گزارشِ تحقیق درباره‌ی انواع روش‌های ممکن جهتِ دور زدن تحریم‌های نرم‌افزاری

تهیه و تنظیم: مبین خیبری

شماره دانشجویی: 994421017

استاد راهنما: دکتر میرسامان تاجبخش

چکیده:

در این گزارش قصد داریم روش‌های ممکن جهت دسترسی به محتوای وبسایت‌هایی که کشور ایران را در لیستِ تحریم‌های نرم‌افزاریِ خود قرار داده‌اند، بپردازیم. به کمکِ سرویس‌هایی نظیرِ Shecan می‌توان با تغییرِ DNS و به‌کارگیریِ تعدادی دستورالعملِ مشخص، به این هدف رسید. تمرکزِ ما در این گزارش، بر یافتنِ راه‌حل‌های دیگر جهتِ رسیدن به این هدف معطوف گردیده، اما به اقتضای مطلب، روش فوق را نیز معرفی و بررسی خواهیم کرد. همچنین به دلیلِ اینکه ابزارها و تکنیک‌های لازم جهتِ دور زدنِ تحریم‌ها با روش‌های موجود جهتِ دور زدنِ سیستم‌های فیلترینگِ گسترده در سطح شبکه‌های کامپیوتری هم‌پوشانیِ زیادی دارند، در برخی قسمت‌های این گزارش توضیحاتی درباره‌ی نحوه دور زدنِ سیستم‌های فیلترینگ نیز ارائه شده است. این گزارش به کمکِ منابعِ پرشمارِ موجود در سطح اینترنت تهیه و تدوین شده است.

DNS برای دور زدن تحریم ها – چگونه تحریم های مجازی را بی اثر کنیم؟

برای اینکه بتوانید درک بهتری نسبت به دی این اس داشته باشید، ابتدا بهتر است تا با تعریفی از (Domain Name System) یا Name Server یا سیستم نام سرور آشنا شوید. دی ان اس در اصل یک استاندارد تکنولوژی است که برای مدیریت نام وبسایت‌ها و دامنه‌های موجود در اینترنت و تحت وب مورد استفاده قرار می‌گیرد. به زبان ساده‌تر شبیه به دفترچه تلفن آنلاینی است که اطلاعات کامل مخاطبین اعم از نام و نام خانوادگی در آن درج شده و با یک جستجو ساده شما را به مخاطب مورد نظرتان متصل می‌کند.

همان‌طور که در قسمت بالا اشاره شد، دی ان اس همانند یک دفترچه تلفن در بستر اینترنت عمل می‌کند. اجازه دهید تا با یک مثال برایتان بهتر این موضوع را توضیح دهیم. دی ان اس دقیقاً مانند یک دفترچه تلفن اینترنتی است و کامپیوترها برای اتصال به یکدیگر از اعداد یا همان IP آدرس‌ها استفاده می‌کنند، حفظ کردن این IP آدرس‌ها توسط انسان کار سخت و غیر ممکنی است. اما با کمک دی ان اس دیگر نیازی به حفظ کردن IP آدرس‌ها نیست.

DNS چگونه کار میکند؟

زمانی که قصد بازدید از یک سایتی را دارید، کامپیوتر شما مراحلی را برای تبدیل آدرس وب قابل خواندن انسان به یک IP آدرس قابل خواندن ماشین تبدیل می‌کند. این اتفاق هر بار که شما در حال بازدید از یک وب سایت، فرستادن ایمیل و یا حتی گوش دادن به ایستگاه‌های رادیویی اینترنتی هستید رخ می‌دهد. اما آیا DNS برای دور زدن تحریم ها روشی کارآمد است؟

گاها ممکن است که یک سایت با بیش از یک آدرس IP مطابقت داشته باشد. در اصل برخی از سایت‌ها دارای صدها آدرس IP می‌باشند که با یک نام دامنه واحد مطابقت دارد. در این مرحله دی ان اس وارد کار می‌شود و آدرس‌ها را به نام دامنه خوانا تبدیل می‌کند. دی ان اس شامل سلسله مراتب از یک پایگاه داده حاوی اطلاعات نام دامنه می‌باشد. برای مثال هنگامی که شما در مرورگر خود نام یک دامنه را وارد می‌کنید، کامپیوتر شما به سرعت درخواست را به سرور دی ان اس محلی سیستم عامل ارسال می‌کند تا بررسی شود که آیا گزینه مورد نظر در حافظه نهان (Cash) کامپیوتر ذخیره شده است یا نه؟! اگر در حافظه پنهان نبود؛ درخواست از طریق اینترنت به چندین سرور مختلف دی ان اس دیگر ارسال می‌شود. در غیر این صورت اطلاعات لازم به سرورهای خارجی دیگر ارسال می‌گردد.

مزایای DNS

یکی از مهم‌ترین مزیت‌های سیستم دی ان اس استفاده راحت و بی دردسر از اینترنت است. اگر دی ان اس وجود نداشت، شما برای دسترسی به هر سایتی می‌بایست تمامی آدرس‌های IP آن را حفظ می‌کردید. که خب این یک کار غیر ممکن و دشوار بود. از دیگر مزیت‌های قابل توجه دی ان اس، می‌توان به ثبات آن اشاره کرد. در برخی شرایط، بنا به دلایل مختلفی آدرس‌های IP تغییر می‌کند، در چنین حالتی برای دسترسی به وبسایت نه تنها نیاز به دانستن آدرس IP، بلکه اطلاعات به روز شده نیز بود. اما یکی از کارهای دی ان اس به روز رسانی سریع و ثابت آدرس‌های IP می‌باشد. که همین موضوع دسترسی به وبسایت‌های مورد نظر را بسیار آسان کرده است. همچنین از DNS برای دور زدن تحریم ها استفاده می‌شود. دی ان اس سیستم می‌تواند با به روز رسانی ایمن، زیرساخت‌ها را ارتقا بخشد. همچنین یک سیستم قابل اعتماد است که می‌تواند پیام‌ها را با خرابی صفر تحویل کاربران دهد. این سیستم در عملکرد فنی دیتابیس به شما کمک می‌کند. در حقیقت دی ان اس را می‌توان به عنوان یک توازن بار یا یک لایه اضافی نام برد.

معایب DNS

همه ما به خوبی میدانیم که هر سیستمی علاوه بر مزیت‌های بی‌شمار، معایبی نیز دارد، دی ان اس هم از این قاعده مستثنی نیست. شاید بتوان DNS Attacks را یکی از اصلی‌ترین و مهم‌ترین معایب دی ان اس دانست. در چنین حالتی فرد کلاه‌بردار به راحتی می‌تواند آدرس واقعی را با یک آدرس جعلی جایگزین کند و کاربران را به آسانی فریب دهد. معمولاً هدف افراد کلاه‌بردار از این کار گرفتن اطلاعات بانکی کاربران می‌باشد. در مواقعی که یک بدافزار تنظیمات سرور شما را تغییر داده باشد، درست در زمانی که URL مورد نظر خود را وارد می‌کنید، شما را به یک وبسایت کاملاً متفاوت که شبیه به وب سایت بانک می‌باشد انتقال می‌دهد. در چنین حالتی امکان ثبت و ضبط اطلاعات بانکی شما بسیار بالا می‌رود. یکی دیگر از معایبی که در سیستم

دی ان اس به چشم می‌خورد، ربوده شدن برخی از سرورهای دی ان اس توسط بدافزارهاست. در چنین حالتی هنگامی که شما قصد بازدید از یک وبسایت محبوب و پرطرفدار را دارید، این بدافزار شما را به یک وبسایت جعلی و پر از تبلیغات هدایت می‌کند. برای جلوگیری از چنین مشکلاتی، بهترین کار نصب یک آنتی ویروس معتبر بر روی سیستم‌تان است. از ورود به سایت‌هایی که ظاهرشان با وبسایت مورد نظر شما متغیر می‌باشد دوری کنید. همچنین هرگز در سایت‌های نامعتبر اطلاعات شخصی و بانکی خود را وارد نکنید.

تحریم مجازی چیست و چگونه صورت میگیرد؟

همان‌طور که میدانید در چند سال اخیر کشورمان دچار تحریم‌های مختلفی از سمت خدمات دهندگان خارجی شده است. این تحریم‌ها می‌تواند شامل خدمات اینترنتی، سایت‌ها، بازی‌ها و کنسول‌ها نیز باشد. در چنین حالتی برای استفاده از برخی از خدمات و دسترسی به آنها مجبور به دور زدن تحریم‌ها می‌شویم. به همین منظور از DNS برای دور زدن تحریم ها استفاده می‌شود. اما این تحریم‌ها به چه صورت عمل می‌کنند؟ در واقع تحریم به معنی محدود کردن دسترسی عده‌ای به برخی خدمات مشخص می‌باشد. چند سالی است که تحریم‌های وضع شده نسبت به ایران بسیار افزایش یافته و گریبان برخی از خدمات مجازی همچون؛ سایت‌ها، بازی‌ها، اپلیکیشن‌ها و ... که خارج از کشور پشتیبانی می‌شود را گرفته است. در چنین مواردی اگر IP آدرس شما ایران یا هر کشور دیگر جزء تحریم باشد، متأسفانه ارائه خدمات به شما امکان پذیر نیست.

چگونه تحریم‌های مجازی را دور بزنیم؟

تا اینجا به خوبی دریافتیم که اگر بخواهیم با آدرس IP ایران از برخی از خدمات تحریمی استفاده کنیم با مشکل مواجه خواهیم شد. یکی از راه‌های استفاده از این خدمات، تغییر آدرس IP می‌باشد، در این وضعیت باید از طریق آدرس IP کشوری که در لیست تحریم‌ها نیست برای استفاده از خدمات کمک بگیریم. در ادامه به برخی از روش‌های تغییر آی پی خواهیم پرداخت.

استفاده از VPN

VPN ها انواع مختلفی دارند و شما رو به یک سرور خارجی هدایت می‌کند. پس از اینکه عملیات متصل شدن به یک سرور خارجی با موفقیت به اتمام رسید، می‌توانید از خدمات تحریمی به راحتی استفاده کنید. اما در بیشتر مواقع VPN ها ثابت نیستند. در برخی از موارد حتی اگر شما از VPN پولی استفاده کنید، در دانلودهای سنگین گاهی با مشکل روبه‌رو شده و در استفاده بلند مدت باعث مصرف بیش از حد حجم اینترنت و یا باتری می‌شود. حتی استفاده مداوم از VPN در بلند مدت می‌تواند به باتری گوشی‌های موبایل صدمه بزند. در نتیجه بهتر است تا برای کارهای کوتاه و سبک از VPN استفاده کنید.

از DNS برای دور زدن تحریم ها استفاده کنید

یکی دیگر از کارهایی که برای دور زدن تحریم‌ها توصیه می‌شود، استفاده از سیستم دی ان اس می‌باشد. کارایی دی ان اس به این صورت است که وقتی دی ان اس به دستگاه شما متصل می‌شود، سرورهای دی ان اس به صورت ناشناس هویت شما را به سرورهای تحریمی ارسال می‌کنند و همین امر تشخیص هویت شما را برای تحریم کنندگان ناممکن می‌سازد.

اما از چه سرورهایی استفاده کنیم؟

شکنShecan

یکی از سریع‌ترین و بهترین راه‌های دور زدن تحریم‌های مجازی استفاده از سرویس دی ان اس شکن است. در ادامه به قابلیت‌های بی‌نظیر این سرویس اشاره میکنیم.

- بومی بودن
- نبود محدودیت در سیستم عامل
- سرعت بسیار بالا
- استفاده راحت و سادگی در نرم افزار

به جرات میتوان گفت که این نوع از دی ان اس سرعت بسیار بالایی نسبت به سرورهای دیگر دارد. یکی دیگر از ویژگی‌های این سرویس بالا نگهداشتن سرعت برای دانلود بازی‌ها و فایل‌های سنگین و فعالیت‌های زمان‌بر میباشد.

۲-دی ان اسLevel3

از دیگر مواردی که میتواند دسترسی شما را به خدمات دهندگان خارجی آسان سازد، سرویس Level3 میباشد که علاوه بر سرعت نسبتا خوب میتوان زمان زیادی را بدون افت سرعت از آن استفاده کرد.

۳-Open DNS

OpenDNSیکی از آن دسته از سرویس‌هایی‌ست که به امنیت زیاد شناخته میشود. این سرویس توسط شرکت Casio در سال ۲۰۰۵ ساخته شده و به یکی از بزرگترینPublic DNS های جهان تبدیل شده است. این سرویس به دلیل افزایش سرعت در بازی طرفداران بسیاری دارد. همچنین افزایش ping در بازی‌ها بسیار کم اتفاق می‌افتد و علاوه بر یک سرعت خوب در بازی، شما را از سرورهای آلوده دور میکند.

تفاوت DNS و VPN چیست؟

دی ان اس‌ها تفاوت زیادی به پروکسی دارند؛ با این تفاوت که دی ان اس آدرس IP کاربران را مخفی میسازد ولی محتوای مسدود شده و تحریمی را برای شما باز میکند. در نتیجه DNS برای دور زدن تحریم ها یک روش کار آمد میباشد. اتصال را کند نمیکند؛ بر خلاف VPNها که ترافیک مصرفی شما را افزایش و سرعت اینترنت را کاهش میدهد، دی ان اس‌ها تاثیری بر روی اتصال شما به اینترنت ندارند. استفاده راحت بر روی هر نوع دستگاه؛ فناوری به کار رفته در هسته دی ان اس بسیار ابتدایی و ساده است. برای استفاده از این سیستم نیاز به هیچ قابلیت خاص و پیچیده‌ای نیست. در نتیجه میتوان آن را بر روی هر سیستمی که دارای اینترنت باشد نصب کرد، بدون نیاز به تنظیمات پیچیده و پیکر بندی خاص. تنها کافی‌ست دی ان اس را روی روتر WiFi یا کارت شبکه و مودم قرار دهیم.

در ادامه و به اقتضای مطالبِ بعدی، 5 روشِ معمول جهتِ دور زدنِ سیستم‌های فیلترینگ را مرور خواهیم کرد.

5 روشِ عمده‌ی دور زدن فیلترینگ

استفاده ازVPN

یکی از روش های باب شده در کشور استفاده از VPN است. ولی آیا شما نحوه عملکرد وی پی ان ها را میدانید؟ اگر دقت کرده باشید برای اتصال به فیلترشکن از شما کشوری به عنوان مقصد می خواهند که بیشتر کشورها قابل مشاهده است .حال شما یک کشور به عنوان مثال ژاپن را انتخاب میکنید، ترافیک شما به سمت کشور ژاپن منتقل می شود و سپس به مقصد میرسد.

پاسخ به درخواست شما نیز عینا به همین روش بازمی گردد VPN .ها علاوه دور زدن فیلترینگ امینت فوق العاده بالایی دارند، شما با اتصال به وی پی ان بصورت کد گزاری شده متصل می شوید یعنی تنها چیزی که در فضای مجازی قابل رویت است یک اتصال کدگزاری شده است.

استفاده ازTor

مرورگر تور این امکان را به شما می دهد تا بصورت نا شناس در فضای اینترنت به گشت و گذار بپردازید . Torدرخواست شما را از بین چندین سیستم رمزگذاری شده عبور می دهد و به این دلیل می توانید به تمام شبکه های مسدود شده دسترسی پیدا کنید. حتی در مواقعی که VPN یا Proxy شما غیر فعال باشد تور بار آنها را به دوش میکشد.

استفاده ازProxy

پراکسی نظیر VPN عمل می کند و تمام اطلاعات شما را کد گذاری میکند ولی با این تفاوت که شما هنگامی که VPN را فعال میکنید کل سیستم و برنامه های شما ایمن می شود و میتوانید با خیل راحت از آنها استفاده کنید. ولی پراکسی فقط یک مرورگر و اپلیکیشن خاص را پشتیبانی میکند.

استفاده ازSSH

اگر شما از سروری استفاده میکنید که امکان برقراری ارتباط با SSH هست، با تنظیمات SSH کاری کنید تا مرورگر خود از طریق تونل SSH عبور کند. این روش دقیقا مانند VPN می ماند.

استفاده ازDNS

برخی از ISP ها DNS خود را تغییر می دهند تا در صورت فیلترینگ آدرس سایت به آدرسی دیگر منتقل شود. شما می توانید با تغیر DNS خود به دی ان اس Google یعنی 8.8.8.8 و 8.8.4.4 این سانسور و فیلترینگ را دور بزنید.

اگر از دسته افرادی باشید که با سایت‌های خارجی زیاد سروکار دارید، احتمالاً برایتان پیش آمده است که با خطای عدم دسترسی به سایت به دلیل حضور در کشور ایران مواجه شده باشید. خیلی از وب‌سایت‌ها به خاطر تحریم‌هایی که توسط آمریکا و کشورهای اروپایی بر علیه ایران انجام شده است، آی پی ایرانی را تحریم کرده‌اند و به ایرانیان این اجازه را نمی‌دهند که بتوانند از وبسایتشان بازدید کنند. به همین دلیل است که نمی‌توانیم از عکس‌ها و محتواهای سایت‌های خارجی استفاده کنیم و به داخل این وب سایت ها وارد شویم. خیلی اوقات طراحان سایت و گرافیست‌ها و افرادی که شغل‌های اینترنتی دارند، نیاز پیدا می‌کنند که به این وبسایتها سر بزنند و از امکانات آنها استفاده کنند. در این قسمت می‌خواهیم به شما بگوییم که چطور می‌توانید با روش تغییر DNS برای دور زدن تحریم‌ها، مشکل خودتان را حل کنید و به راحتی از وب‌سایت‌های دلخواه خودتان بازدید کنید.

DNS برای دور زدن تحریم چیست؟

در ابتدا شاید نیاز باشد که از پایه‌ای‌ترین موضوع شروع کنیم و بگوییم که اصلا DNS برای دور زدن تحریم چیست و چه کاربردی دارد. کامپیوترها این قابلیت را دارند که بتوانید آدرسی به آنها بدهید که در نهایت آی پی سیستم شما تغییر کند و کشور را به درستی نمایش ندهد. مثلا اگر وبسایتی آی‌پی‌های مربوط به ایران را تحریم کرده باشد، شما می‌توانید با استفاده از DNS برای دور زدن تحریم، به‌سادگی این مشکل را برطرف کنید و از وبسایت موردنظر بازدید کنید. البته روش‌های دیگری نیز غیر از DNS برای دور زدن تحریم وجود دارند که در ادامه به برخی از رایج ترین آنها اشاره می کنیم تا بتوانید در صورت نیاز با آنها نیز آشنایی داشته باشید.

روش هایی جهتِ دور زدن تحریم‌ها

استفاده ازVPN

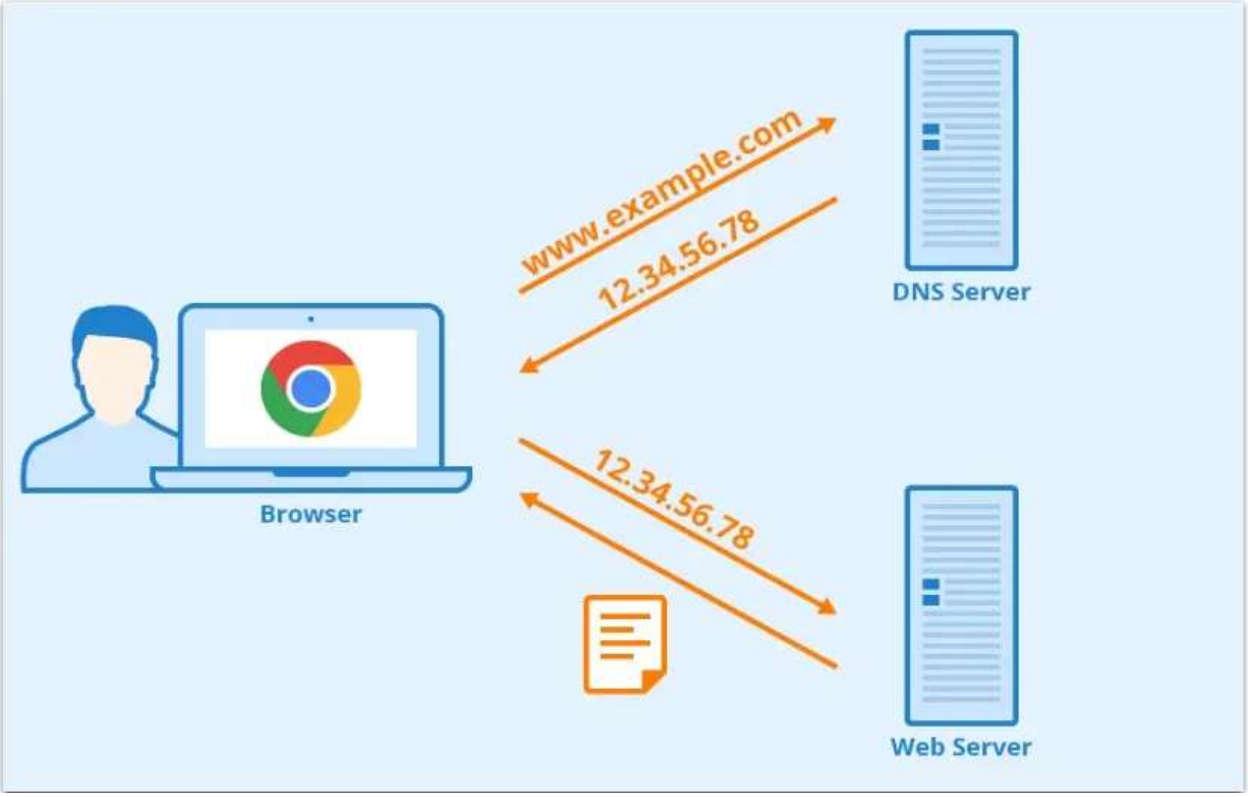
وی‌پی‌ان این امکان را به ما می‌دهد که بتوانیم با خریداری یک سرویس تغییر آی پی، به راحتی آی پی سیستم خودمان را تغییر دهیم. شما می‌توانید در وی‌پی‌ان حتی کشوری که می‌خواهید آی پی خودتان را به آن تغییر دهید انتخاب کنید و این موضوع می‌تواند یکی از مزیت‌های بسیار مناسب VPN باشد. اما مشکلی که در این حالت وجود دارد این است که در وی‌پی‌ان های اشتراکی، شما آی پی ثابتی ندارید و هر دفعه‌ای که به وبسایت وارد می شوید، یک آی پی متغیر خواهید داشت و این موضوع می‌تواند باعث شود برخی از سرویس‌ها به شما شک کرده و شما را ربات شناسایی کنند.

استفاده ازVPS

گاهی اوقات ممکن است کاری که می‌خواهید انجام دهید بسیار حساس باشد و نیاز به یک آی پی ثابت داشته باشید تا خطر هرگونه مشکلی را از بین ببرید .مثلاً اگر فریلنسر باشید و بخواهید از سایت‌هایی مانند فریلنسر دات کام استفاده کنید، اگر کوچکترین خطایی از شما سر بزند و با آی پی نامناسبی وارد شوید، سریعا این سایت‌ها شما را بلاک کرده و تمامی پول‌های حساب کاربری شما را بلوکه می‌کنند. برای جلوگیری از چنین مشکلاتی، راحت ترین راه حلی که وجود دارد این است که از وی‌پی‌اس استفاده کنید. حالا شاید بگوییم که تفاوت وی‌پی‌اس و وی‌پی‌ان در چیست. وی‌پی‌ان همانطور که گفتیم می‌تواند به شما در تغییر آی پی کمک کند؛ اما به شما یک آی پی ثابت ارائه نمی‌دهد و به همین خاطر می‌تواند در برخی از سایت‌ها برایتان مشکل‌ساز شود. اما وی‌پی‌اس به گونه‌ای است که هزینه بیشتری دارد، اما می‌تواند به شما یک آی پی ثابت ارائه دهد و همین موضوع کمک می‌کند که بتوانید با خیال راحت از هر سرویس و وبسایتی استفاده کنید و هیچگونه خطری شما را تهدید نکند.

DNS برای دور زدن تحریم

رسیدیم به یکی از بهترین روش‌ها برای دور زدن تحریم که بسیار کاربردی و عالی است. روشی که در این مقاله می‌خواهیم آن را بررسی کنیم، یعنی DNS برای دور زدن تحریم .این روش همان‌طور که گفته شد به این صورت است که شما می‌توانید دی ان اس سیستم خودتان را به صورتی تنظیم کنید که فقط سایت‌هایی که ایران را تحریم کرده‌اند متوجه نشوند شما از ایران هستید. این کار باعث می‌شود که اینترنت کمتری مصرف کنید و اینترنت شما بین‌المللی محاسبه نشود و همچنین بتوانید به سادگی از سایت‌هایی که می‌خواهید نیز استفاده کنید. در ادامه بیشتر این موضوع را با هم بررسی خواهیم کرد. پس همچنان با ما همراه باشید.



برای دور زدن تحریم را از کجا بیاوریم؟

ممکن است با توضیحاتی که تا به اینجا گفتیم، این سوال برایتان پیش آمده باشد که از کجا باید DNSبرای دور زدن تحریم‌ها پیدا کنیم. باید بدانید که سرویس هایی در این زمینه وجود دارند که هم در ایران و هم خارج از ایران فعالیت می‌کنند و شما می‌توانید با استفاده از این سرویس ها که اکثرا رایگان نیز هستند، به راحتی کار تغییر دی ان اس را انجام دهید و از سایت‌های خارجی به‌راحتی استفاده کنید.

سرویس شکن

شکن یک سرویس ایرانی است که می‌توانید با استفاده از آن، به راحتی به وبسایت‌های موردنظر خودتان دسترسی داشته باشید و بدون هیچ مشکلی تحریم را دور بزنید. این سرویس هم دارای یک اپلیکیشن موبایلی است که می‌توانید آن را روی گوشی خودتان نصب کنید تا تحریم‌ها را دور بزنید و هم دارای دی ان اس اختصاصی است که با تنظیم آن در کامپیوتر خودتان، می‌توانید کار دور زدن تحریم‌ها را انجام دهید. جالب است بدانید که شکن سرویس سازمانی نیز دارد و اگر می‌خواهید برای شرکت خودتان از یک DNSبرای دور زدن تحریم استفاده کنید، می‌توانید به‌راحتی از این سرویس چنین خدماتی را دریافت کنید.

سرویس بگذر

بگذر هم مانند شکن یک سیستم ارائه DNS برای دور زدن تحریم است که می‌توانید با دی ان اسی که به شما ارائه می‌دهد، تحریم‌ها را دور زده و از وب‌سایت‌های دلخواه خودتان به راحتی بازدید کنید. همچنین شما می‌توانید وب‌سایت‌هایی که می‌خواهید را در این سیستم جستجو کنید و ببینید که قابل دسترسی هستند یا خیر و اگر این سرویس از وبسایت خاصی پشتیبانی نکند و آن وبسایت ما را تحریم کرده باشد، پس از جستجوی شما وبسایت در لیست این سرویس اضافه خواهد شد و می‌توانید از آن استفاده کنید.

سرویسlevel3.com

وبسایت level3.com یک سیستم مانند وب‌سایت‌هایی که معرفی کردیم است که DNS برای دور زدن تحریم را ارائه می‌دهد و شما می‌توانید با استفاده از خدماتی که این وبسایت ارائه می‌دهد، به راحتی از وبسایت‌های دلخواه خودتان بازدید کرده و آنها را بدون مشکل باز کنید. این وبسایت خارجی است و برخی از امکانات آن نیز پولی است، اما خدماتی بسیار حرفه‌ای و مناسب ارائه می‌دهد که برای کارهای خودتان می‌توانید از این خدمات استفاده کنید.

چطور DNS برای دور زدن تحریم را برای موبایل تنظیم کنیم؟

ممکن است شما بخواهید با استفاده از موبایل خودتان به سایت‌هایی که تحریم هستند دسترسی داشته باشید. با موبایل این کار را می‌توانید به راحتی انجام دهید و به هر وبسایتی که می‌خواهید دسترسی داشته باشید. برای این کار معمولا سرویس هایی مانند شکن اپلیکیشن موبایل نیز دارند که می‌توانید به راحتی از همان اپلیکیشن استفاده کنید تا نیاز خودتان را برطرف کنید و نیازی به تنظیم دی ان اس به صورت دستی نیست. اما اگر بخواهید به صورت دستی این کار را انجام دهید، باید مراحل زیر را دنبال کنید.

ورود به قسمت وای فای

در ابتدا نیاز است که وارد تنظیمات گوشی خودتان شوید و به قسمت وای فای بروید تا بتوانید به شبکه‌های مختلف دسترسی داشته باشید. حالا روی علامت چرخ دنده در شبکه‌ای که به آن متصل هستید کلیک کنید تا بتوانید وارد تنظیمات آن شبکه خاص شوید.

رفتن به قسمت تغییر آی پی

در مرحله بعد نیاز است که روی قسمت advanced کلیک کنید تا بتوانید به گزینه‌های حرفه ای دسترسی داشته باشید و سپس گزینه IP settings را انتخاب کنید تا بتوانید تغییرات موردنیاز را انجام دهید.

تنظیمات آی پی

در این مرحله که آخرین مرحله است، نیاز است آی پی را از حالت پیش فرض به حالت static تغییر دهید و در کادرهای مربوط به دی ان اس، دو دی ان اسی که از سرویس‌های مختلف دریافت کرده‌اید را وارد کنید و در آخر تغییرات را ذخیره کنید. این مراحل مربوط به گوشی‌های اندرویدی است و به همین ترتیب می‌توانید تغییرات را انجام دهید، اما برای گوشی‌های آی او اس نیز می‌توانید از اپلیکیشنtrust DNS استفاده کنید و به راحتی دی ان اس خودتان را تغییر دهید.

برای تنظیمDNS برای دور زدن تحریم در کامپیوتر چه کاری انجام دهیم؟

اگر می‌خواهید در کامپیوتر خودتان دی ان اس را تغییر دهید تا بتوانید از DNS برای دور زدن تحریم استفاده کنید، باید کارهایی که در ادامه گفته می‌شود را انجام دهید تا بتوانید از این امکان استفاده کنید.

ورود به کنترل پنل

در ابتدا نیاز است که در سیستم ویندوزی خودتان وارد منوی استارت شوید و کنترل پنل را انتخاب کنید و به این بخش وارد شوید. پس از ورود به کنترل پنل، نیاز است که وارد بخش network and internet شوید. سپس وارد قسمت network and sharing centerشوید تا بتوانید به قسمت‌های مختلف دسترسی داشته باشید. در این قسمت نیاز است که از منوی کناری گزینه change adapter settings را انتخاب کنید تا بتوانید به شبکه‌هایی که می‌خواهید دسترسی داشته باشید.

ورود به شبکه اینترنت مورداستفاده

در قسمت بعدی نیاز است که از پنجره باز شده، شبکه اینترنتی که در حال حاضر به آن متصل هستید را انتخاب کنید. فرقی نمی‌کند که از وای فای استفاده می‌کنید یا از شبکه کابلی، لیست تمام سرویس‌ها قابل مشاهده هستند و می‌توانید آنها را انتخاب کنید. در مرحله بعدی روی شبکه موردنظر کلیک راست کنید و گزینه properties را بزنید تا بتوانید وارد تنظیمات همان شبکه خاص شوید.

تنظیم DNS برای دور زدن تحریم

در پنجره‌ای که در مرحله قبل برایتان باز شده است، نیاز است که از بین گزینه‌های موجود، گزینه internet protocol version 4را انتخاب کنید. سپس روی دکمه properties که در پایین این گزینه فعال می‌شود کلیک کنید تا بتوانید تنظیمات موردنظر را انجام دهید. در مرحله بعدی نیاز است که حالت use the following DNS server addressرا انتخاب کنید تا بتوانید دی ان اس های موردنظر خودتان را وارد کنید. در این مرحله دو قسمت برای دی ان اس وجود دارد که کافی است دی ان اس های دریافت شده را در این قسمت‌ها وارد کنید و در نهایت روی گزینه ok بزنید تا تنظیمات ذخیره شود. پس از این مرحله به راحتی می‌توانید از دی ان اس های ذخیره شده روی شبکه‌ای که انتخاب کرده اید استفاده کنید و از سایت‌هایی که می‌خواهید بازدید کنید و مشکلی در این زمینه نداشته باشید.

آیا با DNS برای دور زدن تحریم میتوان سایت‌های فیلتر را مشاهده کرد؟

خیلی از افراد ممکن است این سوال را بپرسند که آیا با تغییر دی ان اس می توان از سایت‌هایی که در ایران فیلتر هستند نیز بازدید کرد. باید بگوییم که این امکان وجود ندارد و دی‌ان‌اس‌ها فقط وبسایت‌هایی را به شما نمایش می‌دهند که ایران را تحریم کرده‌اند. این وبسایت‌ها این اجازه را به شما نمی‌دهند که بتوانید از وبسایت‌هایی که فیلتر هستند بازدید کنید، به همین خاطر برای بازدید از آنها باید از همان وی‌پی‌ان استفاده کنید.

در نهایت به معرفیِ مفهومِ Tunneling می‌پردازیم که یکی از بهترین و بی‌نقص‌ترین روش‌های موجود جهت دور زدنِ تحریم‌ها یا سیستم‌های فیلترینگ است:

تونل زدن یا Tunneling چیست؟

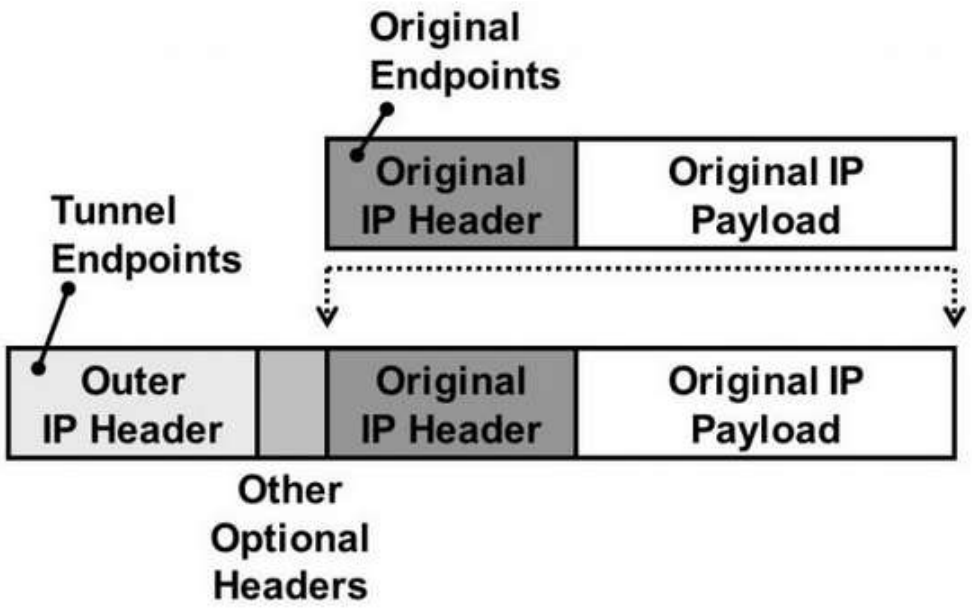
در دنیای فیزیکی، tunnelingراهی برای عبور از زمین یا مرزهایی است که به طور معمول نمی توان از آنها عبور کرد .به همین ترتیب، در شبکه، تونل ها روشی برای انتقال داده ها از طریق شبکه با استفاده از پروتکل هایی هستند که توسط آن شبکه پشتیبانی نمی شوند tunneling .با کپسوله سازی بسته ها انجام میشود که به صورت بسته بندی بسته ها در داخل بسته های دیگر تعریف میشود.

از tunneling اغلب در شبکه های خصوصی مجازی یا همان VPN ها استفاده میشود. همچنین از دیگر ویژگی های آن میتوان به ایجاد ارتباط ایمن بین شبکه ها، امکان استفاده از پروتکل های پشتیبانی نشده، حفاظت ازfirewall ها، اشاره کرد.

کپسوله سازی بسته ها چگونه انجام می شود؟

داده هایی که قصد ورود به شبکه را دارند به بسته هایی تقسیم می شوند. یک بسته معمولی دارای دو قسمت استheader :، که شامل آدرس مبدا و مقصد و پروتکل مورد استفاده است، و payload که محتوای واقعی بسته را شامل می شود و حاوی دیتا است.

یک بسته کپسوله شده در اصل یک بسته در داخل یک بسته دیگر است. در یک بسته کپسوله شده، headerو payhoad بسته اول وارد قسمت payload بسته دوم می شود. در واقع بسته اصلی خود به payloadتبدیل می شود.



پروتکل های : Tunneling

داده ها از طریق اینترنت توسط پروتکل ها بین هر دو دستگاه دیجیتالی جریان می یابند. به طور کلی، پروتکل های tunnelingبرای ارسال داده های شبکه خصوصی از طریق یک شبکه عمومی استفاده می شوند و همچنین می توانند برای افزایش امنیت داده های رمزگذاری نشده هنگام ارسال از طریق شبکه عمومی استفاده شوند. از جمله پروتکل های معروف می توان به(Secure Shell (SSH ، Point-to-Point Tunneling (PPTP)و IPsec ، L2TPاشاره کرد که هر کدام برای یک هدف خاص و متفاوت طراحی شده اند.

از آنجا که در پروتکل هایtunneling ، یک بسته بطور کامل در payload قرار میگیرد، احتمال سوءاستفاده نیز به وجود می آید. از tunneling برای عبور از فایروال های پیچیده یا پیکربندی های نامناسب نیز استفاده می شود به این صورت که پروتکل هایی که اجازه عبور از فایروال را ندارند کپسوله سازی می شوند و از طریق پروتکل هایی دیگر از فایروال عبور میکنند. همچنین، استفاده از پروتکل های tunneling، اقداماتی مانند بازرسی بسته های اطلاعاتی در جایی که شبکه به دنبال بسته های مشکوک است را دشوار میکند.

در ادامه به تعریف و بررسی برخی از پروتکل های tunneling می پردازیم:

- PPTPاین پروتکل توسط شرکت ماکروسافت ساخته شده که مخفف Point to Point Tunneling Protocolاست و جز اولین پروتکل‌های استاندارد VPN به حساب می‌آید و همچنین اولین پروتکل VPN است که توسط ویندوز پشتیبانی شد و امنیت آن به واسط نحوه احراز هویت آن تامین می‌شود. تقریبا هر وسیله‌ای که قابلیت VPN را دارد، PPTPرا نیز دارد. اما با توجه به این

که رمزگذاری 128 بیتی دارد، مشکلات امنیتی متعددی نیز دارد که توسط سازمان‌های مختلف امنیتی و سیاسی قابل بازگشایی هستند. اگر امنیت ارتباطتان اهمیت ندارد PPTPمی‌تواند بهترین گزینه برای شما باشد.

- L2PT/ IPsecمخفف Layer 2 Tunneling Protocol می‌باشد و برخلاف بقیه پروتکل‌های VPNاز هیچ متد رمز گذاری استفاده نمی‌کند. با توجه به این موضوع عموما با پروتکل رمزگذاری دیگری پیاده‌سازی می‌شود که با IPsec شناخته می‌شود و امنیت و حریم خصوصی را برای کاربران تامین می‌کند. همه دستگاه‌های مدرن قابلیت استفاده از L2TP را دارد که نصب آن مانند PPTP آسان است. اما مشکل آن این است که از پورت UDP 500 استفاده می‌کند که به راحتی توسط فایروال‌ها بسته می‌شود. در حال حاضر مشکل امنیتی مهمی در IPsec وجود ندارد و اگر به درستی استفاده شود همچنان می‌تواند امن باشد.

- SSTPدر زمان ویندوز ویستا توسط ماکروسافت معرفی شد که مخفف Secure Socket Tunneling Protocolاست. در لینوکس و برخی از RouterOS ها نیز وجود دارد اما معمولا در دستگاه‌های ویندوزی استفاده می‌شود. از آنجایی که از SSL v3استفاده می‌کند مزایای آن مشابه OpenVPNاست، مثلا مشکل نت و فایروال را ندارد. این VPN با ثبات بود و به راحتی قابل استفاده است ولی چون معمولا در ویندوز استفاده می‌شود به عنوان استاندارد مانند بقیه پروتکل‌ها شناخته نمی‌شود.

- IKEv2پروتکلی است بر پایه IPsec که مخفف Internet Key Exchange Version 2 می‌باشد. محصول مشترک Cisco و Microsoft است و با پلتفرم‌های مختلف نیز سازگار است. زمانی که اتصال قطع شود به سرعت ارتباط را مجدد وصل می‌شود که این مزیت بسیار خوبی برای کابران موبایل است IKEv2 .جز معدود پروتکل‌هایی است که Blackberry را پشتیبانی میکند IKEV2 . نسبت به IPsec کمتر است ولی بسیار امن، پایدار، و کارآمد است.

VPN Tunnelingچیست؟

VPNیک اتصال امن و رمزگذاری شده بر روی یک شبکه عمومی و مشترک ایجاد میکند tunneling . فرایندی است که طی آن بسته های VPN به مقصد مورد نظر خود می رسند که معمولاً یک شبکه خصوصی است .بسیاری از VPN ها از مجموعه پروتکل IPsec استفاده می کنند. بسیاری از VPN ها از مجموعه پروتکل IPsec استفاده می کنند. پروتکل دیگری که برای VPN استفاده می شود، Transport Layer

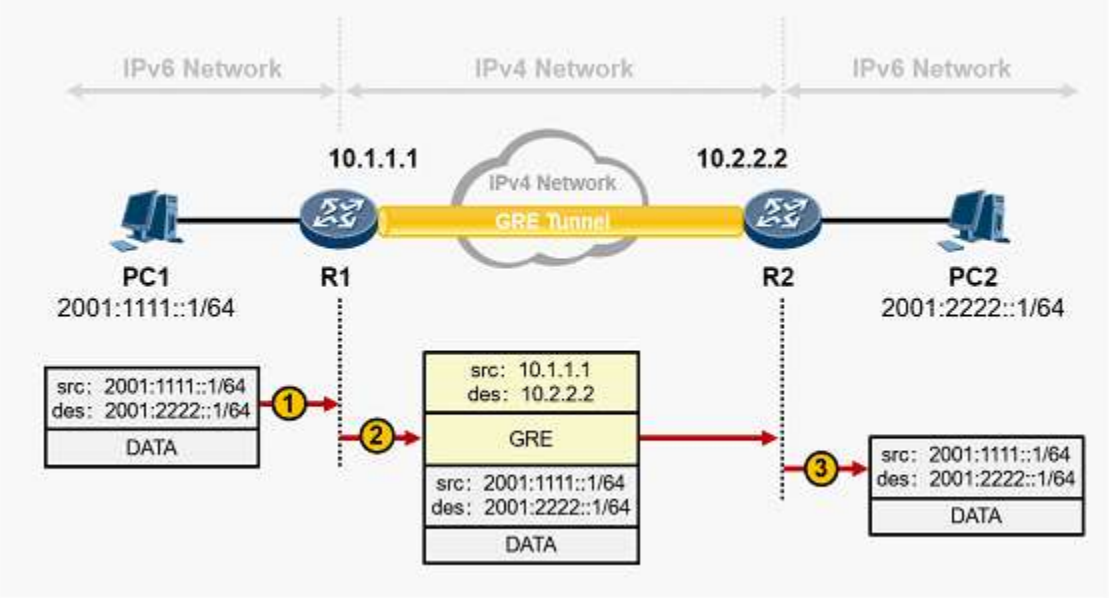
Security (TLS)است. این پروتکل بسته به نحوه تفسیر مدل در لایه 6 یا لایه 7 مدل OSI کار می کند . TLSرا گاهی SSL می نامند ، اگرچه SSL به پروتکل قدیمی تری اشاره دارد که دیگر از آن استفاده نمی شود.

Split tunnelingچیست؟

معمولاً وقتی کاربر دستگاه خود را به VPN متصل می کند، تمام ترافیک شبکه وی از طریق تونل VPN عبور می کند Split tunneling .به برخی از ترافیک ها اجازه می دهد تا خارج از تونل VPN حرکت کنند. در حقیقت ، Split tunnelingبه شما امکان می دهد دستگاه های کاربر به طور همزمان به دو شبکه متصل شوند: یکی عمومی و دیگری خصوصی.

GRE tunnelingچیست؟

تونل‌های بنا شده بر پایه پروتکل GRE به طور معمول بین دو روتر مشخص برقرار می‌شوند به شکلی که هر روتر نقش یک سر تونل را ایفا می‌کند. تنظیمات روترها به شکلی ایجاد شده تا پکت‌های GRE را مستقیما به یکدیگر انتقال دهند. هر روتر دیگری بین این دو، پکت‌های کپسوله‌سازی شده را باز نمی‌کند و تنها آن‌ها را انتقال می‌دهد.



IP-in-IP tunnelingچیست؟

IP-in-IPیک پروتکل تونل زنی برای کپسوله سازی بسته های IP در داخل بسته های IP دیگر است-IP . in-IPبسته ها را رمزگذاری نمی کند و برای VPN ها استفاده نمی شود. کاربرد اصلی آن تنظیم مسیرهای شبکه است که معمولاً در دسترس نیستند.

مفهوم تانلینگ در شبکه

پروتوکل تونلینگ یا تانلینگ **(Tunneling)** به عنوان راهکاری برای برقراری ارتباط از طریق یک شبکه خصوصی ویژه شبکه های درون سازمانی است.

در این روش تونل ارتباطی، بسته دیتا که در درون یک بسته دیگر قرار گرفته را از طریق یک شبکه عمومی به مقصد می رساند.

راهکار تونلینگ در بستر های مختلف مخابراتی، ارتباط داخلی بین شعبات و یا دفاتر یک شرکت یا سازمان را فراهم می کند و همچنین ویژگی های امنیتی بسیاری مانند گزینه های رمزگذاری را ارائه می دهد.

تعریف تانلینگ (Tunneling)

تانلینگ پروتکلی است که امکان جابجایی امن داده ها از یک شبکه به شبکه دیگر را فراهم می کند. تونلینگ مستلزم ارسال دیتای ارتباطات شبکه خصوصی از طریق فرآیندی به نام **محصور سازی** از طریق شبکه عمومی مانند اینترنت است.

فرایند محصور سازی اجازه می دهد تا بسته های داده در یک شبکه عمومی ظاهر شوند تا به آنها امکان عبور از بستر امن تونل داده شود.

در فرایند تونلینگ، داده ها به قطعات کوچکتر به نام بسته ها شکسته می شوند تا بتوانند درفرایند ارسال و دریافت در طول تونل حرکت می کنند. با بسته شدن بسته ها از طریق تونل، آنها رمزگذاری می شوند و فرآیند دیگری به نام محصور سازی اتفاق می افتد.

داده های شبکه خصوصی و پروتکل اطلاعاتی که با آن همراه است، برای ارسال در واحدهای انتقال شبکه عمومی محصور می شوند .واحدها مانند داده های عمومی هستند و امکان انتقال آنها از طریق اینترنت فراهم می شود. محصور کردن اجازه می دهد تا بسته ها به مقصد مناسب خود برسند. در انتها فرایند رمزگشایی بسته ها در مقصد نهایی اتفاق می افتد.

در شبکه های رایانه ای، پروتکل تونلینگ یک پروتکل ارتباطی است که امکان جابجایی داده ها از یک شبکه به شبکه دیگر را بطور اختصاصی فراهم می کند. از آنجا که تونلینگ شامل دسته بندی مجدد داده های تولید شده به شکل دیگری است، با رمزگذاری به صورت استاندارد، می تواند ماهیت ترافیکی را که از طریق یک تونل اجرا می شود مخفی کند.

مثالی برای تانلینگ

به عنوان مثال شما صاحب یک شرکت دارای شبکه کامپیوتری هستید و می خواهید شعبه ای از شرکت را در خارج از محل شرکت را به قسمتی از اطلاعات درون شرکت متصل کنید، برای این کار با ایجاد ارتباط تونلینگ بستر امن ایجاد کرده و دسترسی به منابع اشتراک گذاری شده مقدور می باشد.
برای پیاده سازی تونلینگ باید در هر دو طرف ارتباط نیازمند یک روتر با قابلیت پشتیبانی از یکی از پروتکل های تونلینگ و ارتباط با شبکه اینترنت یا اینترانت تحت IP استاتیک می باشد.

سپس با تنظیمات هر دو شبکه این ارتباط برقرار شده و امکان تبادل اطلاعاتی مانند انتقال تصویر سیستم های نظارتی (دوربین مدار بسته)، سیستم های تلفن تحت شبکه(VOIP) ، سیستم های اتوماسیون اداری و مالی تحت شبکه و ... امکان پذیر می باشد.

مزایا و معایب تونلینگ

از مزایای ارتباط تونلینگ میتوان به امنیت بالای اطلاعات رمزنگاری شده جهت جلوگیری از دسترسی و سواستفاده از اطلاعات اشاره کرد. همچنین میتوان کنترل و نظارت بر اطلاعات تبادل شده را نیز برای مراتب امنیتی ایجاد کرد.
یکی ازمعایب تونلینگ میتواند وابستگی به پایداری و ارتباط هر دو طرف در شبکه باشد . انتخاب پروتکل نامناسب بدون در نظر گرفتم نوع اتصال شبکه نیز از دیگر معایب کیفیت پایین تونلینگ و ارتباط ناپایدار آن می باشد.

هزینه ی ارتباط تونلیگ اغلب از هزینه ارتباط مستقیم بین شعب و سازمان ها کمتر بوده و بستگی به میزان و نرخ اطلاعات منتقل شده محاسبه می گردد . همچنین در مواردی که نیازمند ارتباط از راه دور بین شهری یا حتی بین کشوری باشد تونلینگ بهترین و مقرون به صرفه ترین گزینه ارتباطی می باشد.

پروتکل های تانلینگ یا تونلینگ

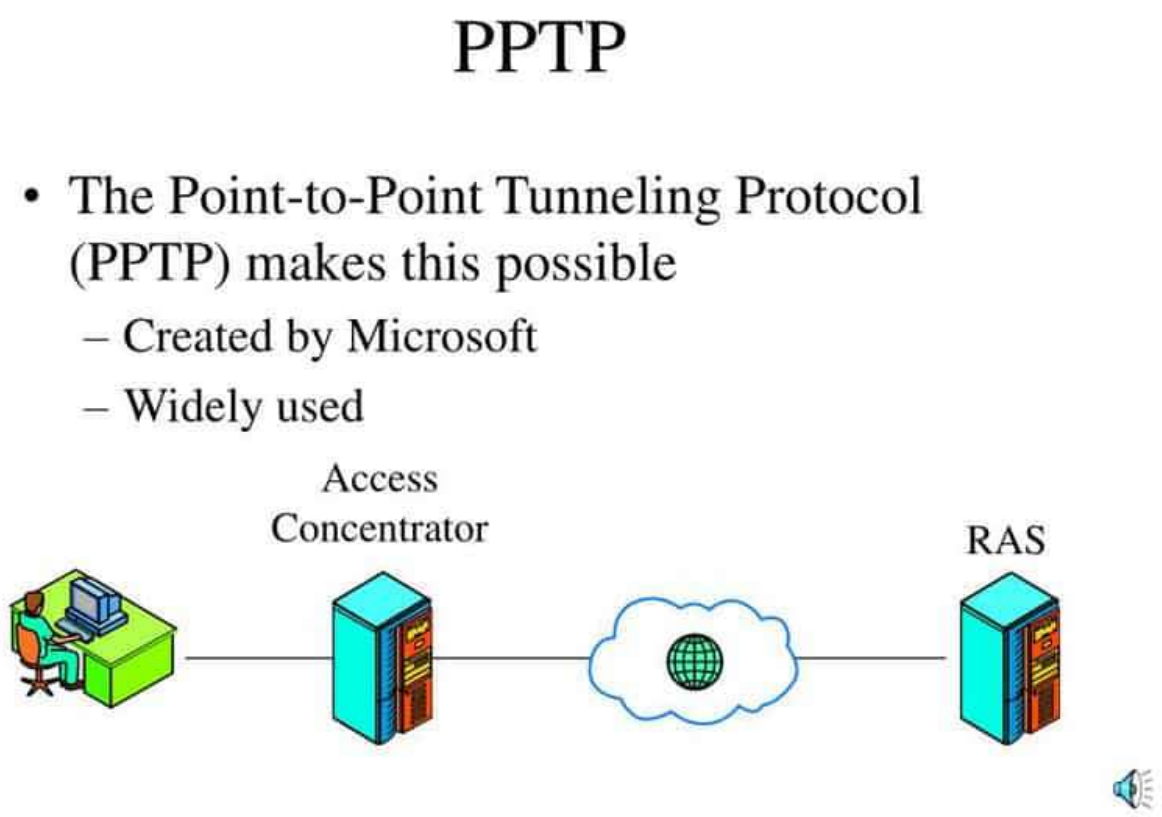
انواع پروتکل های تونلینگ و همچنین روش های پیاده سازی آن در شبکه عبارتند از

1. PPTP
2. IPsec
3. sstp
4. open VPN
5. GRE
6. Ethernet over IP (EoIP)

1. PPTP

پروتکل تونلینگ Point to Point (PPTP) یکی از قدیمی ترین پروتکل هایی است که امروزه توسط کارشناسان شبکه مورد استفاده قرار می گیرد PPTP . توسط مایکروسافت ایجاد و با ویندوز ۹۵ منتشر شد، داده های شما را در بسته ها رمزگذاری می کند و آنها را از طریق تونلی که ایجاد می شود از طریق اتصال به شبکه شما ارسال می کند.

PPTPیکی از ساده ترین پروتکل ها برای پیکربندی است و برای اتصال به سرور فقط نیاز به نام کاربری، رمز عبور و آدرس سرور دارد. این یکی از سریعترین پروتکل های تانلینگ به دلیل سطح رمزگذاری پایین است.



2. L2TP / IPSec

پروتکل تونلینگ لایه ۲ (L2TP) برای ایجاد یک پروتکل تونل ایمن تر از PPTP استفاده می شود L2TP . داده ها را رمزگذاری می کند ، اما به اندازه کافی رمزگذاری نمی شود تا زمانی که IPSec (پروتکل اینترنت ایمن) داده ها را دوباره با رمزگذاری خود پیچاند تا دو لایه رمزنگاری را ایجاد کند و محرمانه بودن بسته های داده را که از طریق تونل عبور می کند ، تضمین کند.

L2TP / IPSecرمزگذاری AES-256 بیتی را ارائه می دهد ، یکی از پیشرفته ترین استانداردهای رمزنگاری که قابل اجرا است. این محصور سازی دو برابر ، آن را کمی آهسته تر از PPTP می کند. همچنین می تواند با دور زدن دیوارهای فایروال محدود شود زیرا از پورت های ثابت استفاده می کند و باعث می شود اتصالات VPNبا L2TP مسدود شود. با این وجود L2TP / IPSec با توجه به سطح بالای امنیتی که ارائه می دهد ، پروتکل بسیار محبوب است.

3. SSTP

پروتکل Secure Socket Tunneling، که به دلیل توانایی حمل و نقل داده ها از طریق لایه های Secure Sockets Layerیا SSL نامگذاری شده است ، بصورت محلی در ویندوز پشتیبانی می شود و تنظیم این پروتکل خاص را برای کاربران ویندوز آسان می کند SSL .داده های اینترنت را از طریق SSTP بسیار ایمن می کند و از آنجا که پورتی که از آن استفاده شده ثابت نیست ، احتمالاً با فایروال ها کمتر از L2TPمی جنگد. به عنوان یک پروتکل تونل سازی مبتنی بر ویندوز، SSTPدر هیچ سیستم عامل دیگری موجود نیست.

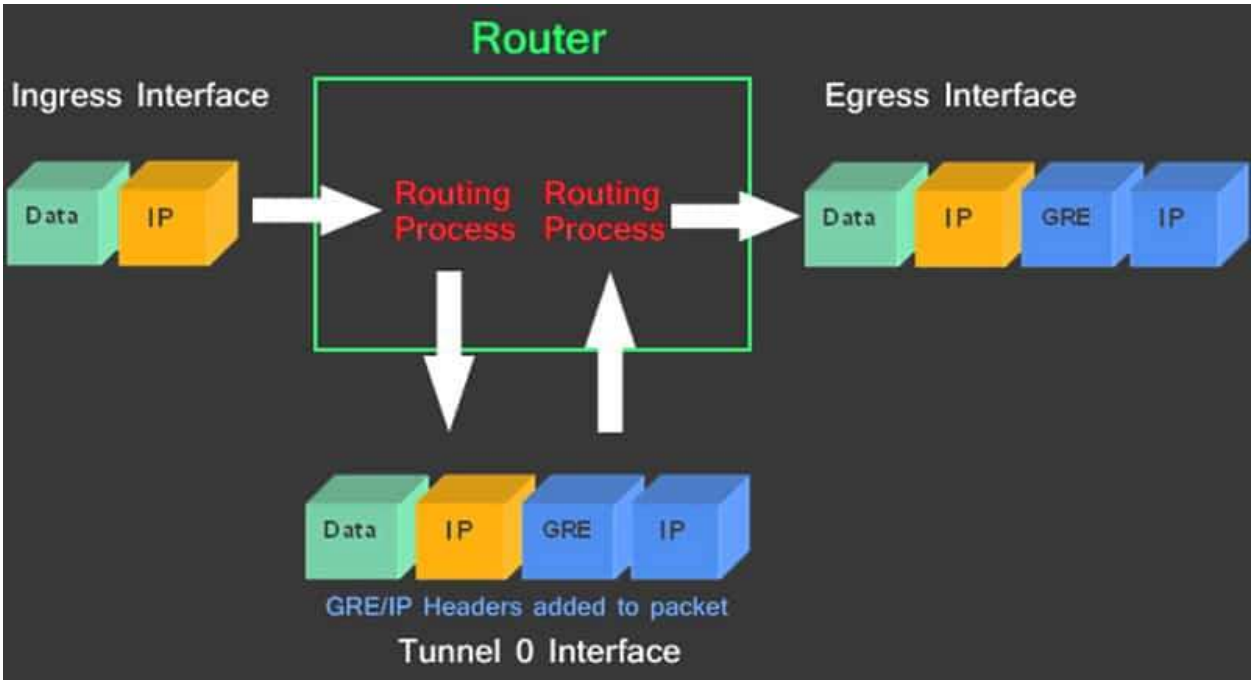
OpenVPN .4

OpenVPNیک پروتکل تونل سازی منبع باز نسبتاً اخیر که از رمزگذاری AES 256 بیتی برای محافظت از بسته های داده استفاده می کند. از آنجا که پروتکل منبع باز است ، کد امنیتی توسط جامعه امنیتی شبکه که دائما به دنبال نقص امنیتی احتمالی هستند ، به طور کامل و منظم مورد بررسی قرار می گیرد.

این پروتکل در ویندوز ، مک ، اندروید و iOS قابل تنظیم است، اگرچه برای تنظیم پروتکل به نرم افزار شخص ثالث نیاز است و پیکربندی پروتکل به سختی ممکن است. با این وجود، OpenVPNپس از پیکربندی، الگوریتم های رمزنگاری گسترده و گسترده ای را فراهم می کند که به کاربران امکان می دهد داده های اینترنتی خود را ایمن نگه دارند و حتی با سرعت سریع اتصال فایروال ها را دور بزنند.

5. GRE (Generic Routing Encapsulation)

GREو IP / IP تونل های رمز نگاری نشده هستند. آنها بدون مخفی کردن ارتباطات، اتصالات مجازی را بر روی IP استاتیک بین روتر ها ارائه می دهند. بنابراین به دلیل سادگی، آنها می توانند جایگزین های جذابی باشند. با این حال ، تونل های IP / IP هیچ اهراز هویتی را ارائه نمی دهند، و تونل های GRE تنها احراز هویت ضعیفی را ارائه می دهند.



6. Ethernet over IP (EoIP)

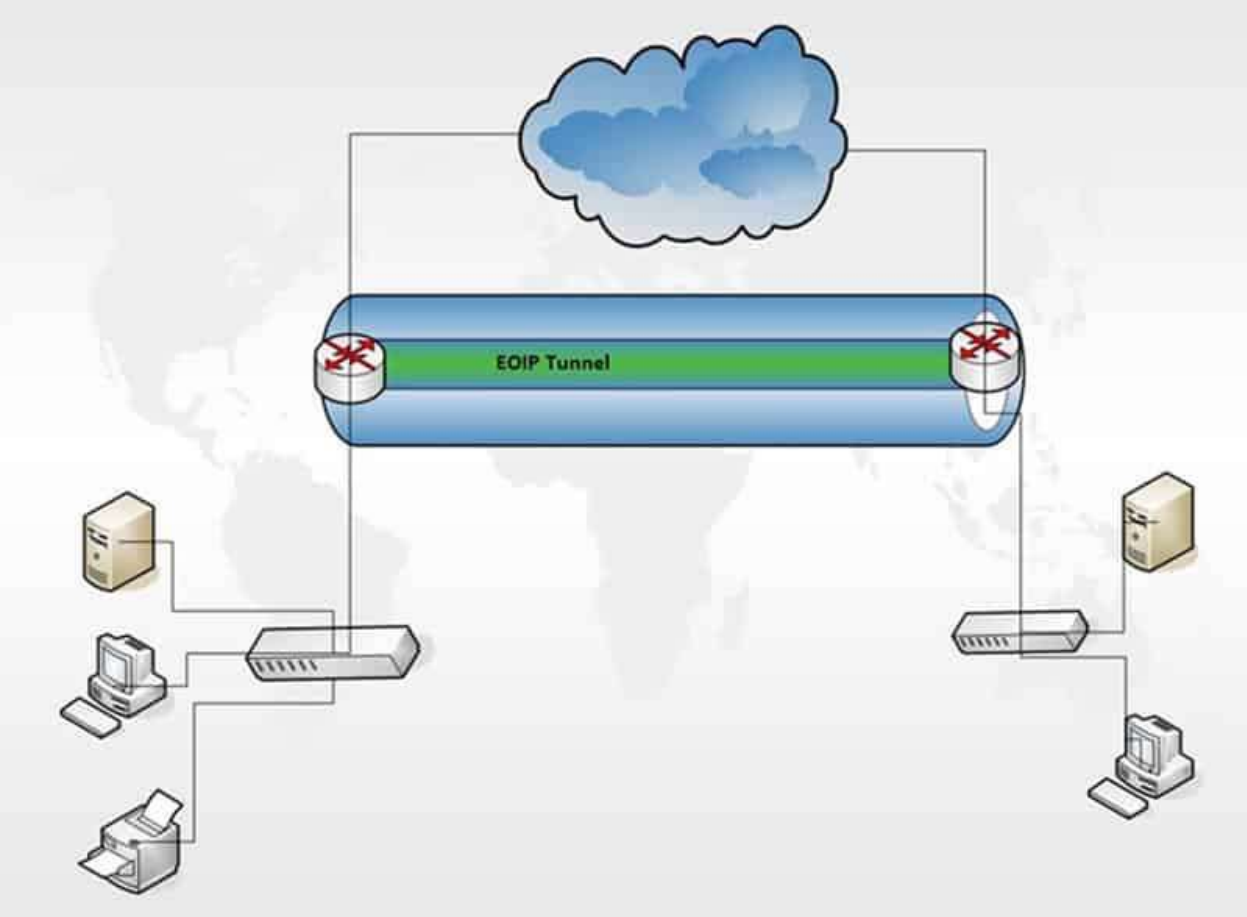
(EoIP)یک پروتکل MikroTik RouterOS است که یک تونل اترنت بین دو روتر را در بالای یک اتصال IPایجاد می کند. رابط EoIP به عنوان یک رابط اترنت ظاهر می شود. دقیقاً به عنوان جائی که در آنجا یک رابط اترنت فیزیکی و کابل بین دو روتر (با امکان فعال کردن پل) وجود دارد. این پروتکل چندین طرح شبکه را امکان پذیر می کند.

راه اندازی شبکه با رابط های:EoIP

امکان Bridge کردن LAN ها از طریق اینترنت

امکان Bridge کردن LAN ها بر روی تونل های رمزگذاری شده

امکان Bridge کردن شبکه ها از طریق شبکه های بی سیم802.11b ’ad-hoc‘



فرق بین وی پی ان و تانل چیست؟

(شبکه مجازی اختصاصی) و تونل زنی تکنیکهایی هستند که امکان اتصال رمز شده بین کامپیوتر شما و یک کامپیوتر دیگر را فراهم میکنند. آن کامپیوتر ممکن است متعلق به شرکت شما، یک فرد مورد اعتماد یا یک سرویس تجاری VPN باشد. تونل زنی یک جریان داده خاص را با یک پروتکل رمزنگاری ارائه میکند، و در نتیجه اطلاعاتی که در تونل مبادله میشوند برای سایرین غیر قابل خواندن نخواهد بود. استفاده از VPN ها در شرکتهایی که کارمندان آنها از خانه و از طریق اینترنت به اطلاعات حساس و محرمانه شرکت دسترسی دارند، بکار میرود.

استفاده از VPN یا انواع دیگر تونلها برای رمز کردن اطلاعات، راه حل مناسبی برای اطمینان از اینکه کسی به جز شما و افراد مورد اعتمادتان به اطلاعات دسترسی ندارند، میباشد. تاثیر دیگر اینکار اینست که کل اطلاعاتی که مورد دسترسی شما قرار میگیرد از دید استراق سمع کننده یا مسدود کننده دسترسی، یکسان بنظر برسد. از آنجا که بسیاری از شرکتهای بین المللی از VPNاستفاده میکنند، کمتر احتمال میرود که اتصال VPN مسدود شود.

در این تکنیکها یک تونل از کامپیوتر شما به کامپیوتر دیگری در اینترنت ایجاد می شود. داده شما از طریق این تونل در وب به مقصد منتقل میشود. جامعیت داده و محرمانه بودن ترافیک داخل تونل با استفاده از رمز نگاری اعمال میشود.

TUNNEL

تفاوت اصلی بین اتصال VPN و یک تونل اینست که سیستم VPN بگونه ای تنظیم شده که تمام داده جابجا شده را بین کامپیوتر شما و اینترنت رمز میکند ولی تونل فقط داده جابجا شده توسط کاربردهای خاصی از طریق شماره پورتهای مشخصی را رمز میکند. برخلاف VPN ، تونلها نیاز دارند که هر کاربردی نظیر مرورگر وب، نرم افزار ایمیل یا برنامه ارسال پیام آنی را که نیاز به ارسال امن اطلاعات دارند، بطور جداگانه برای استفاده از تونل پیکربندی شوند.

بطور مشخص، همه برنامه های کاربردی قادر به ارسال اطلاعات از طریق تونل نیستند. بیشتر سیستمهای ارسال صوت از طریقIP (VoIP)، از پروتکل UDP استفاده میکنند که در بیشتر سیستمهای تونل زنی، پشتیبانی نمیشود. همچنین، بعضی کاربردهای معمول نظیر مرورگرِ وب Opera دارای پشتیبانی داخلی از پراکسی Socks که متداولترین نرم افزار تونل زنی است، نیستند. در این موارد، نیاز به استفاده از یک نرم افزار جداگانه نظیر FreeCap (http://www.freecap.ru/eng/) تحت ویندوز، یا tsocks(http://tsocks.sourceforge.net/) تحت لینوکس خواهید داشت.

وقتی که یک تونل برقرار شد و نرم افزارهای کاربردی برای استفاده از آن پیکربندی شدند، آنها اطلاعات خود را بطور رمز شده از طریق تونل ارسال خواهند کرد. کاربران با یک سرویس تونل زنی در کشوری که

فیلتر گذاری ندارد، مرتبط شده و از طریق آن مبادله اطلاعات میکنند. سرویسهای تجاری تونل زنی، معمولا هزینه ای حدود پنج دلار در ماه دارند (که معمولا با کارت اعتباری قابل پرداخت است).

سرویسهای مختلف تونل زنی نیز قابل دسترسی هستند. وقتی که از سرویسهای تونل زنی مجانی استفاده شود، کاربران باید توجه داشته باشند که این سرویسها معمولا همراه با تبلیغات هستند، که تبلیغات معمولا بصورت متن رمز نشده منتقل میشود و در نتیجه ممکن است، نظارتگر شبکه را متوجه استفاده از سرویس تونل زنی، نماید. بعلاوه بیشتر سرویسهای تونل زنی مبتنی بر پراکسی Socks هستند که ممکن است دارای روزنه نفوذی DNS باشند. بعضی از سیستمهای تونل زنی مجانی (و با سرعت کم) در زیر آورده شده اند:

- http://www.http-tunnel.com/
- http://www.hopster.com/
- http://www.htthost.com/

VPN

برخلاف تونل ها، سیستمهای VPN تمام داده منتقل شده، از جمله صوت روی IP و ارتباطات برنامه های کاربردی بدون پشتیبانی از Socks را رمزنگاری میکنند. وقتی VPN آماده به کار شد، ابزار کاملتری برای کار نسبت به تونل است، ولی در عوض پیچیدگی راه اندازی آن بیش از تونل زنی است.

استانداردهای مختلقی برای راه اندازی شبکه های VPN وجود دارد، شامل IPSec، SSL/TLS و PPTP که دارای پیچیدگیها، سطح امنیتی و قابلیت اجرا روی سیستم عاملهای مختلف هستند. همچنین پیاده سازیهای مختلف هر استاندارد در نرم افزارها به همراه قابلتهای گوناگونی در دسترس میباشند.

با اینکه PPTP در رمزنگاری، ضعیفتر از IPSec یا SSL/TLS قلمداد میشود، ممکن است برای دور زدن سدهای اینترنتی مفید باشد، زیرا در بیشتر نرم افزارها و همچنین نسخه های مختلف ویندوز بصورت درونساز قابل دسترس است.

شبکه های VPN مبتنی بر SSL/TLS برای پیکربندی نسبتا ساده هستند و سطح قابل اطمینانی از محرمانگی را ارائه میکنند.

IPSec در سطح اینترنت اجرا میشود و در معماری اینترنت وظیفه انتقال بسته ها را بر عهده دارد، ولی سایر روشها در لایه برنامه کاربردی اجرا میشوند. همین ویژگی، IPSec را نسبت به سایر روشها که در لایه بالاتر اجرا میشوند، امن تر میسازد. نیازی نیست که برنامه کاربردی برای کار با IPSec بطور خاص طراحی شود، ولی برای استفاده از SSL/TLS یا سایر پروتکلهای لایه بالاتر بایستی تدابیر خاصی در طراحی

نرم افزار کاربردی در نظر گرفته شوند.

VPN ها اغلب توسط شرکتها و سازمانها بعنوان کانالهای ارتباطی خصوصی و امن، استفاده میشوند. به دلیل رایج بودن آنها، سرویسهای تجاری VPN متعددی وجود دارند که با پرداخت هزینه حدود 5 تا 10

دلار در ماه قابل دسترس هستند. برای استفاده از چنین سرویسهایی لازم است که ارائه دهنده سرویس قابل اعتماد باشد. لیست سرویس دهندگاه VPN تجاری در اینجا قابل دسترسی است:

http://en.cship.org/wiki/VPN

بعنوان جایگزینی برای سرویسهای تجاری VPN، کاربرانی که دارای دوست یا آشنائی در محلی که اینترنت سانسور نمیشود، باشند، میتوانند سرویس VPN اختصاصی راه اندازی نمایند. این شیوه مجانی خواهد بود، ولی نیاز به دانش فنی بیشتر خواهد داشت. همچنین اختصاصی بودن این سرویس احتمال مسدود شدن آن نسبت به یک سرویس تجاری را کمتر خواهد کرد. یکی از محبوب ترین نرم افزارهای VPN اختصاصی OpenVPN (http://openvpn.net/) میباشد، که میتوان آن را روی ویندوز، MacOS و لینوکس و بسیاری سیستمهای عامل دیگر نصب کرد.

مزایا

نرم افزارهای تونل زنی و VPNها امکان انتقال رمز شده داده را فراهم می آورند. این نرم افزارها معمولا نه تنها دارای امکان انتقال ترافیک وب، بلکه دارای بسیاری قابلیتهای مربوط به اتصال پراکسی امن نیز هستند. به همین جهت یکی از مطمئن ترین روشهای دور زدن سانسور اینترنتی میباشند. و وقتی که پیکربندی شدند، استفاده از انها نیز ساده خواهد بود.

استفاده از نرم افزارهای تونل زنی و VPN برای کاربرانی که از نظر فنی توانمند بوده و نیاز به سرویس دور زدن سانسور و دسترسی به اینترنت از طریق کامپیوتر خود دارند، روش مناسبی است. سرویسهای تونل زنی تجاری برای کاربرانی که در محلهای با سانسور زندگی میکنند و کسی را در محلهای بدون سانسور ندارند، نیز میتواند روش مناسبی باشد؛ تکنولوژی VPN نیز از آنجا که معمولا در کاربردهای تجاری مورد استفاده قرار میگیرد، بعید است که مسدود شود.

بعضی (نه همه) سرویسهای VPN و تونل زنی تجاری در تبلیغات خود حفظ ناشناسی را نیز عنوان میکنند، که در سرویسهای اختصاصی قابل حصول نیست. اگر سرویس دهنده تجاری تونل یا VPN قابل اعتماد باشد، "ناشناسی" در حد قابل قبولی حفظ خواهد شد.

معایب و ریسکها

سرویسهای تونل زنی و VPNهای تجاری، قابل شناسائی و فیلتر گذاری هستند. این سرویسها معمولا در محلهای عمومی (نظیر کافی نت یا کتابخانه) که امکان نصب نرم افزار وجود ندارد قابل استفاده نیستند. استفاده از نرم افزار های VPN و مخصوصا تونل زنی ممکن است نیاز به دانش فنی بیشتری نسبت به سایر روشهای دور زدن داشته باشد.

یک اپراتور شبکه میتواند استفاده از VPN و همچنین سرویس دهنده VPN را تشخیص دهد. اپراتور شبکه قادر به مشاهده اطلاعات مبادله شده با VPN (اگر VPN درست نصب شده باشد) نخواهد بود.

اپراتور VPN یا تونل (مشابه اپراتور پراکسی) میتواند به عملیات شما نظارت کند، مگر اینکه از رمز نگاری اضافه بر VPN استفاده نمائید؛

در غیر اینصورت میبایست در مورد قابل اطمینان بودن اپراتور VPN یا تونل اطمینان حاصل نمائید.

معرفی SSH Tunneling

تعریفSSH

SSH(پوسته امن)،پروتکل استانداردی برای مبادله ی رمز شده بین یک کامپیوتر و یک سرویس دهنده است. پروتکل رمزنگاری از مشاهده اطلاعات مبادله شده توسط اپراتور شبکه جلوگیری میکند SSH . میتواند برای کاربردهای متعددی بکار رود، که برقراری اتصال امن (secure login) و انتقال فایل امن (SCP/SFTP)کاربردهای رایج آن هستند.

کاربردهایSSH Tunneling

پروتکل SSH از آن دسته پروتکل هایی است که قابلیت های مرموز و در عین حال مخفی ای دارد که بسیاری از افرادی که از این پروتکل استفاده میکنند، به آن پی نبرده اند. یکی از این قابلیت ها، توانایی در ایجاد تونل های Encryptشده در بطن پروتکل SSH است، که کانال های ارتباطی دو طرفه را پشتیبانی میکند SSH . یک پروتکل امن ارتباطی است که داده ها را از میان یک Tunnelارتباطی امن منتقل می کند SSH . Tunnelingتکنیک دیگری است که مهاجمین می توانند از طریق آن محدودیت های فایروال ها را دور بزنند و از آنها عبور کنند. با استفاده از SSH Tunneling آدرس IP شما نیز در محیط اینترنت مخفی باقی می ماند بنابراین هیچکس نمی تواند شما را مانیتور و یا شنود کند.

یکی از دلایلی که پروتکی مثل SSH طراحی شد مشکلاتی بود که در بحث استفاده از آدرس های IP عمومی یا Public وجود داشت ، به این معنی که هر کسی می توانست از هر جای دنیا به آدرس IP سرور شما متصل شود و این شخص ممکن است یک هکر باشد. مهاجمین با داشتن آدرس IP Public شما امکان حمله به شما از هر جای دنیا را داشتند. توسعه و طراحی SSH Tunneling مشکلات بسیاری که در حوزه امنیت آدرس های IP عمومی وجود داشت را حل کرد.

مکانیزم کاری SSH Tunnel زیاد پیچیده نیست و در واقع این تکنیک از یک سرور و یک کلاینت تشکیل شده است که Session ارتباطی امنی بین همدیگر برقرار می کنند که هیچکس نمی تواند وارد این Sessionو ارتباطات آن شود و به همین دلیل امنیت بالایی دارد و از طرفی تجهیزات یا افرادی که در مسیر راه امکان شنود اطلاعات را دارند نیز نمی توانند وارد مسیر مورد نظر بشوند. ایجاد کردن یک Tunnelبرای ارتباط بین دو ماشین با آدرس های IP غیر عمومی یا Private نیازمند پیاده سازی سه مرحله ای و حداقل داشتن سه ماشین است ، این سه ماشین که در فرآیند SSH Tunnel استفاده می شوند موارد زیر هستند:

.1ماشین محلی(Local Machine)

.2یک ماشین واسط میانی دارای آدرس IP Public جهت ارتباط اینترنتی

.3ماشین هدف که دارای یک آدرس IP غیر عمومی است و قبل از ارتباط ماشین محلی بایستی ارتباطش با ماشین میانی برقرار شود.

SSH Tunneling

شما می توانید به ترتیب زیر Tunnel ایجاد کنید:

•یک SSH Connection از Local Machine تا ماشین واسط یا Intermediate Machine ایجاد کنید که دارای آدرس IP Public است.

•به SSH Connection فرمان بدهید که صبر کند و ترافیک را از Local Port به سمت Intermediate Machineیا ماشین واسط منتقل کند تا ماشین واسط به سمت ماشین هدف (Target Machine) ترافیک را با آدرس IP Private انتقال دهد ! به اینکار Port Acceleration یا Port Forwarding گفته می شود.

•بر روی Local Machine نرم افزاری که می خواهید با ماشین مقصد ارتباط داشته باشد را انتخاب می کنید و تنظیمات Port Forwarding را بر روی آن انجام می دهید. حالا هر زمان که شما به local port متصل شوید ! ترافیک شما خودکار به سمت Remote Machine منتقل می شود.

بصورت ساده تر شما از کامپیوتر مبدا یک ارتباط SSH با کامپیوتر واسط برقرار می کنید. کامپیوتر واسط یک آدرس IP معتبر اینترنتی دارد، شما هر ترافیکی که از ماشین مبدا بخواهید به مقصد برسد طبیعتا اول باید با کامپیوتر واسط ارتباط بگیرد. یعنی اگر بخواهیم بگوییم یک فایل را آپلود کند اول باید دستور ما به کامپیوتر واسط برسد .سیستم مقصد الزامی ندارد که IP عمومی داشته باشد چون اگر اینترنت داشته باشد کافی است که بتواند به کامپیوتر واسط وصل شود، هر ترافیکی با هر پورتی بخواهد از کامپیوتر مبدا به کامپیوتر مقصد منتقل شود باید در تونل SSHقرار بگیرد یعنی به عبارت دیگر تبدیل به پورت 22 شود!! خوب اینکار را میگوییم تبدیل پورت یا .Port Forwarding حالا هر نرم افزاری که قرار بود از سیستم مبدا به مقصد متصل شود را باید تنظیمات استفاده از SSH Tunnel را روی آن انجام بدهیم. شما اگر یک کامپیوتر با پروکسی اینترنت داشته باشید طبیعی است که باید تنظیمات پروکسی را روی نرم افزارهایی که اینترنت میخواهند انجام بدهید.

خوب برای اینکه ارتباط بین سیستم ها امن باشد SSH از دو کلید رمزنگاری PKI برای رمزنگاری مسیر و داده ها استفاده می کند. این کلیدها نمایانگر کامپیوترهای مورد اعتماد در مسیر ارتباطی هستند .زمانیکه یک SSH Connectionدر حال ایجاد شدن است ، هر دو ماشین کلیدهای عمومی خودشان را به همدیگر می دهند ، اما فقط کامپیوتری قادر به رمزگشایی خواهد بود که کلید خصوصی را داشته باشد.

HTTP Tunneling چیست؟

شما می توانید از پروتکل HTTP که بصورت ویژه برای استفاده از وب سایت ها کاربرد دارد برای Tunnelingبین کلاینت و سرور استفاده کنید Tunneling . را ما می توانیم به عنوان Port Forwarding نیز یاد کنیم که در واقع روشی است که شما اطلاعات شبکه محرمانه خودتان را در قالب اطلاعات یک

شبکه عمومی منتقل می کنید در عین حال که داده های شما درون کپسول های اطلاعاتی قرار میگیرند که برای دیگران نامفهوم است.

متوجه این موضوع هستم که کمی گنگ به نظر می رسد برای ساده تر شدن بیشتر مسئله فرض کنید که شما در شبکه داخلی یا هر شبکه دیگری یک فایروال دارید که اجازه عبور ترافیک پورتهای 20 و 21 که مخصوص ترافیک FTP هستند را نمی دهد ! اما طبیعی است که پورتهای 80 و 443 که مربوط به پروتکل های HTTP و HTTPS هستند بر روی این فایروال ها باز هستند ! حالا تصور کنید که ما درخواست های FTPخودمان را تبدیل یا بهتر بگوییم درون بسته های HTTP قرار بدهیم و از فایروال عبور بدهیم!!

این تکنیک را HTTP Tunneling می گوییم که یکی از روشهای دور زدن فایروال ها و عبور از مکانیزم های امنیتی محسوب می شود. در لفظ باز هم ساده تر شما در HTTP Tunneling یک پروتکل را درون پروتکل دیگر قرار می دهید و فایروال هم اجازه عبور آن را به شما می دهد HTTP Tunneling.بیشتر در مواردی که نوع پروتکل ها از نوع TCP هستند کاربرد دارد. ساختار کاری این تکنیک بصورت کلاینت و سروری است . این تکنیک بیشتر در زمانی کاربرد دارد که ارتباط بین دو نقطه شبکه از نظر فایروال بسته شده است و فقط پروتکل HTTP حق عبور دارد ، برای مثال در جاهایی که سرویس های NAT و Firewall و Proxy Serverقرار دارند این تکنیک می تواند بسیار کاربردی باشد.

دقت کنید که پروتکل های مشابه در مبدا و مقصد بایستی برای انتقال داده تعریف شوند یعنی در قسم مبدا فرآیند قراردادن درخواست ها در HTTP انجام شده و در قسمت مقصد عکس این عمل بایستی انجام شود. در این فرآیند از درخواست های POST ای که توسط HTTP ارسال می شود و دریافت پاسخ ها برای ارتباط استفاده می شود. بیشترین کاربرد از HTTP Tunneling در مبحث Video Streaming ، استفاده از RPC برای مدیریت شبکه ، هشدارهای سیستم های تشخیص نفوذ و البته فایروالها می باشد.

نکته: بخش بعدی، تنها با هدفِ ارائه‌ی یک روش، جهتِ دور زدنِ پروتکلِ SSL در گزارش آورده شده.

روش‌های دور زدن مکانیزم‌های امنیتیِ SSL Pinning در اپلیکیشن‌های موبایل

به طور کلی دور زدن مکانیزم امنیتی SSL Pinning توسط مهاجمین به یکی از دو روش زیر قابل انجام است:

1. از طریق جلوگیری از بررسی SSL پین شده و یا دستکاری نتیجه حاصل از این بررسی.
2. از طریق جایگزینی داده های پین شده در اپلیکیشن، به عنوان مثال جایگزینی گواهی موجود در assetها و یا کلید هش شده.

در قسمت های بعدی، هر دو روش با استفاده از یک اپلیکیشن نمونه و همچنین معرفی ابزارهای مربوطه توضیح داده خواهد شد.

آزمون و هدف

در ادامه به توضیح چگونگی دور زدن TrustKit SSL Pinning در نرم افزار نسخه دموی TrustKit که بر روی نسخه ی جیلبریک شده آیفون اجرا می گردد، پرداخته می شود. برای این کار، از ابزارهای زیر استفاده خواهیم کرد:

- از mitmproxyبرای تجزیه و تحلیل داده های ارسالی در شبکه استفاده می شود که ابزارهای جایگزین آن Burp Suiteیا Charlesهستند.
- ابزار Fridaبرای متدها و حملات hooking و patching استفاده می شود. از دیگر فریمورک های محبوب برای hooking میتوان به Cydia Substrate، Cycriptیا Substituteاشاره نمود.
- برای جایگزینی رشته ها در باینری، از ابزار Disassembler Hopperاستفاده خواهیم کرد.

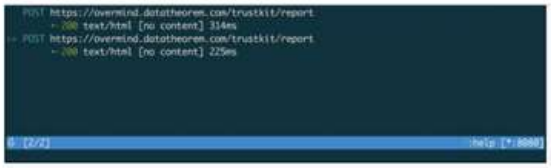
طبیعتا نرم افزار نسخه دموی TrustKit قابلیت کمتری نسبت به نسخه تجاری آن را دارد و تنها قابلیتی که ما از آن استفاده می کنیم، تلاش برای اتصال به https://www.yahoo.com با استفاده از یک هش پین نامعتبر برای آن دامنه می باشد.

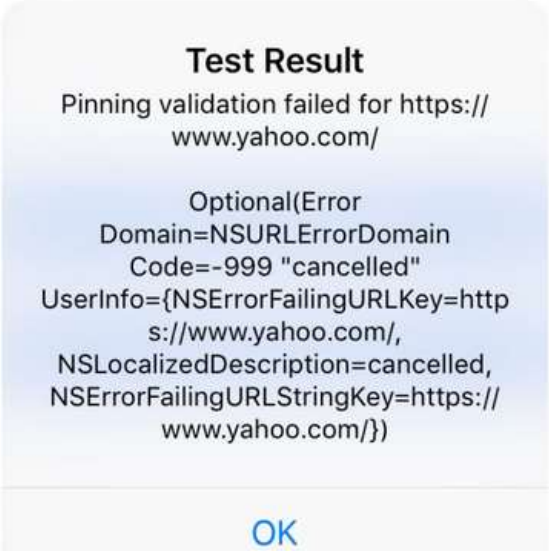
```
let trustKitConfig: [String: Any] = [
          kTSKSwizzleNetworkDelegates: false,
          kTSKPinnedDomains: [
              "yahoo.com": [
                  kTSKEnforcePinning: true,
                  kTSKIncludeSubdomains: true,
                  kTSKPublicKeyAlgorithms: [kTSKAlgorithmRsa2048],

                  // Invalid pins to demonstrate a pinning failure
                  kTSKPublicKeyHashes: [
                      "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA=",
                      "BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB="
                  ],
                  kTSKReportUris:["https://overmind.datatheorem.com/trustkit/report"],
              ],
```

توجه داشته باشید حتی اگر هشهای ارائه شده برای دامنه yahoo.com معتبر باشند، اعتبار سنجی SSL Pinningبایستی رد شود زیرا ما از پراکسی مردمیانی یا Man-in-the-Middle استفاده میکنیم.

هنگام اتصال به دامنهyahoo.com ، ابزار mitmproxy نشان می دهد که دامنه در واقع بازدید نمی شود و فقط گزارش اعتبارسنجی Pinning SSL به سرورهای مورد نظر ارسال می گردد. از سوی دیگر دستگاه خود پیامی با محتوای رد شدن اعتبارسنجی Pinning نمایش می دهد. تمامی این رفتارها با توجه به فعال بودن SSL Pinningکاملا طبیعی و قابل پیش بینی هستند.





متد اول: جلوگیری از بررسی SSLپین شده

در ادامه به بررسی چگونگی دور زدن SSL Pinning با استفاده از ابزار Fridaمی پردازیم. اما پیش از آن بایستی بدانیم که در کدام قسمت از کد، در واقع چک کردن و بررسی SSL Pinning انجام می شود.

پیدا کردن محل بررسی

از آنجا که TrustKit منبع باز است، بنابراین به راحتی می توان دریافت که منطق اعتبار سنجی گواهی واقعی در کجا می افتد .[TSKPinningValidator evaluateTrust:forHostname:]- :در مواردی که سورس کد در دسترس نباشد، با یک بررسی دقیق تر از API کتابخانه Pinning SSL می توان دریافت فعالیت اصلی اعتبار سنجی در کجا اتفاق می افتد.

امضای :evaluateTrust:forHostname حاوی اطلاعات زیادی در خصوص متد مربوطه می باشد.

```
- (TSKTrustDecision) evaluateTrust :( SecTrustRef _Nonnull) serverTrust
forHostname :( NSString * _Nonnull)serverHostname
```

همان طور که مشاهده می شود این متد 2 ورودی شامل نام سروری (Hostname) که قصد اتصال به آن وجود دارد را شامل شده و در نهایت TSKTrustDecision را به عنوان خروجی باز می گرداند. این متغیر از نوع enum می باشد.

```
/**
 Possible return values when verifying a server's identity against a set of pins.
 */
typedef NS_ENUM(NSInteger, TSKTrustEvaluationResult)
{
    TSKTrustEvaluationSuccess,
    TSKTrustEvaluationFailedNoMatchingPin,
    TSKTrustEvaluationFailedInvalidCertificateChain,
    TSKTrustEvaluationErrorInvalidParameters,
    TSKTrustEvaluationFailedUserDefinedTrustAnchor,
    TSKTrustEvaluationErrorCouldNotGenerateSpkiHash,
};
```

همان طور که در سورس کد مشاهده می گردد، هر یک از فیلدهای مربوطه مورد اشاره قرار گرفته است، اما روشن است که مهمترین مقدار در میان آنها، مقدار فیلد TSKTrustEvaluationSuccess می باشد.

دور زدن بررسی SSL

برای دور زدن بررسیTrustKit SSL pinning ، ما متد :[TSKPinningValidator estimateTrust forHostname:]را با استفاده از ابزارFrida ، دستکاری (یا به اصطلاح (hook خواهیم کرد و اطمینان حاصل می کنیم که همیشه مقدار مورد نظر ما را برمی‌گرداند. در ابتدا اسکریپت مورد نیاز ابزار Frida را ایجاد می کنیم و آن را با عنوان disable_trustkit.js ذخیره می کنیم.

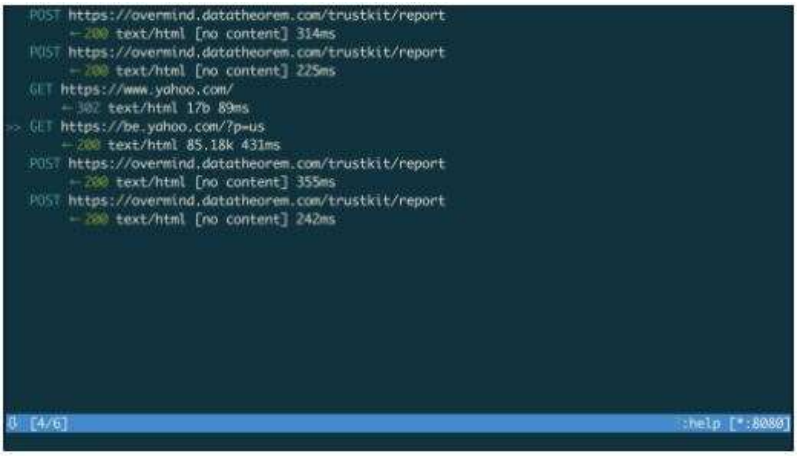
```
var evalTrust = ObjC.classes.TSKPinningValidator["- evaluateTrust:forHostname:"];
Interceptor.attach(evalTrust.implementation, {
    onLeave: function(retval) {
        console.log("Current return value: " + retval);
        retval.replace(0);
        console.log("Return value replaced with (TSKTrustDecision) \
                                TSKTrustDecisionShouldAllowConnection");
    }
});
```

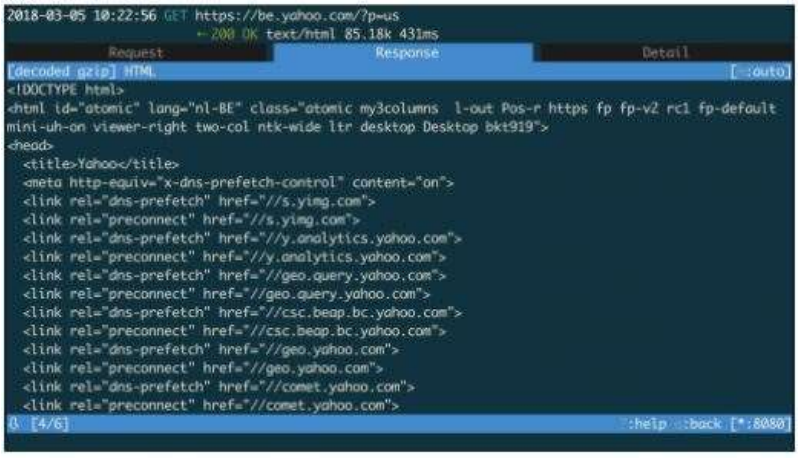
این اسکریپت در واقع Frida را به متد evaluateTrust:forHostname: instance در محیط TSKPinningValidatorمتصل می کند و کد مربوطه را هر بار که این متد باز گردانده می شود، اجرا می کند. این کد، بدون در نظر گرفتن مقدار قبلی و واقعی (TSKTrustEvaluationSuccess) ، آن را با مقدار صفر (0) جایگزین کرده و بر می گرداند.

حال Frida را اجرا نموده و به فرآیند TrustKitDemo موجود در دستگاهمان متصل نموده و اسکریپ را اجرا می نماییم:

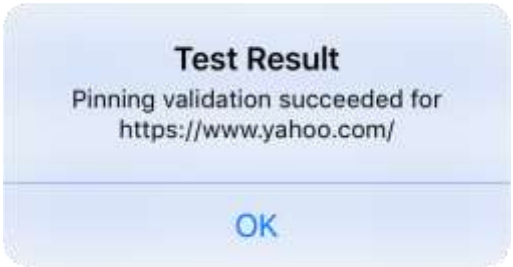
```
frida -U -l disable_trustkit.js -n TrustKitDemo-Swift.
```

اکنون اگر https://www.yahoo.com را لود کنیم، می بینیم که در mitmproxy suite ، این URL با موفقیت بارگذاری شده است.





همچنین مطابق با شکل زیر در موبایل نیز این پیام را مشاهده می کنیم: تأیید پین با موفقیت انجام شده است.



همجنین، Fridaخروجی زیر را برای حصول اطمینان از اینکه فرآیند دستکاری (hook)مطابق با انتظار ما عمل کرده و مقدار مطلوب را برگردانده است، ارائه می دهد.

[iPhone::TrustKitDemo-Swift]->

Current return value: 0x1

Return value replaced with (TSKTrustDecision)

TSKTrustDecisionShouldAllowConnection

Current return value: 0x1

Return value replaced with (TSKTrustDecision)

TSKTrustDecisionShouldAllowConnection

اکنون فرآیند دور زدن Pinning TrustKit SSL با موفقیت انجام شده و تمامی درخواست های وب قابل مشاهده و تغییر می باشند. البته مثال ارائه شده تنها یک نمونه ساده و ابتدایی از دور زدن Pinning SSL تنها با تغییر مقدار بازگشتی متد می باشد .

استفاده از سایر ابزارها

دور زدن SSL Pinning را می توان حتی با استفاده از ترفندهای موجود برای موبایل های جیلبریک شده، از طریق روش های ساده‌تری انجام داد. برای مثال، SSL Kill Switch 2پشته TLS در سیستم عامل iOS را پچ کرده و بدینوسیله کلیه SSLپیاده سازی شده که از آن استفاده می نمایند را غیرفعال می کند. یکی از این ترفندها می باشد. از سوی دیگر ابزار Objection SSL Pinning disablerدرFrida ، بررسی های سطح پایین SSL Kill Switch 2 را اجرا می کند و چند نمونه هوک در اسن فریمورک را ایجاد می نماید.

جدول زیر متدهایی را که می توانند برای بعضی از فریمورک های SSL Pinning ، هوک شوند را تشریح می کند.

libcoretls_cfhelpers.dylib	tls_helper_create_peer_trust
NSURLSession	-[* URLSession:didReceiveChallenge:completionHandler:]
NSURLConnection	-[* connection:willSendRequestForAuthenticationChallenge:]
AFNetworking	-[AFSecurityPolicy setSSLPinningMode:] -[AFSecurityPolicy setAllowInvalidCertificates:] +[AFSecurityPolicy policyWithPinningMode:] +[AFSecurityPolicy policyWithPinningMode:withPinnedCertificates:]

روش مقابله: تشخیص و شناسایی hooking

قبل از تأییدSSL Pin ، می توان به منظور شناسایی حملات هوکینگ، یکپارچگی و عدم دستکاری شدن یا تغییر غیرمجاز توابع فوق را مورد بررسی قرار داد. به عنوان مثال، از SSL Kill Switch 2 که در بالای فریمورک معروف Cydia Substrate جهت انجام حملات هوکینگ در زمان اجرا، ساخته شده است، استفاده خواهیم کرد. هوکینگ در این فریمورک از طریق MSHookFunction API انجام می شود.

روش توضیح داده شده در اینجا تنها یک اثبات مفهومی است و پیشنهاد می شود از کد شناسایی هوک که در این روش توضیح خواهیم داد، در نرم افزارهای تولیدی خود استفاده نکنید. در واقع این یک روش ساده است و تنها نوع خاصی از هوک را در ARM64 تشخیص می دهد. استفاده از این روش بررسی، بدون بهره گیری از مکانیزم های مبهم سازی کد(Obfuscation) ، حذف آن را بسیار آسان خواهد کرد.

یک روش معمول برای هوک کردن توابع اساسی(native) ، جایگزین نمودن چند دستور اولیه آنها با یک ترامپلاین (Trampoline) است. ترامپلاین به مجموعه ای از دستورها گفته می شود که مسئول انتقال جریان کنترل به یک قطعه کد جدید برای جایگزینی یا تقویت رفتار اولیه است. با استفاده ازlldb ، می توانیم دقیقا متوجه شویم "ترامپلاین" چیست و چگونه به نظر می رسد.

10دستور اول تابع اولیه (unhook) به شرح ذیل است:

```
(lldb) dis -n tls_helper_create_peer_trust
libcoretls_cfhelpers.dylib`tls_helper_create_peer_trust:
    0x1a8c13514 <+0>:   stp    x26, x25, [sp, #-0x50]!
    0x1a8c13518 <+4>:   stp    x24, x23, [sp, #0x10]
    0x1a8c1351c <+8>:   stp    x22, x21, [sp, #0x20]
    0x1a8c13520 <+12>:  stp    x20, x19, [sp, #0x30]
    0x1a8c13524 <+16>:  stp    x29, x30, [sp, #0x40]
    0x1a8c13528 <+20>:  add    x29, sp, #0x40            ; =0x40
    0x1a8c1352c <+24>:  sub    sp, sp, #0x20             ; =0x20
    0x1a8c13530 <+28>:  mov    x19, x2
    0x1a8c13534 <+32>:  mov    x24, x1
    0x1a8c13538 <+36>:  mov    x21, x0
```

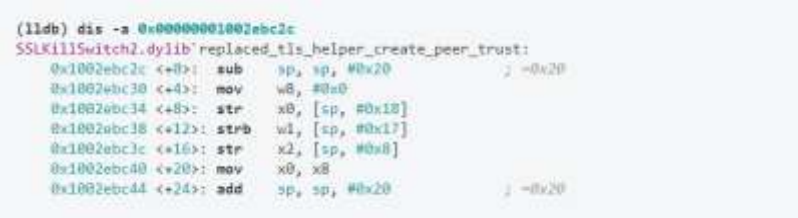
10دستور اول تابع هوک شده به شرح ذیل است:

```
(lldb) dis -n tls_helper_create_peer_trust
libcoretls_cfhelpers.dylib`tls_helper_create_peer_trust:
    0x1a8c13514 <+0>:   ldr    x16, #0x8                 ; <+8>
    0x1a8c13518 <+4>:   br     x16
    0x1a8c1351c <+8>:   .long  0x00267c2c                ; unknown opcode
    0x1a8c13520 <+12>:  .long  0x00000001                ; unknown opcode
    0x1a8c13524 <+16>:  stp    x29, x30, [sp, #0x40]
    0x1a8c13528 <+20>:  add    x29, sp, #0x40            ; =0x40
    0x1a8c1352c <+24>:  sub    sp, sp, #0x20             ; =0x20
    0x1a8c13530 <+28>:  mov    x19, x2
    0x1a8c13534 <+32>:  mov    x24, x1
    0x1a8c13538 <+36>:  mov    x21, x0
```

در تابع هوک شده، 16 بایت اول، ترامپلاین را تشکیل می دهند. آدرس 0x00000001002ebc2cدر رجیستر x16 بارگذاری می شود و سپس به آن آدرس می رود .(BR X16)این آدرس به المان زیر اشاره می کند:

```
SSLKillSwitch2.dylib`replaced_tls_helper_create_peer_trust
```

همان گونه که مشاهده می شود، در آن SSL Kill Switch 2 جایگزین شده است.



اگر پیاده سازی تابع از پیش مشخص شده باشد، چند بایت اول از تابع یافت شده را می توان با بایت های مشخص شده مقایسه کرد. بدین ترتیب می توان بدون نقض Pinning را اجرا نمود. در خصوص Cydia Substrate، مشاهده می شود که تابع با استفاده از یک برنچ غیرشرطی به یک رجیستر (BR Xn) پچ شده است، در این حالت می توانیم وجود این دستور را در چند بایت اول بررسی نماییم. در صورتیکه دستور برنچ یافت شد، فرض بر این است که تابع هوک شده و در غیر اینصورت تابع معتبر است.

روش مقابله: مبهم سازی اسامی(Name Obfuscation)

همان طور که در بالا دیدیم، برای دور زدن مکانیزمSSL Pinning ، نفودگر ابتدا باید بفهمد که کدام مکانیزم را باید هوک کند. با استفاده از یک ابزار مبهم سازی (Obfuscation) متادیتاهای اپلیکیشن های iOS نوشته شده به زبان Swift و یا Objective-C ، برنامه نویسان می توانند این تشخیص را برای نفود گر بسیار دشوار سازند.

مبهم سازی اسامی همچنین قادر است، مانع از عملکرد صحیح تمامی ابزارهای خودکار برای جستجوی نام متدهای شناخته شده شود. یک ابزار مبهم ساز می تواند متدها را به شیوه ای متفاوت در ساختار هر یک از نسخه های اپلیکیشن تغییر دهد، به گونه ای که نفوذگر را مجبور به جستجوی نام واقعی متدها در هر نسخه جدید گرداند.

توجه داشته باشید که مبهم سازی اسامی فقط قادر است از برنامه در مقابل ابزارهای دور زدن SSL که در آنها، گواهی SSL در کد برنامه یا کتابخانه های برنامه جاگذاری شده است، محافظت نماید. ابزارهایی که با فریم ورک های هوکینگ سیستم کار می کنند، با این روش قابل جلوگیری نمی باشند.

متد دوم: جایگزینی داده های SSL Pinning

راه دیگر برای دور زدن SSL Pinning این است که داده های پین شده را در داخل برنامه جایگزین نماییم. اگر ما قادر به جایگزینی فایل گواهی پین شده اصلی یا رشته کلید عمومی با گواهی یا کلید موجود در سرور مردمیانی (Man-in-the-Middle)خودمان باشیم، قاعدتا میتوانیم سرور خودمان را به جای سرور اصلی پین کنیم.

جایگزینی یک فایل گواهی جاسازی شده می تواند به آسانی جایگزینی یک فایل در پکیج IPA باشد.

در اپلیکیشن هایی که هش کلید عمومی سرور را پین می کنند، می توانیم رشته را با هش کلید عمومی سرور خودمان جایگزین کنیم. تصویر زیر نشان می دهد که چگونه برنامه Demo TrustKit در ابزار Hopper بارگذاری شده است Hopper .به مهاجم اجازه می دهد که رشته ها را در فایل MachO جایگزین نموده و آن را مجددا به شکل یک فایل قابل اجرا و معتبر تبدیل نماید.

هنگامی که فایل یا رشته جایگزین می شود، دایرکتوری تحت عملیات باید مجددا به صورت یک IPA امضا و زیپ شود.

روش مقابله: مبهم سازی رشته ها(String Obfuscation)

هنگام پین کردن گواهینامه ها با یک لیست از هش های کلید عمومی hard-code شده، بهتر است که مقادیر و ارزش ها را رمزگذاری کنید. این عمل در واقع اپلیکیشن شما را در برابر حملات hooking محافظت نخواهد کرد، اما نفوذگر را برای جایگزینی هش های اصلی با گواهی ساختگی از سوی او، با مشکل جدی رو به رو می سازد. مبهم سازی و رمزگذاری رشته ها (مقادیر) در این بخش قابل استفاده می باشد. ابزارهای DexGuard برای اپلیکیشن های اندرویدی و همچنین iXGuard برای برنامه های iOS می توانند مبهم سازی رشته های (حساس) مدنظر برنامه نویس را انجام دهند.

روش مقابله: مبهم سازی جریان کنترل(Control Flow Obfuscation)

یک مهاجم با استفاده از تکنیک های مهندس معکوس قادر است جریان و روند کنترل برنامه را تجزیه و تحلیل نموده تا بتواند از این طریق محل دقیقی که در آن، برنامه هش واقعی را تایید می کند، پیدا نماید. اگر او موفق به پیدا کردن این محل گردد، می تواند ببیند که کدام رشته مورد استفاده قرار گرفته و همچنین می تواند محل رشته هش در باینری را پیدا کند. مبهم سازی جریان کنترل برنامه توسط برنامه نویس، باعث می شود تا تجزیه و تحلیل دستی از کد برای نفوذگر بسیار مشکل گردد. ابزارهای DexGuard و همچنین iXGuard می توانند مبهم سازی جریان کنترلی نرم افزار را انجام دهند.

پایان.