکرد را به دست می‌آورد.

به طور پیش‌فرض، Shadow با یک تولیدکننده ترافیک پایه به نام tgen ارائه می‌شود که این امکان را فراهم می‌کند تا رفتارهای ترافیکی ساده کاربران مانند دانلود انبوه و گشت و گذار اولیه در وب شبیه‌سازی شود. متأسفانه، این مولد ترافیک واقعاً برای ایجاد رفتار ترافیکی پیچیده‌تر مانند ارتباطات IRC و SSH مناسب نیست. برای غلبه بر این مشکل، یک پلاگین جدید برای پخش مستقیم ردیابی‌های ترافیک IRC و SSH در شبکه شبیه‌سازی شده Tor طراحی شده است. این افزونه وظیفه ایجاد دو همتای مجزا را بر عهده دارد که ترافیک TCP ذخیره شده در فایل‌های pcap را دوباره پخش می‌کنند. یک همتا به عنوان کاربر و دیگری به عنوان همتای راه دور اتصال عمل می‌کند. کلاینت ترافیک در نظر گرفته شده برای همتای راه دور را ارسال می‌کند، همتای راه دور ترافیک در نظر گرفته شده برای کاربر را با توجه به محتوای فایل‌های pcap ارسال می‌کند. بنابراین، هر ترافیک TCP که فقط دو همتا را شامل می‌شود، می‌تواند در Shadow بازتولید شود. علاوه بر این، دست دادن پراکسی Socks برای اجازه دادن به همتایان برای ارسال ترافیک خود از طریق شبکه Tor شبیه‌سازی شده‌است. اطلاعات دقیق‌تر و پیاده سازی در مخزن افزونه‌های Shadow Github موجود است [۴].

[8] De-anonymisation attacks
[9] Network Disruption attacks

راه اندازی شبیه سازی

به منظور مطالعه امکان‌سنجی و عملکرد حمله توسعه‌یافته بسته به مدل کاربر از چهار توپولوژی (یعنی balk، web، SSH، IRC)، برای هر نوع ترافیک، با استفاده از نسخه اصلاح‌شده اسکریپت generate.py ایجاد شد. با شدو این اسکریپت تضمین می‌کند که هر شبیه‌سازی تا حد امکان از رفتار شبکه واقعی Tor تقلید می‌کند.

- ۹ رله گارد
- ۲ رله گارد خروج
- ۳۳ رله وسط
- ۴ رله خروجی
- ۲ مقام دایرکتوری

تعداد کاربران در توپولوژی‌ها برابر است. این ابتدا با ایجاد یک توپولوژی وب با ۵۰۰ کلاینت انبوه انجام شده است. این میزان کلاینت‌های bulk است که تقریباً تمام رم موجود دستگاه را مصرف می‌کنند. سپس بر اساس توان کل در توپولوژی bulk، یک توپولوژی web با ۵۰۰ کلاینت وب، یک توپولوژی IRC با ۵۰۰ کاربر IRC و یک توپولوژی SSH با ۵۰۰ کلاینت SSH راه اندازی شده است. از آنجایی که کلاینت‌های Web، Irc و ssh ترافیک کمتری نسبت به کلاینت‌های bulk تولید می‌کنند، چند bulk با بارگذاری بالا در آن توپولوژی‌ها اضافه شده است تا کمبود بار شبکه را جبران کند. برای به دست آوردن نتایج قابل اعتماد، دو توپولوژی از هر نوع تولید و شبیه‌سازی شده است که در مجموع ۸ شبیه سازی را ارائه می‌دهد و ۱۰۰۰ مشتری از هر نوع را جمع‌آوری می‌کند.

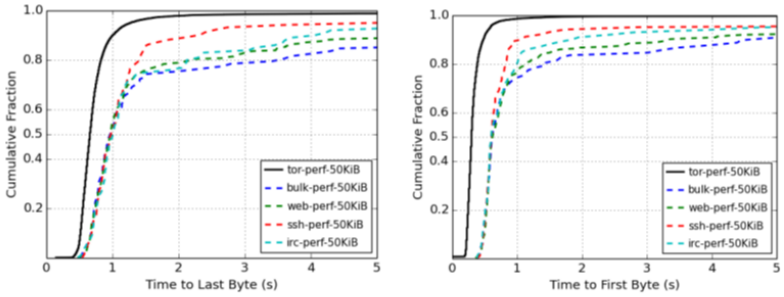
علاوه بر این، به منظور مقایسه عملکرد شبیه‌سازی‌ها با شبکه Tor زنده، هر شبیه‌سازی شامل تعدادی کلاینت خاص است که عملکرد شبکه را اندازه‌گیری می‌کنند. آنها به گونه‌ای پیکربندی شده‌اند که به صورت تصادفی و مکرر فایل‌های ۵۰ KB ، MB ۱ یا ۵ MB را از سرورهای مختلف دانلود کنند. هر کاوشگر آمار دانلود خود را ثبت می‌کند (به عنوان مثال زمان تا بایت اول، زمان تا آخرین بایت). این آمارها با آمارهای شبکه Tor مقایسه می‌شوند تا اطمینان حاصل شود که شبیه‌سازها یک رفتار ثابت را اتخاذ می‌کنند.

تجزیه و تحلیل شبیه سازی

این بخش به بررسی عملکرد شبکه‌های شبیه‌سازی شده در مقایسه با شبکه زنده Tor اختصاص دارد. از آنجایی که کارایی حمله همبستگی توسعه‌یافته مستقیماً تحت تأثیر عملکرد شبکه است، اطمینان از اینکه شبیه‌سازی‌های Shadow تا حد امکان نزدیک به شبکه زنده رفتار می‌کنند بسیار مهم است. در واقع، به نوعی، هر چه شبیه‌سازی‌ها دقیق‌تر باشند، نتایج حملات قابل اعتمادتر هستند.

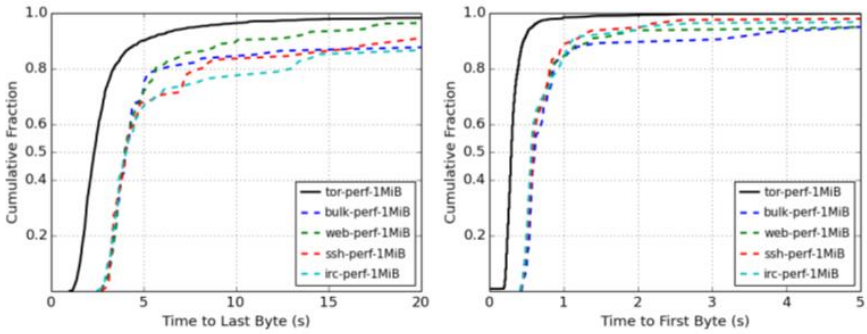
زمان دانلود اولین و آخرین بایت بارگیری به ترتیب نشانگر خوبی از تأخیر و توان عملیاتی شبکه است. شکل ۵، شکل ۶ و شکل ۷ به ترتیب زمان دانلود اولین و آخرین بایت از بار را هنگام دانلود فایل‌های ۵۰ کیلو بایت، ۱ مگابایت و ۵ مگابایت نشان می‌دهند. خطوط پررنگ نشان دهنده اندازه‌گیری‌های شبکه Tor زنده و خطوط نقطه چین اندازه گیری‌های شبیه‌سازی برای حالت‌های مختلف شبیه سازی است. همانطور که در نمودارها مشاهده می‌شود، زمان دانلود اولین بایت پیلود در شبکه زنده کاملاً شبیه به زمانی است که در شبیه‌سازی‌ها مشاهده شده است. این بدان معنی است که شبیه‌سازی‌ها به اندازه کافی تأخیر شبکه زنده را تقریب می‌زنند. از طرفی به نظر می‌رسد در شبیه‌سازی‌ها دانلود فایل‌ها زمان بیشتری می‌برد. این نشانه آن است که در شبکه شبیه‌سازی شده بیش از حد ترافیک بارگذاری شده است. با این حال، همه شبیه‌سازی‌ها با هر نوع کلاینت شبیه‌سازی شده کاملاً یکسان عمل می‌کنند. این تضمین می‌کند که نتایج حملات همبستگی برای یک شبیه‌سازی معین با نتایج به‌دست‌آمده از شبیه‌سازی‌های دیگر مشابه می‌باشد.

فصلنامه علمی تخصصی ایده های نو در علوم، مهندسی و فناوری ، دوره ۷، شماره ۱، بهار ۱۴۰۲، ص ۱۰-۱
ISSN: 2588-3984
http://www.Tajournals.com



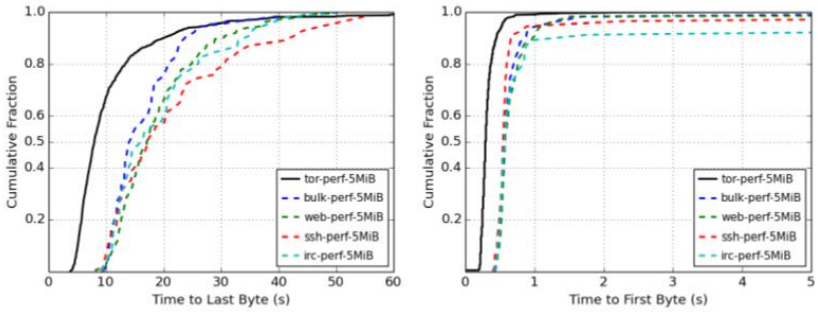
الف: ۵۰ کیلو بایت – زمان تا اولین بایت ب: ۵۰ کیلوبایت – زمان ماندن بایت

شکل ۵: زمان دانلود فایل ۵۰ کیلو بات



الف: ۱ مگابایت – زمان تا اولین بایت ب: ۱ مگابایت – زمان برای آخرین بایت

شکل ۶: زمان دانلود فایل ۱ مگا بایتی



الف: ۵ مگابایت – زمان برای اولین بایت ب: ۵ مگابایت – زمان برای آخرین بایت

شکل ۷: زمان دانلود فایل ۵ مگا بایتی

تجزیه و تحلیل انجام شده نشان می‌دهد که شبیه سازی انجام شده شبکه Tor در نرم‌افزار Shadow تا ۸۰ درصد به شبکه واقعی Tor نزدیک است. یا بطور دقیق‌تر می‌توان گفت که میزان تاخیر شبکه شبیه‌سازی شده بسیار به شبکه Tor واقعی نزدیک است. با این حال، به نظر می‌رسد که در شبیه‌سازی‌ها ترافیک بارگذاری شده کمی بیش از حد است، اما با توجه به اینکه ارتباطات شبیه‌سازی‌شده باید مانند شبکه‌های واقعی حداقل تحت تأثیر منفی قرار گیرند، مشکل بزرگی نیست. این تضمین می‌کند که نتایج حملات توسعه‌یافته سازگار و قابل اعتماد هستند و تا حد امکان رفتاری مشابه یا نزدیک شبکه واقعی داشته باشد. علاوه بر آن، تجزیه و تحلیل عملکرد به دشمن احتمالی بینش‌هایی در مورد نحوه انجام حمله او می‌دهد. در واقع، از آنجایی که زمان تا بایت اول تقریب خوبی از میانگین RTT مشاهده شده در شبکه می‌دهد، مهاجم می‌تواند به راحتی تاخیر شبکه‌ای را که برای یک حمله همبستگی موفق‌تر استفاده می‌کند، پیش‌بینی کند. اگر نیم ثانیه طول بکشد تا درخواست به سرور راه دور برسد و اولین بایت بار در کاربر دریافت شود، تقریباً ۲۵۰ میلی ثانیه طول می‌کشد تا اولین بایت‌ها از سرور به کاربر منتقل شوند. بنابراین،

جریان‌های بایتی مشاهده شده در رله‌های خروجی، به طور متوسط تقریباً ۲۵۰ میلی ثانیه از جریان‌هایی که در رله‌های ورودی مشاهده می‌شوند، به تأخیر می‌افتند. مهاجم می‌تواند از این مقدار برای اصلاح حمله خود و افزایش دقت همبستگی استفاده کند.

منابع

[۱] B. Evers *et al.*, "Thirteen Years of Tor Attacks," ed, ۲۰۱۶.

[۲] S. Retzkin, *Hands-On Dark Web Analysis: Learn what goes on in the Dark Web, and how to work with it*. Packt Publishing Ltd, ۲۰۱۸.

[۳] R. Dingledine, N. Mathewson, and P. Syverson, "Tor: The second-generation onion router," Naval Research Lab Washington DC, ۲۰۰۴.

[۴] J. Fajfer, "Korelační útoky na TOR," České vysoké učení technické v Praze. Vypočetní a informační centrum., ۲۰۱۸.

[۵] R. Magán-Carrión, A. Abellán-Galera, G. Maciá-Fernández ,and P. García-Teodoro, "Unveiling the I۲P web structure: A connectivity analysis," *Computer Networks*, vol. ۱۹۴, p. ۱۰۸۱۵۸, ۲۰۲۱.

[۶] S. J. Murdoch, "Hot or not: Revealing hidden services by their clock skew," in *Proceedings of the ۱۳th ACM conference on Computer and communications security*, ۲۰۰۶, pp. ۲۷-۳۶.

[۷] L. Overlier and P. Syverson, "Locating hidden servers," in ۲۰۰۶*IEEE Symposium on Security and Privacy (S&P'۰۶)*, ۲۰۰۶: IEEE, pp. ۱۵pp.- ۱۱۴.

[۸] "۱"https://next.gazeta.pl/next/,۷,۱۵۶۸۳۰,۲۱۵۰۹۹۲۰korzystasz-z-۴-procent-internetu-reszta-jest-niewidzialna.html (accessed.

[۹] I. Karunanayake, N. Ahmed, R. Malaney, R. Islam, and S. K. Jha, "De-anonymisation attacks on Tor: A Survey," *IEEE Communications Surveys & Tutorials*, vol. ۲۳, no. ۴, pp. ۲۳۲۴-۲۳۵۰, ۲۰۲۱.