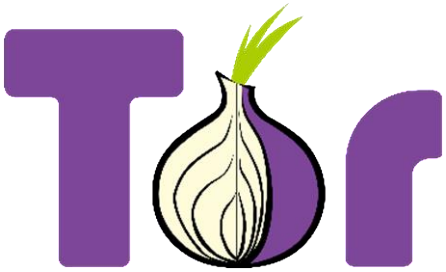
1393



Tor

تور چطور کار میکند؟

محمد باقر رستمی

فهرست

تور

تور یک نرم افزار آزاد و رایگان است که به شما کمک میکند تا حضور شما در اینترنت پنهان شود. بنابراین یافتن موقعیت و فعالیت های شما در اینترنت پنهان خواهد ماند. تور از یک مدار مجازی و یا مجموعه ای از سیستم های داوطلب متصل به هم برای عبور اطلاعات و ترافیک اینترنت استفاده میکند. گاهی به اشتباه گفته می شود که تور سبب افزایش امنیت اطلاعات می شود اما در واقع اینچنین نیست. تور از روشی به نام مسیریابی پیازی برای ایجاد مدار استفاده می کند.

مسیریابی پیازی

مسیریابی پیازی روشی است برای پنهان کردن ارتباطات در شبکه و اینترنت که در این تکنولوژی اطلاعات در لایه های مختلفی رمز نگاری می شود و اطلاعات رمز نگاری شده از طریق تعدادی از سیستم های موجود در شبکه که با نام (Onion Router) شناخته می شوند به مقصد منتقل می شوند. هر سیستمی که از تور استفاده میکند می تواند خود را به عنوان Onion Router یا OR در شبکه تعریف نماید تا شبکه تور بتواند از آن سیستم به عنوان یک روتر پیازی استفاده کند. این کار در تنظیمات تور با عنوان relay قابل فعال سازی است. به آغاز کننده این ارتباط Onion Proxy یا OP می گویند که در واقع همان مبدا ارتباط است.

D-H

قبل از هر چیز بهتر است نگاهی به Diffie–Hellman key exchange یا D-H که در تور استفاده میشود بیندازیم.

این روش برای ایجاد یک کلید رمز مشترک امن (Shared Secret) بین دو سیستم استفاده می شود به نحوی که هیچ فرد دیگری در بین راه امکان تشخیص کلید مشترک را نداشته باشد حتی اگر شبکه نا امن باشد. البته باید در نظر گرفت که اگر تبادل اطلاعات بدون رمزنگاری انجام شود امکان حمله از نوع MITM یا Man In The Middle وجود دارد بنابراین همواره بهترین راه برای استفاده از این روش رمزنگاری تبادل کلید با استفاده از رمزنگاری نامتقارن است. گرچه این روش از انواع رمزنگاری های متقارن محسوب می شود اما بدون درگیر شدن رمزنگاری نا متقارن امنیت در این روش نیز کاهش خواهد یافت.

به طور خلاصه اطلاعاتی از این تکنولوژی را در تصویر زیر مشاهده میکنید:

Alice	
knows	doesn't know
$p = 23$	$b = ?$
base $g = 5$	
$a = 6$	
$A = 5^a \bmod 23$	
$A = 5^6 \bmod 23 = 8$	
$B = 19$	
$s = B^a \bmod 23$	
$s = 19^6 \bmod 23 = 2$	
$s = 2$	

Bob	
knows	doesn't know
$p = 23$	$a = ?$
base $g = 5$	
$b = 15$	
$B = 5^b \bmod 23$	
$B = 5^{15} \bmod 23 = 19$	
$A = 8$	
$s = A^b \bmod 23$	
$s = 8^{15} \bmod 23 = 2$	
$s = 2$	

Eve	
knows	doesn't know
$p = 23$	$a = ?$
base $g = 5$	$b = ?$
	$s = ?$
$A = 8$	
$B = 19$	
$s = 19^a \bmod 23 = 8^b \bmod 23$	

Image reference : http://en.wikipedia.org/wiki/Diffie–Hellman_key_exchange

در تصویر فوق Alice و Bob می خواهند ارتباط برقرار کنند. هر دو نفر از مقدار p اطلاع دارند و حتی ممکن است نفر سومی مانند Eve نیز از مقدار p اطلاع داشته باشد. Alice و Bob یک رمز اختصاصی برای خود در نظر میگیرند که هیچ کس از آن اطلاعی ندارد. برای Alice عدد a و برای Bob عدد b. سپس بر اساس محاسباتی که بر روی عدد p انجام میدهند به عددی مانند A برای Alice و B برای Bob می رسند. سپس A و B را برای همدیگر ارسال میکنند. ارسال اطلاعات ممکن است در شبکه نا امن باشد لذا Eve هم از هر دو مقدار مطلع می شود. سپس هر دوطرف بر اساس A و B (که هر دو میدانند) و مقادیر a و b (که فقط مختص خودشان است) محاسبه ای انجام داده و به یک عدد یکسان مانند s می رسند. Eve از این عدد هیچ اطلاعی ندارد و حتی بر اساس اطلاعاتی که در اختیار دارد نمی تواند عدد s را تشخیص دهد. اگر Eve را یک هکر در نظر بگیریم با اطلاعاتی که این هکر می تواند بین ارتباط دو نفر دیگر به دست بیاورد امکان تشخیص کلید رمز مشترک وجود ندارد و فقط Bob و Alice هستند که از کلید رمز مشترک یکسان(s)اطلاع دارند.(Shared Secret).

این روش برای رمزنگاری های متقارن استفاده میشود تا هر دو طرف با یک کلید مشترک امکان رمزنگاری و رمزگشایی اطلاعات را داشته باشند.

نحوه کار تور

طبق تصویر یک نمونه از اتصال تور را در نظر میگیریم و مرحله به مرحله پیش می رویم :

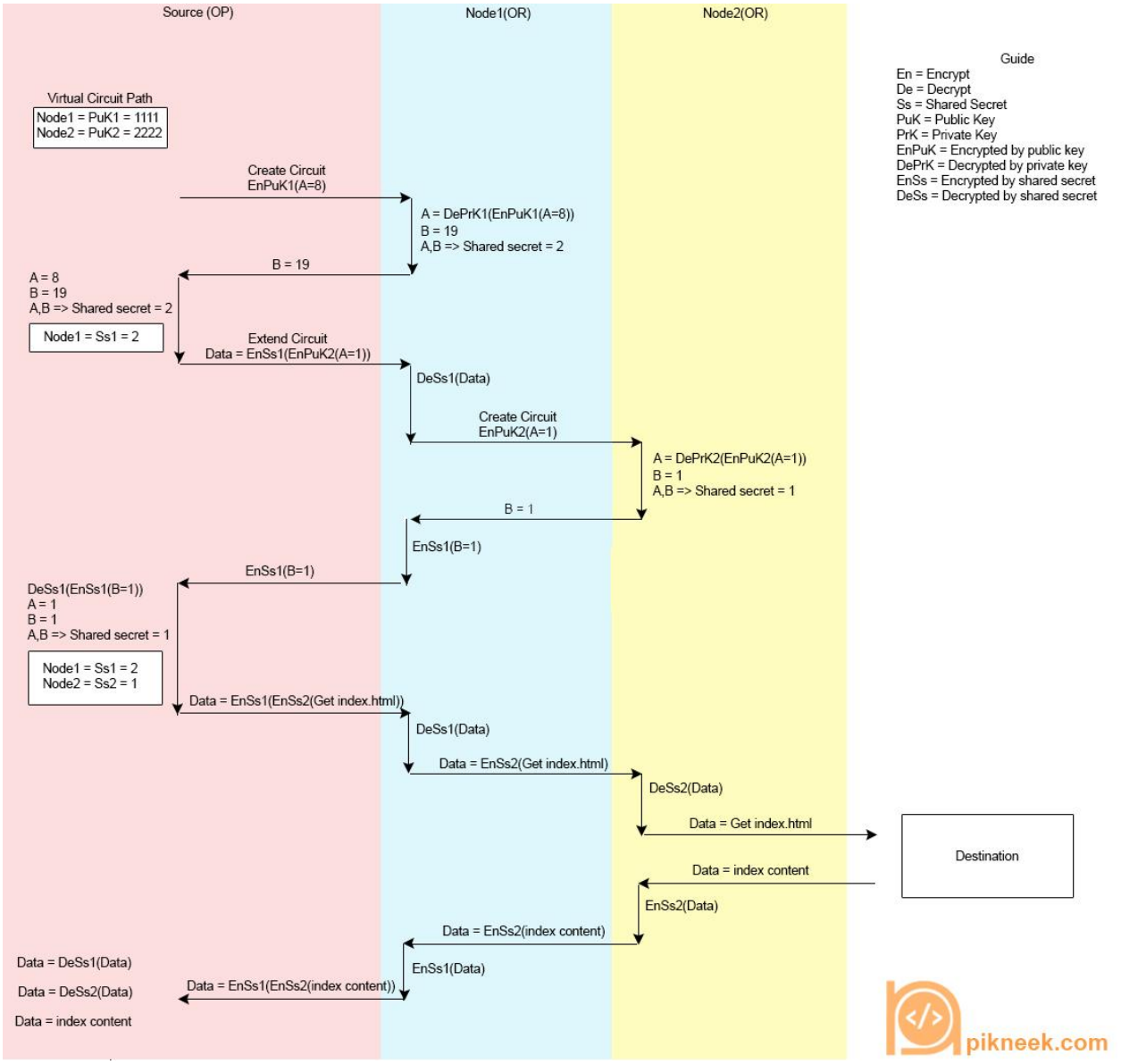


Image reference : http://pikneek.com

۱ - بعد از نصب تور و اتصال به شبکه تور لیستی از سیستم هایی که در شبکه تور به عنوان روتر (OR)کار میکنند مشخص می شود(کلید های عمومی هر سیستم در این لیست مشخص شده است) و تور بر اساس این لیست تعدادی از سیستم ها را برای ایجاد یک مدار مجازی انتخاب می کند. طبق روش D-H مبدا (OP) بعد از محاسبات, کلید A خود (مثلا 8) را به وسیله ی کلید عمومی Node1 رمزنگاری کرده و برای Node1 ارسال می کند.(علاوه براین دستور ایجاد یک مدار را نیز ارسال میکند) وقتی حرف از کلید عمومی Node1 می شود باید به این نکته توجه کنیم که تنها کسی که می تواند

اطلاعات رمز شده را رمزگشایی نماید Node1 است و نه حتی ارسال کننده اطلاعات. هر کدام از نود ها(سیستم ها) ممکن است در هر کجای جهان و با آی پی های مختلف باشند.

۲ - اطلاعات به وسیله ی Node1 و کلید خصوصی Node1 رمزگشایی می شود. و Node1 حالا می داند که A = 8. زمانی که A و B در هر سیستم مشخص شد سیستم میتواند کلید رمز مشترک را تولید نماید.

حال Node1 می داند که کلید رمز مشترک بین مبدا (OP)و Node1 برابر ۲ است.

۳ - کلید B توسط Node1 برای OP به صورت متن خام ارسال می شود. (قرار نیست کسی از کلید عمومی OP اطلاع داشته باشد لذا امکان رمزنگاری وجود ندارد. هدف تور این است که OP به صورت ناشناس باقی بماند). باید دقت داشت که بدون داشتن A یا B نمی توان رمز مشترک را تولید کرد و چون A به صورت رمز شده ارسال شده است لذا میتوان گفت امنیت در این مرحله برقرار شده است.

۴ - حال OP هم A و هم B را دارد لذا میتواند با محاسبات خود رمز مشترک را تشخیص دهد.(در این مثال 2). این رمز مشترک برای Node1 در OP برای استفاده های بعدی ذخیره می شود.(برای رمزنگاری و رمزگشایی)

۵ - مبدا (OP)حال می خواهد مدار را گسترش داده و به Node2 برساند. لذا مجددا محاسبات D-H مجددا انجام میشود. کلید A جدید تولید شده بایستی به Node2 برسد. لذا این کلید را با استفاده از کلید عمومی Node2 رمزنگاری می نماید و آنرا در بسته اطلاعاتی ارسالی به Node1 قرار می دهد و تمام این بسته اطلاعاتی را با استفاده از کلید رمز مشترک بین OP و Node1 رمزنگاری کرده و ارسال می نماید. در این بسته مشخص می شود که Node1 بعد از گرفتن بسته, اطلاعات رمز شده را برای گسترش به کجا ارسال نماید .(Node2)دقت داشته باشید که بعد از توافق OP و Node1 بر روی رمز مشترک تمام اطلاعات ارسالی بین این دو, با همین کلید رمز مشترک رمزنگاری و رمزگشایی خواهد شد. در رابطه با دیگر نود ها نیز همین موضوع وجود دارد.

۵ - اطلاعات توسط Node1 تا یک لایه(اولین لایه رمزنگاری شده) به وسیله رمز مشترک رمزگشایی می شود و اطلاعات نود بعدی مشخص میشود.

۶ - حال Node1 اطلاعات رمزشده ای که از OP دریافت کرده بود را به همان نحو به Node2 ارسال مینماید. (اطلاعاتی که Node1 پردازش کرده بود از بسته حذف می شود).

۷ - حال مرحله ۱ و ۲ و ۳ این بار بین Node1 و Node2 مجددا انجام می شود و در نهایت مقدار B که از Node2 دریافت شده توسط Node1 و با استفاده از کلید رمز مشترک(بین Node1 و OP) رمزنگاری شده و به OP ارسال می شود.

۸ - اطلاعات توسط رمز مشترک Node1 در OP رمزگشایی می شود. با استفاده از مقدار B به دست آمده حال OP و Node2 نیز یک کلید رمز مشترک جداگانه دارند که Node1 از آن هیچ اطلاعی ندارد. پس یک ارتباط امن بین OP و Node2 برقرار شد.

۹ - این گسترش می تواند تا چندین نود مختلف ادامه داشته باشد اما باید در نظر گرفت که تعداد نود ها هرچه قدر بیشتر باشد کارایی و سرعت کاهش می یابد.

۱۰ - حال که مدار تکمیل شد OP, می تواند درخواست خود را از طریق نود ها به مقصد ارسال نماید. بعد از تکمیل مدار ایجاد شده تمام رمزنگاری ها و رمزگشایی ها فقط با استفاده از کلید های رمز مشترک ایجاد شده انجام میشود. بنابراین درخواست خود را به تعداد نود های موجود رمزنگاری می نماید. یعنی بر روی یک بسته اطلاعات به تعداد نودهای موجود در مدار لایه های رمزنگاری ایجاد می شود که هر لایه فقط و فقط توسط نود مربوط به خود قابل رمزگشایی است. بر همین اساس است که به این نوع مسیریابی, مسیریابی پیازی گفته میشود. چرا که رمزنگاری مانند لایه های یک پیاز دور هسته یا همان اطلاعات خام قرار میگیرد.

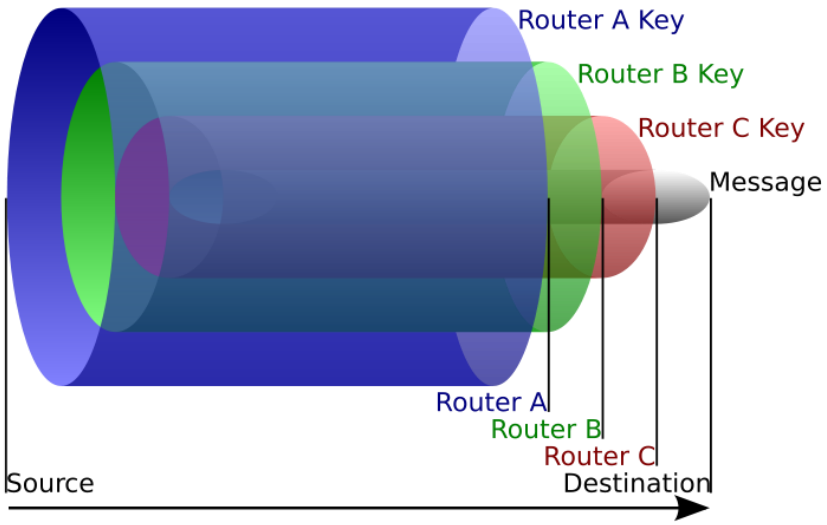


Image reference : http://en.wikipedia.org/wiki/Onion_routing

۱۱ - درخواست به نود بعدی ارسال می شود و سپس نود بعدی و ... تا به آخرین نود در مدار می رسیم که با رمزگشایی شدن آخرین لایه اطلاعات خام به دست می آید. به این نود که در آخرین مرحله مدار قرار گرفته است Exit Node یا نود خروجی گفته میشود. دلیل اینکه تور باعث افزایش امنیت اطلاعات نمی شود همین Exit Node است. چرا که این امکان وجود دارد که نود خروجی اطلاعات را به صورت متن خام مشاهده نماید. این اطلاعات میتواند شامل کلمه عبور ها و ترافیک های نا امن اینترنت باشد که از OP شروع شده است. در نظر داشته باشیم که اکثر پروکسی های دیگر به غیر از

شبکه تور نیز این نقطه ضعف را دارند, لذا می توان گفت که با استفاده از پروکسی های ناشناس کلمات عبور و ترافیک مهم و حیاتی خود را در بستر نا امن اینترنت نباید انتقال داد.

۱۲ - اطلاعات خام به وسیله ی Exit Node به مقصد ارسال می شود و مقصد بر اساس آن پاسخی را به Exit Node ارسال می نماید .

۱۳ - مجددا مراحل رمزنگاری آغاز می شود و اولین لایه رمزنگاری این بار توسط Exit Node به وسیله کلید رمز مشترک بین Exit Node و OP رمزنگاری می شود. مجددا باید در نظر داشته باشیم که نود ها به هیچ وجه از مسیر مدار آگاهی کامل ندارند و فقط و فقط از نود بعدی و قبلی خود اطلاع دارند.

۱۴ - نود بعدی نیز اطلاعات دریافتی از نود قبلی را رمزنگاری می نماید و به نود بعدی ارسال می نماید. (این نود ممکن است OP و یا یک نود دیگر در مدار باشد).

۱۵ - در نهایت اطلاعات به OP می رسد و تنها OP است که بر اساس کلید های رمز مشترک ذخیره شده لایه به لایه اطلاعات را رمزگشایی می نماید و به پاسخ مقصد می رسد.

این پروسه در طول زمان اتصال برقرار است و از بین نمی رود. در مسیریابی پیازی برای هر بار درخواست، این اتصال مجددا بایستی برقرار شود وتمام مراحل قبل مجددا بایستی تکرار شود اما در تور که از مسیر یابی پیازی استفاده میکند این امکان نیز وجود دارد که بدون از بین رفتن اتصال قبلی امکان برقراری ارتباط وجود داشته باشد تا سرعت و کارایی شبکه افزایش پیدا کند .

در تمام این مراحل هر نود فقط از نود قبلی و بعدی خود اطلاع دارد و امکان تشخیص اینکه ارتباط از کجا آغاز شده است وجود ندارد. همینطور ارتباط بین تک تک نود ها با پروتکل TLS امن شده است. هر کدام از OR ها به عنوان یک سرویس دهنده SOCKS فعالیت می کنند تا ارتباط همواره امن باشد.

سرویس های مخفی

در تور امکانی به عنوان سرویس های مخفی وجود دارد که میتوان یک سرویس دهنده را به عنوان یکی از اعضای تور در نظر گرفت و با این امکان اتصال به صورت نقطه به نقطه رمزنگاری شده و امنیت از مبدا تا مقصد برقرار می شود. در این نوع از سرویس ها Exit Node وجود ندارد و آخرین نود یک مدار همان سریس دهنده است. برای اتصال به این سرویس های مخفی داشتن تور الزامی است و همچنین بایستی از آدرس سرویس دهنده اطلاع داشته باشیم. معمولا آدرس یک سرویس مخفی به صورت آدرس اینترنتی + onion. شناخته می شود. به طور مثال یک سرویس مخفی میتواند آدرسی مانند زیر داشته باشد :

```
http://duskgytldkxiuqc6.onion
```

البته این آدرس یک نام دامنه نیست و فقط مختص تور است.

کجا از تور استفاده نکنیم؟

همانطور که گفته شد مشکل اصلی تور وجود Exit Node است که می تواند اطلاعات خام را بررسی نماید لذا هرگز نباید از تور برای انتقال اطلاعات مهم و حیاتی خود استفاده کرد مگر در شرایطی که یک لایه رمزنگاری دیگر مانند SSL نیز بین مبدا و مقصد وجود داشته باشد. اما در این خصوص نیز نمی توان گفت ارتباط به طور حتم امن شده است. فقط در نظر داشته باشید که تور یک ابزار است برای ناشناس ماندن شما. بعد از اطلاعاتی که ادوارد اسنودن در رابطه با شنود ارتباطات اینترنتی منتشر کرد درصد استفاده مردم از تور بسیار بالا رفت اما بیشتر مردم نمی دانند که تور مانند هر پروکسی دیگری سبب افزایش امنیت نمیشود و حتی در شرایطی باعث کاهش امنیت نیز می شود. تنها دلیل استفاده از تور ناشناس ماندن است. استفاده از پروکسی باعث نمی شود که اطلاعات شما مخفی بماند اما تور برای حل این مشکل ایجاد شد.

منابع

http://en.wikipedia.org/wiki/Onion_routing

http://www.onion-router.net

http://www.onion-router.net Tor Design

http://groups.csail.mit.edu

http://www.lsa.umich.edu TOR Routing Infomation

https://tor2web.org

نویسنده

محمد باقر رستمی

mb.rostami.h@gmail.com

http://pikneek.com