TOR (The Onion Router) - systém pro vysoce anonymní a šifrovaný přístup k Internetu

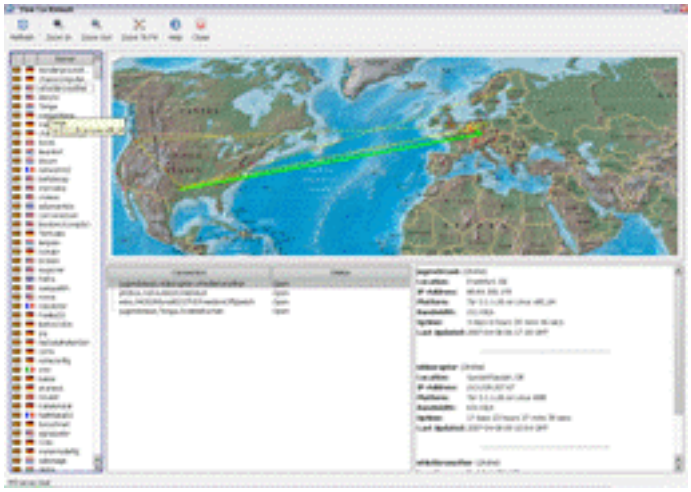
Vložil/a cm3l1k1 [1], 18 Duben, 2007 - 22:26

- Anonymita [2]
- Recenze [3]
- Security [4]

TOR (The Onion Router) je systém umožňující na Internetu skrýt vaši identitu a vámi přenášená data. Data jsou zasílaná přímo od vás šifrovaně k prvnímu onion routeru v řetězci (který ustavuje Tor) a veškerá další komunikace mezi routery, které si předávají payload a řídící informace, je taktéž šifrována (každé spojení jiným sdíleným klíčem). Navíc každý router má informaci jen o tom, od koho data přijal a kam je má přeposlat. Obsah dat nebo jejich zdroj nelze vysledovat.

URL souvisejícího projektu: http://tor.security-portal.cz/ [5] (Czech & Slovak TOR Community)

Tor je síť virtuálních nodů (onion routerů), které mezi sebou sdílejí veřejné šifrovací klíče všech nodů v síti a asymetrickým šifrováním si vyměňují dynamicky generované sdílené klíče pro jeden konkrétní řetězec ustavený klientem (např. vámi, když se připojíte do sítě).



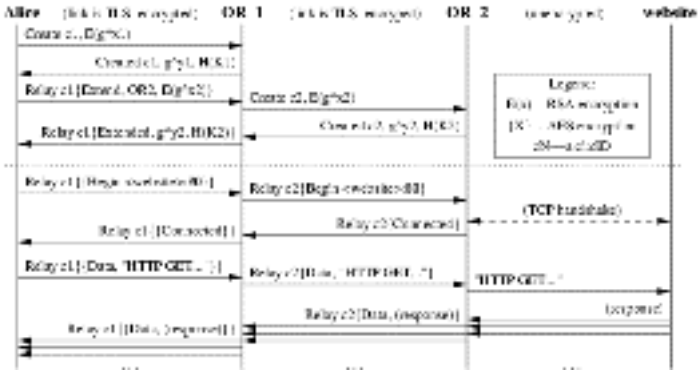
[6]

Cílem těchto onion routerů je šifrovat/dešifrovat data a přeposílat je dalším onion routerům v řetězci. Pokud jsou v řetězci posledním bodem (gateway), vyšlou požadavek do Internetu (např. zobrazení webové stránky). Vrácená data odchytí, zašifrují a pošlou zpět onion routeru, od kterého data s požadavkem dostali apod., až se dostanou ke klientovi, který požadavek vyslal.

Řetězec (circuit) ustavuje klient, aby si mohl vybrat přes kolik a přes jaké onion routery bude požadavek směrován, čímž je pak složitější odchytit data či zjistit identitu klienta. Každý onion router může přeposílaná data předávat se zpožděním nebo v jiném pořadí, než je přijal, což situaci „odposlechu/analýzy“ komplikuje ještě mnohem více. Konkrétně Tor je však nízkolatencový, takže tyto techniky nepoužívá, ale i tak je reálná možnost analýzy dat v praxi velice složitá. Veškerá komunikace (router-router, klient-router) je šifrovaná díky TLS.

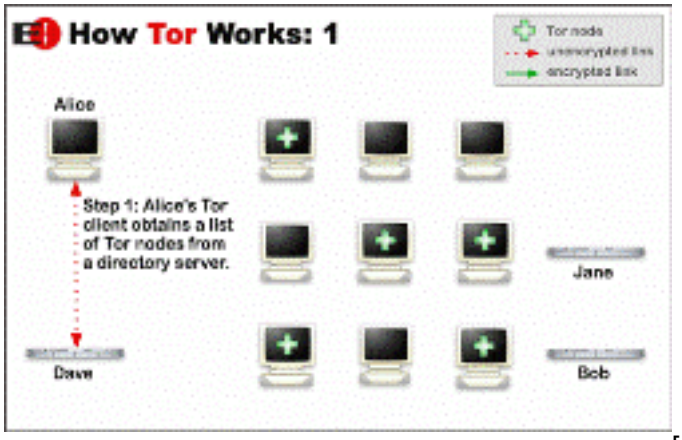
Řetězec se po několika minutách (nebo po určitém objemu dat) rozpadne a utvoří se nový (přes jiné routery). Vytváří se nezávisle (na pozadí) a lze ho během komunikace různě prodlužovat, měnit a

posílá se jím i „šum, dummy traffic“ paketů (to vše také značně ztěžuje odposlech/analýzu dat).

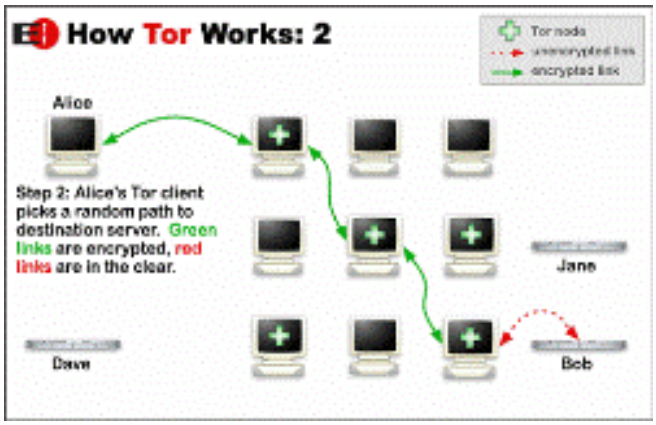


[7]

Routery, které v řetězci sousedí mezi sebou, vygenerují unikátní šifrovaný kanál (cell, rychlým symetrickým šifrováním – AES 128 v counter módu, tzn. bloková šifra se používá jako proudová), kterým pak posílají sousednímu routeru data při posílání dat tímto konkrétním řetězcem (cell ID). Tím jsem chtěl říct, že těmito kanály se posílají jen data proudící řetězcem ustaveným klientem. Onion router může obsluhovat stovky řetězců, ale pro každý má jiné vygenerované šifrovací klíče.



[8]

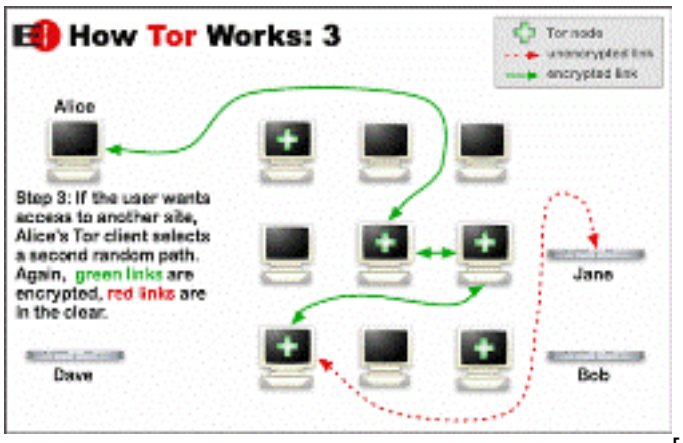


[9]

Posílání zpráv v důsledku vypadá tak, že payload (data) je několikrát zašifrován veřejnými klíči routerů, přes které bude požadavek směrován, a to směrem od posledního (gateway) k prvnímu (router C -> router B -> router A) klientem předem ustaveným řetězcem. Ke každé zašifrované zprávě je přidán digitální podpis, aby se data nedala zfalšovat. Data, která chcete vyslat do Internetu, se tedy nejdříve zašifrují veřejným klíčem posledního onion routeru v řetězci (gateway, C), dále pak veřejným klíčem B routeru i s informací (hlavičkou), která mu řekne, že má data poslat

routeru C. Toto vše se zašifruje veřejným klíčem routeru A s hlavičkou, že má data poslat routeru B. Tento balík se pak pošle zašifrovaný klíčem routeru A šifrovaným kanálem.

Data = sifra_A(hlavicka+sifra_B(hlavicka+sifra_C(payload)))



[10]

Putování dat od klienta vypadá tedy tak, že router A zprávu převezme, dešifruje a má data + hlavičku, ať to pošle routeru B, pošle tedy data také jedinečným šifrovaným kanálem. Router B zprávu také dešifruje, z hlavičky si přečte, že má data směrovat na router C, což udělá. Router C finálně dešifruje zprávu a zjistí, že jde o požadavek do Internetu a ten provede. Vrácená data odchytne a pošle zpět. Ale jak? :)

Nemůže přeci vrácená data zašifrovat veřejným klíčem klienta, protože by tím pádem (přibližně) věděl, kdo data požadoval. Odpověď na tuto otázku jsem našel (thx to tao) až v dokumentu Tor Design [11], podrobně popisujícím fungování systému Tor (něco jako technická specifikace). Router C zprávu zašifruje svým privátním klíčem, takže ji lze dešifrovat jeho veřejným klíčem, který zná každý (simply cool) a data následně také zašifruje veřejnými klíči všech routerů v řetězci. Klient data příjme, dešifruje veřejným klíčem routeru C a má výsledná data.

Co z toho dále plyne?

Router C vidí vaše požadavky i odpovědi na ně, takže si také dávejte pozor na vyplňování soukromých údajů na stránkách nebo na přístup pod heslem a používejte HTTPS (SSL atd.). Na druhou stranu nikdy nezjistí, komu jsou určena a žádný z dalších routerů nikdy nebude znát obsah dat. Router A by mohl zjistit, že je prvním routerem v řetězci, když porovná seznam známých serverů s klientskou IP, ale tohle se běžně neděje a klient se k němu chová jako kterýkoliv jiný onion router (i když jím není), takže router A neví, jestli data předává dál nebo rovnou klientovi. Co je obsahem dat nezjistí nikdy.

Toto je jen zjednodušený popis vytváření tunelu, šifrování a přenosu dat. Kdyby někoho zajímalo více podrobností, nasměruji ho na dokument Tor Design [11].

Pěkně řešené, co říkáte? :)
Z pohledu aplikací vypadá Tor jako SOCKS proxy, kterou mohou použít ke směrování jakýchkoliv TCP spojení.

Hidden services

V systému TOR je možné použít i tzv. hidden services. Představte si to jako intranet sítě Tor. Můžete takto publikovat web server, SSH server, chat server atd., který je přístupný jen klientům sítě Tor. Tyto servery jsou dostupné přes jejich FQDN (neco.onion) a top level doména je .onion.

Příkladem může být např. hidden wiki, která je přístupná jen klientům sítě Tor pod adresou http://6sxoyfb3h2nvok2d.onion/ [12]

[13]

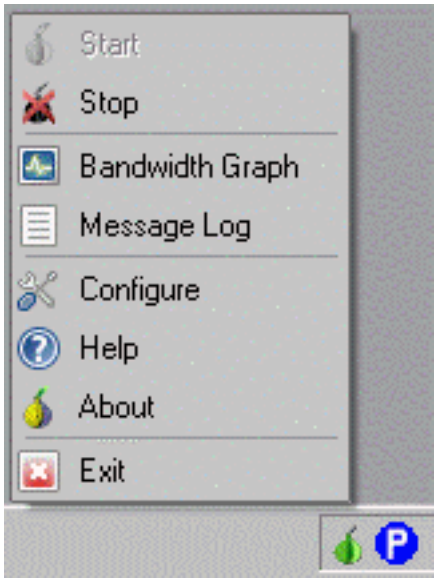
Nejedná se o ekvivalent DNS, ale všechny hidden services jsou uvedeny v souboru na webu, odkud si ho klient stáhne, když chce k některé přistupovat.

Přístup k hidden services vypadá tak, že server, který publikuje některou ze služeb, vytvoří několik tunelů přes onion routery (introduction points), které vedou k jeho službě. Tyto introduction pointy spolu s veřejným klíčem publikuje na Internetu. Veřejný klíč se musí lišit od klíče, který používá na serveru, aby nebylo možné vysledovat jeho IP adresu.

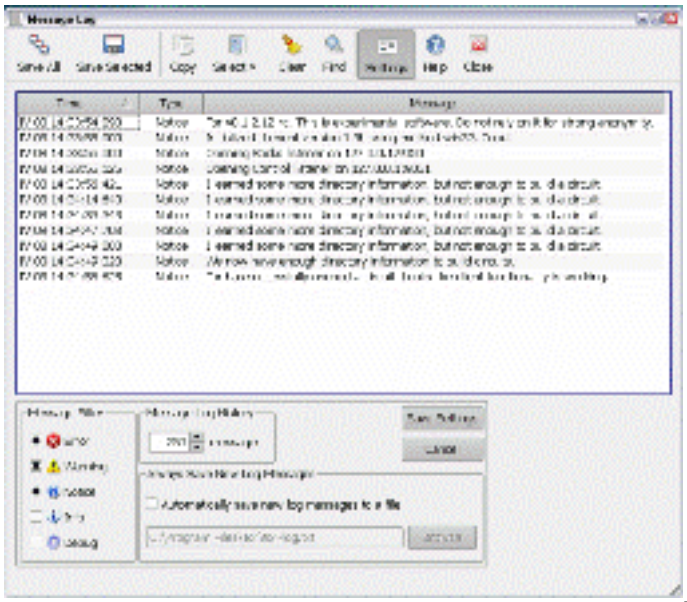
Zájemce si stáhne veřejný klíč publikované služby, vytvoří řetězec a poslední router v řetězci zastupuje funkci zvanou randevous point (místo setkání/schůzky), kontaktuje jeden z introduction pointů, vygeneruje randevous cookie (náhodné číslo) a zašle informaci o umístění randevous pointu. Tato komunikace je zašifrovaná veřejným klíčem služby, během které se zájemce a protistrana domluví na session keyi. Služba se pak už jen připojí na randevous point, kde mu předá totožné randevous cookie a spojení je navázané. Zájemce ani server o vzájemné totožnosti nic nezjistí a veškerá jejich komunikace probíhá šifrovaně.

Instalace a používání

Celý balík, který v sobě zahrnuje Tor (samotný klient), Vidalia (grafické rozhraní pro Tor), Privoxy (web proxy server) a Torbutton (rozšíření do Firefoxu pro jednoduché přepínání mezi používáním běžné a Tor sítě), lze stáhnout ze stránek http://tor.eff.org/download.html.en [14]
Instalace je naprosto jednoduchá (next, next, next) a poté se vám již Tor (resp. Vidalia) a Privoxy bude spouštět po startu a umístí si ikonky do traye, odkud můžete měnit jejich nastavení a zkoumat jejich aktivitu.

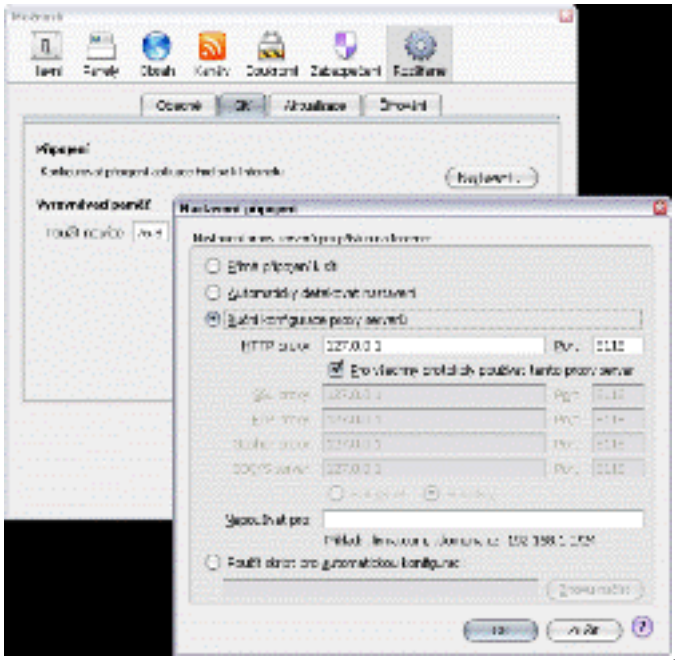


[15]



[16]

Privoxy slouží jako web proxy server, takže pokud chcete prohlížet webové stránky přes síť Tor, stačí jen nastavit **proxy** na localhost a **port 8118**.



[17]

Samotný Tor jako **SOCKS proxy běží na portu 9050**, takže ostatní aplikace, které mají přes Tor komunikovat, stačí jen nastavit tak, aby požadavky posílaly na tento port.

Tipy pro zvýšení anonymity a bezpečnosti

Komunikace sítí Tor je tedy bezpečná a anonymní. Problém je však s aplikacemi, které budou Tor využívat. Především pak u prohlížečů internetových stránek je nutné vypnout některé pluginy a rozšíření pro zvýšení bezpečnosti. Hlavním rozhraním, které o vás dokáže zjistit obrovské množství informací včetně pravé IP adresy, je JavaScript. Podívejte se na obrázek z anonymity checkeru [18], který máme na SP.

[19]

I když jsem na něj přistupoval ze sítě Tor, bylo možně zjistit schopnosti prohlížeče (zapnutý JavaScript, Java, Flash, Adobe plugin, rozlišení obrazovky atd.). Doporučuje se proto věci jako podporu JavaScriptu, Flashe, Javy, ActiveX, RealPlayeru, QuickTime, Adobe's PDF plugin vypnout nebo omezit pomocí Firefox rozšíření:
-> QuickJava [20]
-> FlashBlock [21]
-> NoScript [22]

Tyto funkce mějte zapnuté jen na důvěryhodných stránkách nebo používejte dva prohlížeče. Jeden

pro přístup ze sítě Tor a druhý pro běžné (nesoukromé, nedůležité) surfování (ono třeba lézt na youtube.com přes Tor není to pravé ořechové).

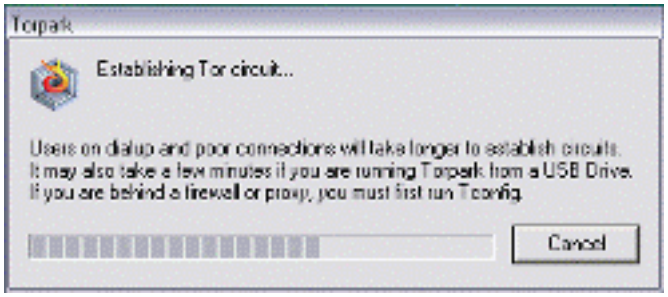
Některé škodlivé HTTP hlavičky a funkce blokuje přímo Privoxy podle definovaných pravidel (mrkněte do privoxy souboru default.filter), ale neochrání nás od všeho.

Další možnou hrozbou je DNS. Když přistupujete na nějaký web apod., nejdříve se jeho název musí přeložit na odpovídající IP adresu. To se provádí tak, že se dotážete svého DNS serveru a ten vám vrátí odpověď. Kdyby někdo odposlouchával vaši komunikaci, tak může zjistit, na které servery jste se snažili přistupovat. Tento problém řeší instalace lokálního DNS serveru, který se dotazuje přes síť Tor. Pokud vám to připadá jako vážný problém (už trochu moc paranoidní, ale na to ještě nikdo neumřel :)), lze to řešit pomocí **dns-proxy-tor** (http://p56soo2ibjkx23xo.onion/ [23] - Multiplatformní).

Tor Browser Bundle

Tor Browser Bundle je portable verze (spustitelná z USB flash disku) Firefoxu s implementovaným TORem a dalšími Firefox rozšířeními pro vyšší bezpečnost a anonymitu. Obrovskou výhodou tohoto all-in-one systému je především to, že ho máte na USB, takže ať přijdete k jakémukoliv počítači, máte během pár sekund přístupný Firefox s komunikací přes Tor síť a navíc Torpark v systému nezanechává naprosto žádné informace o navštívených stránkách, dočasné soubory atd.

Tor Browser Bundle můžete stáhnout zde: http://www.torproject.org/projects/torbrowser.html.en [24]



[25]

[26]

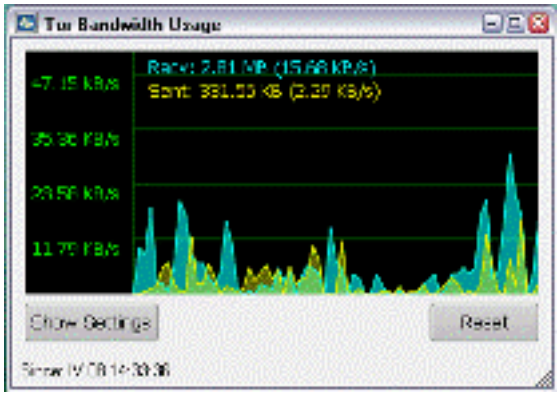
Video znázorňující používání TORu

http://www.irongeek.com/i.php?page=videos/tor-1 [27]

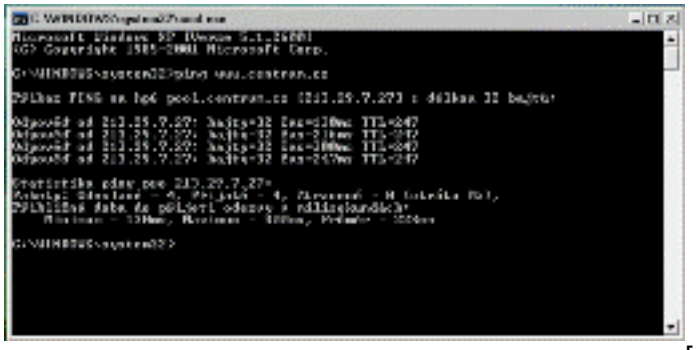
můžete ho stáhnout offline zde: stažení videa Tor z SP [28]

Nevýhody?

Poměrně velkou nevýhodou systému Tor je jeho rychlost, resp. pomalost. Je to trochu způsobené jeho způsobem komunikace s ostatními routery, ale především nedostatkem lidí, kteří by nabídli svůj traffic ve prospěch lidí využívající Tor a velkým množstvím hloupých spammerů a warezáků, kteří takto zneužívají síť a zahlcují jí nesmysly. :o(



[29]


[30]

Cílem projektu Czech & Slovak TOR Community [5] je šířit podvědomí o tomto systému a vyjít vstříc lidem, kteří by se chtěli zapojit do sítě onion routerů a nabídnout tak svůj traffic ostatním lidem využívajícím Tor. Propagací se snažíme také podpořit projekt finančně na oficiálních stránkách, aby mohl být dále vylepšován.
-> Fórum projektu [31]

O nastavení serveru, blokovaní IP a jeho dalších možnostech zabezpečení bude můj příští článek a byl bych rád, kdyby se do něj zapojilo hodně lidí a tím tak zvýšili rychlost a propustnost celé sítě.

Závěr

Snad vás tento systém nadchnul a vyzkoušíte ho. Chtěl bych vás však všechny poprosit, abyste síť nevyužívali k hloupostem (stahování warezu, spam, jiná ilegální či síť zatěžující činnost apod.), protože k tomu není určena a ostatní lidé nenabízejí svůj traffic pro takovéto blbosti (zkuste raději Kademlii [32], nebo WASTE [33], které jsou k bezpečnému P2P určeny).

Odkazy

Homepage projektu TOR [34]

Finanční podpora projektu [35]
Instalace TORu pod Windows [36]
Instalace TORu pod Linuxem [37]
Instalace TORu pod Mac OS X [38]
TOR FAQ [39]
TOR Network Status [40]

Zdar u dalšího článku ve kterém se budeme zabývat (mimojiné) instalací a nastavením TOR serveru.

URL článku:
https://security-portal.cz/clanky/tor-onion-router-syst%C3%A9m-pro-vysoce-anonymn%C3%AD-%C5%A1ifrovan%C3%BD-p%C5%99%C3%ADstup-k-internetu

Odkazy:
[1] https://security-portal.cz/users/cm3l1k1
[2] https://security-portal.cz/category/tagy/anonymita
[3] https://security-portal.cz/category/tagy/recenze
[4] https://security-portal.cz/category/tagy/security
[5] http://tor.security-portal.cz/
[6] http://www.security-portal.cz/img/clanky/114/tor_network_map.png
[7] http://www.security-portal.cz/img/clanky/114/ustaveni_tor_retezce.png
[8] http://www.security-portal.cz/img/clanky/114/htw1.png
[9] http://www.security-portal.cz/img/clanky/114/htw2.png
[10] http://www.security-portal.cz/img/clanky/114/htw3.png
[11] https://svn.torproject.org/svn/projects/design-paper/tor-design.pdf
[12] http://6sxoyfb3h2nvok2d.onion/
[13] http://www.security-portal.cz/img/clanky/114/hidden_wiki.png
[14] http://tor.eff.org/download.html.en
[15] http://www.security-portal.cz/img/clanky/114/vidalia.png
[16] http://www.security-portal.cz/img/clanky/114/tor_log.png
[17] http://www.security-portal.cz/img/clanky/114/firefox_proxy_tor.png
[18] http://anoncheck.security-portal.cz/
[19] http://www.security-portal.cz/img/clanky/114/anonymity_checker.png
[20] https://addons.mozilla.org/en-US/firefox/addon/1237
[21] https://addons.mozilla.org/en-US/firefox/addon/433
[22] http://noscript.net/
[23] http://p56soo2ibjkx23xo.onion/
[24] http://www.torproject.org/projects/torbrowser.html.en
[25] http://www.security-portal.cz/img/clanky/114/torpark_buildingcircuit.png
[26] http://www.security-portal.cz/img/clanky/114/torpark.png
[27] http://www.irongeek.com/i.php?page=videos/tor-1
[28] http://data.security-portal.cz/clanky/114/tor-1.swf
[29] http://www.security-portal.cz/img/clanky/114/tor_bandwidth_usage.png
[30] http://www.security-portal.cz/img/clanky/114/tor_ping_lag.png
[31] https://forum.security-portal.cz/viewforum.php?f=50
[32] http://en.wikipedia.org/wiki/Kademlia
[33] http://www.security-portal.cz/clanky/waste---komunikacni-program-a-sdileni-souboru-pro-paranoiky.html
[34] http://tor.eff.org/
[35] http://tor.eff.org/donate.html.en
[36] http://tor.eff.org/docs/tor-doc-win32.html.en
[37] http://tor.eff.org/docs/tor-doc-unix.html.en
[38] http://tor.eff.org/docs/tor-doc-osx.html.en
[39] http://wiki.noreply.org/noreply/TheOnionRouter/TorFAQ
[40] http://torstatus.blutmagie.de/

CC-BY-SA Security-Portal.cz | secured by paranoid sense | we hack to learn