به نام کیمیاگر عالم

دانشگاه صنعتی امیرکبیر
(پلی تکنیک تهران)

امنیت شبکه

عنوان

تمرین چهارم – مقاله نسل دوم Tor

مدرس

دکتر سیاوش خرسندی

دانشجو

امیرحسین بابائیان

۴۰۱۱۳۱۰۰۲

ترم پاییز ۰۲-۰۱

گروه معماری کامپیوتر و شبکه های کامپیوتری

دانشکده مهندسی کامپیوتر، دانشگاه صنعتی امیرکبیر (پلی تکنیک تهران)

فهرست

خلاصه مقاله

مقاله در اختیار ما در مورد نسل دوم Onion Routers است. ابتدا توضیحات کلی در مورد Tor ارائه شده است و اینکه در گذشته چه قابلیت هایی داشته و مشکلات برطرف شده آن به چه صورت است. در انتها نیز بخشی از سوللات بدون پاسخ مطرح شده است.

تعریف Onion Routing به عنوان یک شبکه همپوشان توزیع شده که بر پایه TCP است اورده شده است و نحوه عملکرد یک node و قابلیت های ان توضیح داده شده است. در ادامه، به مواردی که در این مقاله به عنوان نسل دوم Tor، بهبودی هایی اضافه شده بر نسل قبلی است پرداخته شده است.

رازداری کامل: در نسخه قدیمی، یک مجموعه node با تبانی میتوانست اطلاعات مربوط به گره های متوالی را بدست بیاورد و با استفاده از کلید اطلاعات را رمزگشایی کند اما در نسخه جدید برای هر ارتباط کلید جلسه ای تعریف میشود و براساس ان است که اطلاعات رمزنگاری میشود. با اضافه شدن این قابلیت، دیگر با به دست اوردن کلید جلسه امکان دسترسی به اطلاعات قبلی و رمزگشایی انها وجود ندارد، که امنیت بیشتری را به ارمغان می اورد.

جداسازی پروتکل از ناشناسی: در نسخه قدیمی نیاز بود تا در لایه اپلیکیشن پیاده سازی صورت بگیرد به همین دلیل خیلی از برنامه ها چنین قابلیتی نداشتند این کار در لایه ی نتورک و مبتنی بر TCP پیاده سازی شده است. که نیاز به پیاده سازی مجدد در هر یک از برنامه ها را مرتفع کرده است.

در نسخه قدیمی، بایستی ارتباط در سطح اپلیکیشن برقرار میشد و به ازای هر ارتباط یک مدار مشخص تعبیه میشد اما چون در این نسخه مبتنی بر TCP هستیم یک مدار میتواند چند ارتباط TCP را هندل کند.

در نسخه جدید ما به گره لبه ها اجازه میدیم تا سیل یا ازدحام را جهت کنترل ازدحام شناسایی نماید.

در نسخه ی قدیمی از flood برای اعلام طراحی ها استفاده میشد، حال انکه در نسخه ی جدید از دایرکتوری سرور ها کمک گرفته شده است و از سیاست های خروج گره ها به صورت متغیر پشتیبانی می کند.

از دیگر موارد اضافه شده به نسخه جدید می توان به بحث بررسی انتها به انتهای جامعیت و بحث های مربوط به پنهان بودن نقاط ملاقات و خدمات اشاره کرد که دیگر نیازی به پاسخ onion router ندارد.

در این مقاله به چند کار مشابه نیز پرداخته شده است که از جمله آن میتوان به PipeNet، Hordes، Mix-Net و ... اشاره کرد.

از جمله اهداف اصلی این پروژه می توان به کاهش میزان تاخیر و جلوگیری از حمله های مختلف جهت شناسایی اشاره کرد با این حال موارد دیگری نیز در این بخش اشاره شده اند که عبارتند از : قابلیت استقرار در دنیای واقعی و قابلیت استفاده برای عدم شناسایی، پروتکل انعطاف پذیر و قابل توسعه و طراحی ساده اشاره کرد.

Tor این موارد را ندارد: همتا به همتا نیست، در برابر حملات انتها به انتها ایمن نیست و استگانوگرافی ندارد.

در ادامه به طراحی Tor پرداخته می شود، سلول های با اندازه ثابت را که واحد ارتباط در Tor هستند ارائه می دهد. همچنین توضیح می دهد که چگونه مدارها ساخته می شوند، گسترش می یابند، کوتاه می شوند و از بین می روند. در ادامه نیز چگونگی مسیریابی جریان های TCP از طریق شبکه را توضیح می دهد. به بررسی یکپارچگی محدود کردن منابع می پردازد و در نهایت، مسائل مربوط به کنترل تراکم و عدالت صحبت می کند.

در بخش دیگری به بحث Rendezvous points می پردازد که به ما کمک میکند تا از افشای آدرس IP جلوگیری کنیم تا از حملات متعددی همجون DDoS جلوگیری نماییم و مبتنی بر TCP این کار و اهداف آن عبارتند از : کنترل دسترسی، نیرومندی، مقاومت و شفافیت در application ها.

در ادامه به فرمت های طراحی دیگر موارد تصمیم گیری پرداخته شده است که این موارد عبارتند از: Denial of service، Exit policies and abuse و Directory Servers.

به انواع مختلفی از حملات و دفاعیه ها نیز مانند Active، Passive و Directory اشاره شده است.

در بخش های پایانی به سوالات باز در این زمینه اشاره شده است که حل این سوالات می تواند منجر به اتفاقات موثری در زمینه ی امنیت در Tor شود.

مقیاس پذیری، کلاس بندی پهنای باند، پوشش ترافیک، عملیات کش در گره پایانی، توزیع دایرکتوری مطلوب تر، همکاری چند سیستمه و استقرار در مقیاس یالاتر از جمله مواردی هستند که در این مقاله به عنوان موارد برای کار بر روی مفاهیم در آینده آورده شده است و به نوعی می توان نسل بعدی TOR را با اضافه کردن این قابلیت ها ارائه کرد.

سیستم عامل Tails

The Amnesic Incognito Live System (Tails)

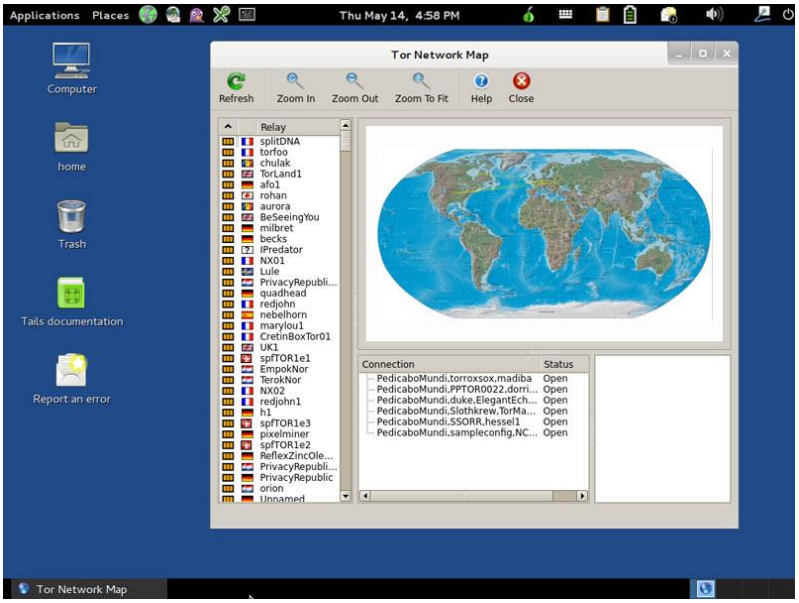
یک توزیع لینوکس مبتنی بر Debian با توجه ویژه بر امنیت است که هدف آن حفظ حریم خصوصی و ناشناس ماندن است، به زبان ساده تیلز یک سیستم عامل Portable است که هدفش مقابله با سانسور و نظارت است.

Tails یک سیستم عامل امن برای مخفی ماندن در دنیای اینترنت است که امکانات بسیار جالبی را در اختیار ما قرار می دهد، این سیستم عامل برپایه لینوکس دبیان است و از مجیط گرافیکی ژیبا GNOME استفاده میکند و در عین حال حجم زیادی را به خود اختصاص نمی دهد و میتوانید یک تجربه متفاوتی را در هنگام استفاده از ان داشته باشید، از مزیت های Tails میتوان کم حجم بودن و سبک بودن ان را مثال زد که به همین دلیل میتوان به راحتی آن را دریافت نمود و در هر سیستمی حتی با سخت افزار نسبتا ضعیف ان را اجرا کرد.

تمام اتصالات در این سیستم‌عامل به‌طور اجباری از طریق شبکه TOR انجام می‌شود و هرگونه اتصال غیرناشناس در این شبکه مسدود می‌شود، Tails به‌گونه‌ای طراحی شده تا با به صورت USB Live اجرا شود و هیچ ردپای دیجیتالی روی سیستم برجای نگذارد. مگر اینکه شما تنظیمات اولیه را تغییر دهید.

پروژه TOR با حمایت مالی به توسعه Tails کمک کرده است.

تصویری از محیط Tails:

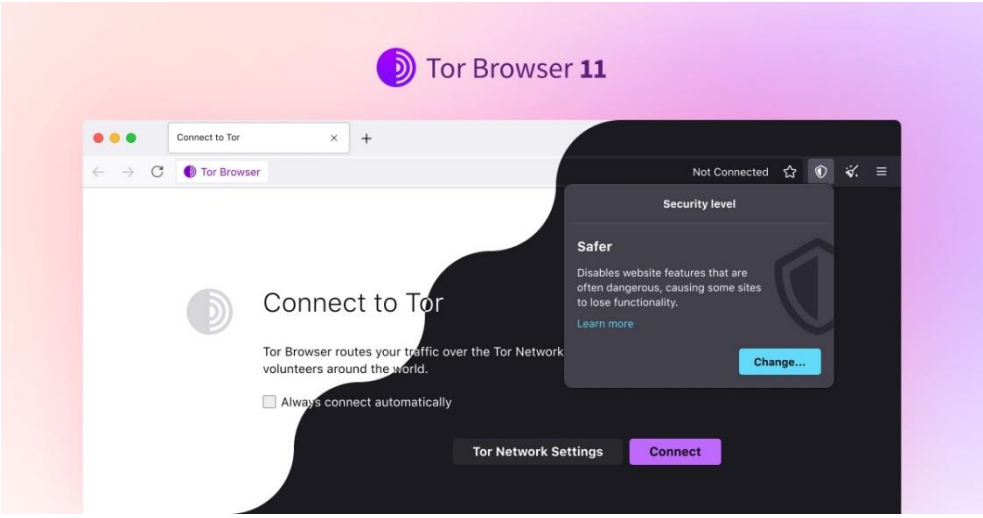


مرورگر Tor

مرورگر Tor یک مرورگر وب است که قادر به دسترسی به شبکه Tor است. این به عنوان بسته مرورگر Tor توسط استیون جی مرداک ایجاد شد و در ژانویه ۲۰۰۸ اعلام شد. مرورگر Tor از یک مرورگر وب Mozilla Firefox ESR اصلاح شده، TorButton، TorLauncher، NoScript و پروکسی Tor تشکیل شده است. کاربران می توانند مرورگر Tor را از رسانه های قابل جابجایی اجرا کنند. این می تواند تحت ویندوز مایکروسافت، macOS، اندروید و لینوکس کار کند.

موتور جستجوی پیش‌فرض DuckDuckGo است (تا نسخه ۴٫۵، Startpage.com پیش‌فرض آن بود). مرورگر Tor به طور خودکار فرآیندهای پس زمینه Tor را شروع می کند و ترافیک را از طریق شبکه Tor هدایت می کند. پس از پایان جلسه، مرورگر داده‌های حساس به حریم خصوصی مانند کوکی‌های HTTP و تاریخچه مرور را حذف می‌کند. این در کاهش ردیابی وب و اثر انگشت بوم موثر است و همچنین به جلوگیری از ایجاد حباب فیلتر کمک می کند.

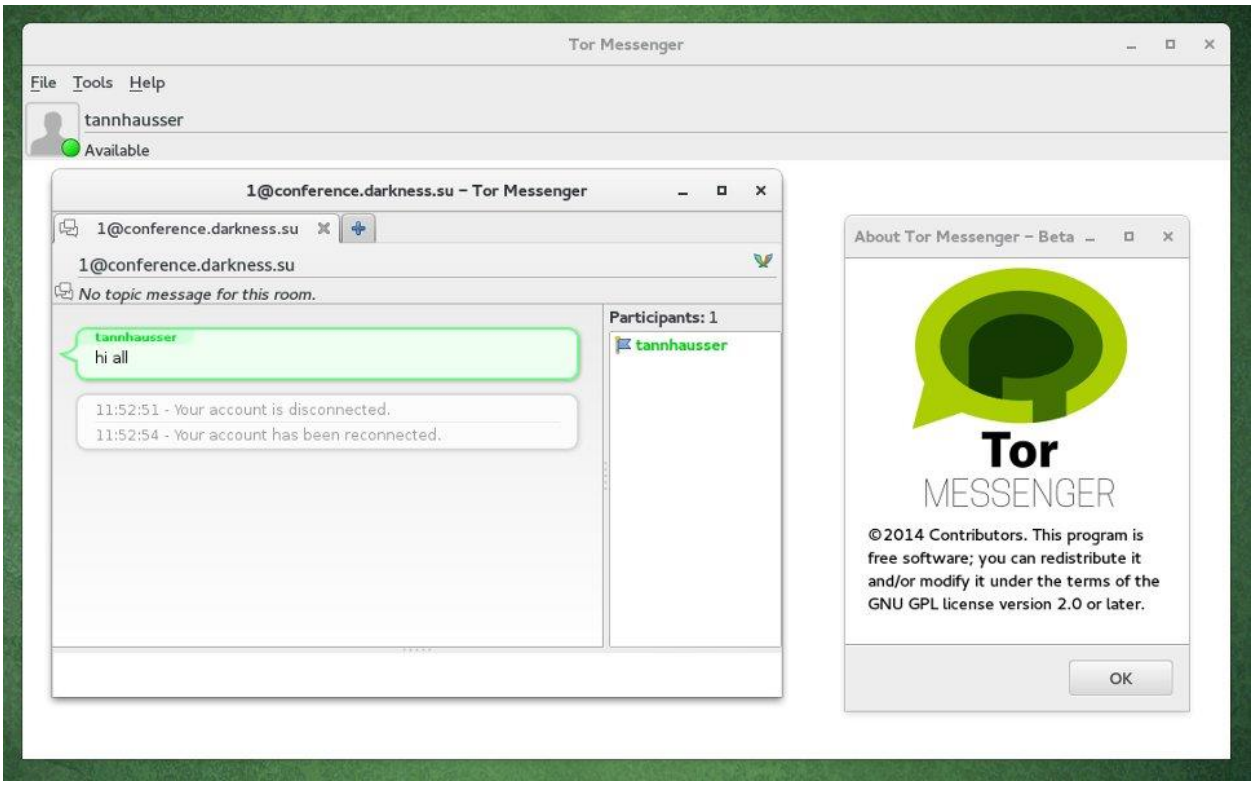
برای اجازه دانلود از مکان هایی که دسترسی به URL پروژه Tor ممکن است مخاطره آمیز یا مسدود باشد، یک مخزن GitHub با پیوندهایی برای نسخه های میزبانی شده در دامنه های دیگر نگهداری می شود.



پیام رسان Tor

در ۲۹ اکتبر ۲۰۱۵، پروژه Tor، Tor Messenger Beta را منتشر کرد، یک برنامه پیام‌رسانی فوری مبتنی بر Instantbird با Tor و OTR داخلی و به‌طور پیش‌فرض استفاده می‌شود. مانند Pidgin و Adium، Tor Messenger از چندین پروتکل مختلف پیام رسانی فوری پشتیبانی می کند. با این حال، این کار را بدون تکیه بر libpurple انجام می‌دهد، و به جای آن همه پروتکل‌های چت را در زبان جاوا اسکریپت ایمن برای حافظه پیاده‌سازی می کند.

به گفته لوسیان آرماسو از Toms Hardware، در آوریل ۲۰۱۸، پروژه Tor پروژه پیام رسان Tor را به سه دلیل تعطیل کرد: توسعه دهندگان "Instabird" [sic] پشتیبانی از نرم افزار خود را متوقف کردند، منابع محدود و مشکلات فراداده شناخته شده.. توسعه دهندگان Tor Messenger توضیح دادند که غلبه بر هر گونه آسیب پذیری کشف شده در آینده به دلیل تکیه پروژه بر وابستگی های نرم افزاری قدیمی غیرممکن خواهد بود.



تلفن همراه اندرویدی Tor

مایک پری، توسعه‌دهنده Tor، یک نمونه اولیه از پایه‌های تلفن هوشمند مجهز به tor در CopperheadOS را اعلام کرد. این به عنوان یک جهت برای tor در تلفن همراه بود. این پروژه "ماموریت غیرممکن" نام داشت. دانیل میکای، توسعه‌دهنده اصلی Copperhead از این نمونه اولیه استقبال کرد. Tor Phone به مفهوم گوشی هوشمندی اشاره دارد که اتصالات اینترنتی را از طریق شبکه Tor هدایت می کند. اولین Tor Phone نمونه اولیه تلفن هوشمندی بود که در سال ۲۰۱۶ توسط The Tor Project منتشر شد که به کاربران این امکان را می داد تا برای ناشناس ماندن، اتصالات اینترنتی را از طریق Tor هدایت کنند. Work on Tor Phone در سال ۲۰۱۴ راه‌اندازی شد، و یک «نمونه اولیه تلفن Android با قابلیت Tor» در سال ۲۰۱۶ اعلام شد

CopperheadOS یک سیستم عامل تلفن همراه برای تلفن های هوشمند است که بر اساس پلت فرم تلفن همراه اندروید است. ویژگی‌های حریم خصوصی و امنیتی را به نسخه‌های رسمی پروژه منبع باز Android توسط Google اضافه می کند. CopperheadOS توسط Copperhead، یک شرکت امنیت اطلاعات کانادایی توسعه یافته است. مجوز آن تحت Creative Commons BY-NC-SA 4.0 است، اگرچه کد منبع آن برای دانلود عمومی در دسترس نیست.

پروژه Tor یک نمونه اولیه تلفن هوشمند مبتنی بر CopperheadOS به نام Tor Phone را منتشر کرد که به کاربران این امکان را می داد تا اتصالات شبکه خود را از طریق Tor برای ناشناس بودن مسیریابی کنند.
CopperheadOS به دلیل تمرکز بر امنیت، به ویژه استفاده از بوت تایید شده و جلوگیری از لغو برنامه های سیستم توسط برنامه های فروشگاه Google Play انتخاب شد. نمونه اولیه فقط روی سخت افزار Google Nexus و Pixel کار می کرد و قطعات ناتمام زیادی داشت.

برنامه های Third Party

کلاینت BitTorrent Vuze (Azureus سابق)، سیستم پیام رسانی ناشناس Bitmessage،و پیام رسان فوری TorChat شامل پشتیبانی Tor هستند. OnionShare به کاربران اجازه می دهد تا فایل ها را با استفاده از Tor به اشتراک بگذارند.

پروژه نگهبان به طور فعال در حال توسعه یک مجموعه رایگان و منبع باز از برنامه ها و سیستم عامل برای سیستم عامل اندروید است تا امنیت ارتباطات سیار را بهبود بخشد. این برنامه‌ها شامل کلاینت پیام‌رسانی فوری ChatSecure،پیاده‌سازی Orbot Tor (همچنین برای iOS در دسترس است)، Orweb (منقضی شده) مرورگر تلفن همراه با حفظ حریم خصوصی، Orfox، همتای تلفن همراه مرورگر Tor، افزونه ProxyMob Firefoxو ObscuraCam.

Onion Browserیک مرورگر وب منبع باز و تقویت کننده حریم خصوصی برای iOS است که از Tor استفاده می کند.در اپ استور iOS و کد منبع در GitHub در دسترس است.

Brave پشتیبانی Tor را در حالت مرور خصوصی مرورگر دسکتاپ خود اضافه کرد. کاربران می توانند با کلیک کردن بر روی منوی همبرگر در گوشه سمت راست بالای مرورگر، به مرور با Tor-enabled تبدیل شوند.

سیستم عامل های متمرکز بر امنیت : چندین سیستم عامل متمرکز بر امنیت از Tor استفاده یا استفاده گسترده ای می کنند. اینها عبارتند از Hardened Linux From Scratch، Incognito، Liberté Linux، Qubes OS، Subgraph، Tails، Tor-ramdisk، و Whonix.