Redogörelse för DFRI:s arbete med Tor- och oniontekniken februari 2012 - augusti 2013

Innehållsförteckning

Bilagor

Introduktion och sammanfattning

Det här dokumentet redogör för DFRI:s arbete med Tor mellan februari 2012 och augusti 2013. Under perioden drev DFRI fyra Tor-exit-relän, med en total kapacitet om ca 250 Mbit/s, och gjorde olika tester av Tor-tekniken.

I samband med att Tor-projektet efterlyste fler bryggor satte DFRI under en period upp 250 bryggor för att undersöka hur mycket trafik de skulle förmedla om de fick tillgång till obegränsad kapacitet. Slutsatsen är att Tor-bryggors behov av kapacitet är låg.

DFRI satte även upp ett testnätverk som användes för tidiga tester av IPv6-stödet i Tor.

DFRI har även investerat i hårdvara för att förmedla mer trafik, och testat gränserna för trafikmängd per Tor-relä.

Föreningen köpte även in 23 stycken RaspberryPi, och konfigurerade dem för att enkelt kunna användas som mellanrelän av ”icke-tekniska” personer. Enheterna delades ut till föreningens medlemmar.

Föreningen har även kartlagt vilken typ av abuse-ärenden som drift av Tor-exit-trafik ger, och tagit fram en policy för att hantera och svara på dessa.

Under de första sex månaderna handlade abuseärendena främst om automatiserade scanningar av sårbarheter, samt scraping, och enstaka fall av webbspam och skräppostningar till forum. Sedan sommaren 2013 har föreningen även tagit emot en stor mängd abuseärenden rörande copyrightskyddat material.

Tor och Prestanda

Vid lägre bandbreddsutnyttjande kräver inte Tor-noder några särskilda optimeringar av prestanda, men när användningen ökar finns det flera parametrar att ta hänsyn till.

Desto fler klienter som använder noden, desto mer ökar mängden kryptooperationer. Därmed är CPU en av de främsta begränsningarna för ett högpresterande Tor-relä. Utöver den TLS-session som etableras för att få trafiken att se ut som vanlig TLS i en nätverksanalysator sker det även en mängd krypterings- och dekrypteringsoperationer för att lägga på och ta bort så kallade onion skins.

Behov av prestanda och bandbredd i Tor-nätet

Ju mer bandbredd och CPU som tillförs Tor-nätet, desto snabbare blir tjänsten. Idag är Tor relativt krångligt och långsamt att använda, men om det vore lika snabbt och enkelt som vanlig Internetanvändning antar DFRI att antalet användare skulle öka kraftigt. Anledningen är att det varit mycket enkelt att för DFRI att nå maxkapacitet på samtliga noder, oavsett om den begränsande faktorn varit CPU eller bandbredd.

Fler användare och noder är i sin tur önskvärt eftersom det:

- Stärker anonymiteten för de som bäst behöver den
- Gör det svårare att lista ut vem en användare är genom trafikanalys på multipla platser i nätet
- Gör det mer normalt att anonymisera trafik, vilket medför att personer som surfar anonymt inte behöver bli misstänkliggjorda
- Gör det dyrare för webbplatsägare att fullständigt blockera Tor-användare

Så ökas prestandan för Tor

DFRI kör idag samtliga Tor-noder på FreeBSD, version 9 eller senare (även om FreeBSD 8 även användes under stora delar av 2012). Då FreeBSD:s bassystem släpps med OpenSSL version 0.9.8 kommer det bli möjligt att öka prestandan markant genom att uppgradera OpenSSL till 1.0.1c.

OS-optimering

DFRI:s erfarenhet är att operativsystemets resursbegränsningar måste anpassas för att nå maximal prestanda. Detta främst på grund av att FreeBSD:s förinställda värden inte är optimala för att köra en eller flera Tor-noder.

SMP och multiCPU-stöd

Eftersom moderna processorer har fler CPU-kärnor med multipla exekveringstrådar är det viktigt att använda operativsystem med bra SMP-stöd. Även om Tor inte skalar linjärt med fler processorer kan en Tor-process avlasta flera operationer på så kallade ”worker-threads”. DFRI har testat flera olika typer av processorer och kommit fram till att även om processorn är ny* kommer det inte finnas CPU-kapacitet för att maximera en gigabitlänk med endast en Tor-process. Det går dock utmärkt att starta flera noder på samma maskin för att ytterligare balansera lasten. De mätningar och praktiska prov som DFRI genomfört pekar på att en processor på 3.6GHz* klarar av att saturera minst 3Gbit/s, förutsatt att det finns tillräckligt med bandbredd och klienter. * 2011, Intel X3850

Mbuf-clusters
FreeBSD använder minneskluster för nätverksanslutningar för att kunna balansera dessa över flera CPU:er, så kallade mbuf-clusters. När denna resurs tar slut kan inga fler nätverksanslutningar skapas, och maskinen slutar att vara nåbar från nätet. Det går givetvis att öka värdet på parametern som styr det maximala antalet, men detta kostar minne, och kräver också en justering av hur mycket minne operativsystemskärnan använder.
Om detta inte görs i takt finns det möjlighet att mbuf-clusters använder för mycket av kärnans reserverade minne, vilket resulterar i att operativsystemet kraschar. Justering av kernel-minne har dock minskad relevans i FreeBSD 9 och senare.

Fildeskriptorer
En högpresterande Tor-nod behöver en stor mängd fildeskriptorer, främst av följande anledningar;

- Samtliga reläer sätter upp persistenta koppel mellan varandra för att inte göra dyra SSL-handskakningar i onödan
- Varje klient som nyttjar noden som guard (första hoppet in Tornätet) nyttjar en fildeskriptor
- Varje klient som nyttjar noden som en exit (sista hoppet ur Tornätet) nyttjar en fildeskriptor

Med fler klienter ökar behovet av fildeskriptorer, vilket också kräver en ökning av operativsystemets basvärde för maximalt antal filer och maximalt antal filer per process.

Optimering av TCP/IP-stacken
För att reducera lasten och öka prestandan finns det flera parametrar som bör anpassas. Dels bör systemet ställas in så att TCP-koppel i sin slutfas städas bort snabbare. Det förinställda värdet här är 30 sekunder, vilket är en mycket lång tid då klienter kan försvinna av en mängd orsaker och således inte kan avsluta sin session korrekt. Detta värde har DFRI reducerat till 7,5 sekunder, vilket också är en väldigt lång tid i sammanhanget.

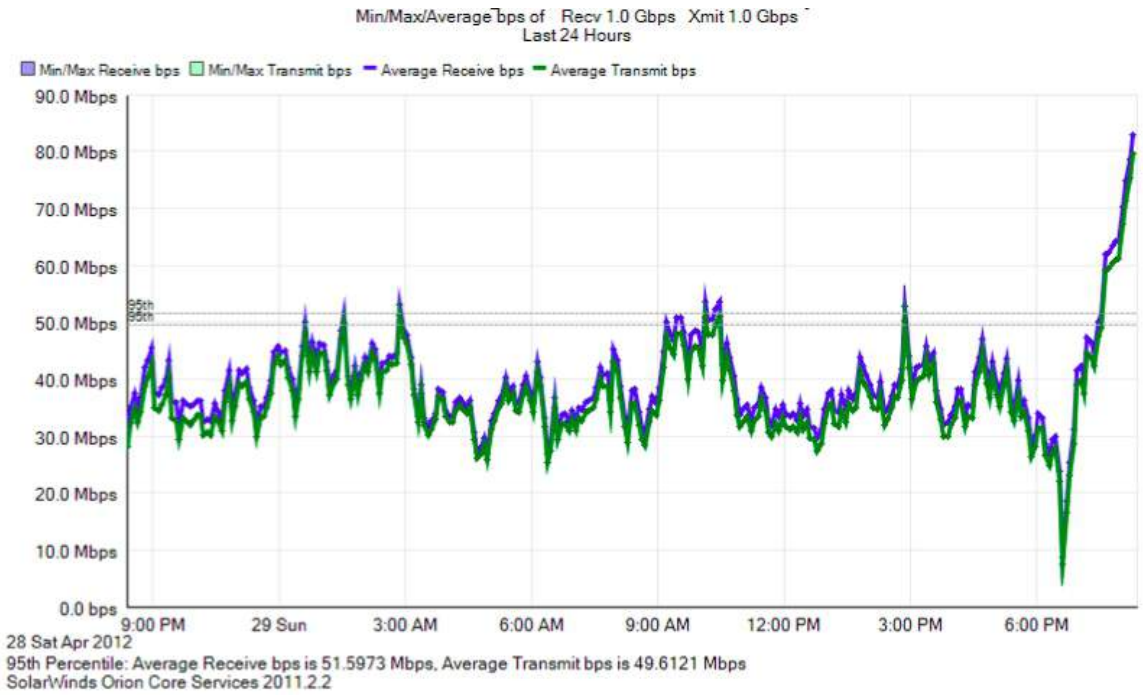
För att klara av ett högre antal klienter bör även det maximala antalet sockets öka. Även socketbuffrarna bör justeras, det minne som reserveras för att hantera olika nätverkskoppel, återigen till en kostnad av minne.

Summering av förändrade sysctl-värden

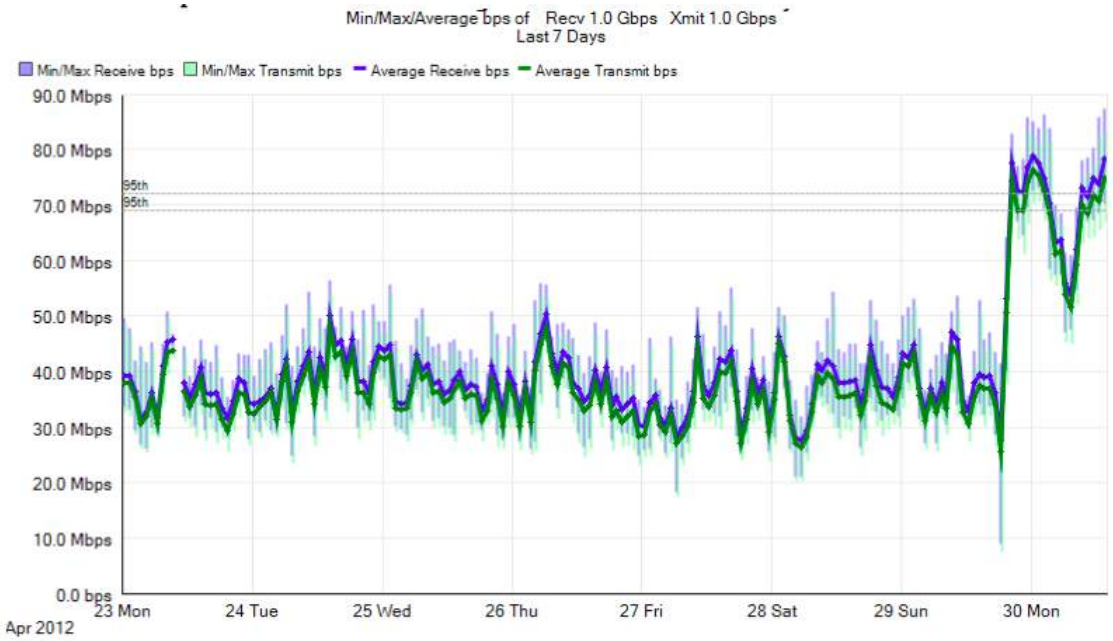
Sysctl-värde	Förinställt värde	Nytt värde
kern.ipc.nmbclusters	25600	262144
net.inet.tcp.msl	30000	7500
kern.ipc.somaxconn	128	32768
kern.ipc.maxsockets	25600	204800
kern.ipc.maxsockbuf	2097152	16777216
net.inet.tcp.recvbuf_max	2097152	16777216
net.inet.tcp.recvspace	65536	8192
net.tcp.sendspace	32768	16384

OpenSSL

Bilden nedan visar ett dygns Tor-trafik från ett av DFRI:s relän, där den stora nedgången beror på uppdatering av OpenSSL-biblioteket. Notera att hårdvaran för denna Tor-nod inte har stöd för AESNI, och denna förbättring endast skett tack vare mer effektiv AES-implementation i OpenSSL. Det går även att tydligt se att förändringen håller i sig.



Bilden nedan visar samma nod, men över ett annat tidsspann



Prestandamätning

Genom att använda program för att testa Tors prestanda går det att se om olika förändringar ger bättre eller sämre resultat. DFRI har genomfört prestandamätningar på flera olika noder med olika processorer och SSL-bibliotek. Slutsatsen är att att snabba SSL-bibliotek gör att noden klarar att leverera mer. En sammanställning av resultatet återfinns i tabellen nedan. Notera att dessa tester inte helt går att sätta i ett 1:1 förhållande med en nod i drift, då det även finns andra parametrar som påverkar.

Nodnamn	Inbound-cells	Outbound-cells	NS/CELL*	AESNI	OpenSSL-version
Kimya	4590.73	4555.30	9.02/8.95	Nej	0.9.8
Kimya	2581.91	2777.1	5.07/5.46	Nej	1.0.1c
Amnesia	3126.88	3131.38	6.14/6.15	Nej	0.9.8
Amnesia	1414.43	1518	2.78/2.98	Ja	1.0.1c
Junebug	292.42	308.62	0.57/0.61	JA	1.0.1c

*Lägre värden innebär högre prestanda.

Bryggor till Tor-nätet

Alla klienter kan inte fritt ansluta till Tor-nätet som de vill. Tor-bryggor (bridges) är ingångar till Tor-nätet som inte är publikt publicerade utan istället delas ut i begränsad omfattning till användare för att kringgå blockering. De används av klienter som ett extra första hopp för att ansluta till Tor-nätet från nätverk där Tor blockeras, eller för att inte lika tydligt visa att Tor används.

Flera länder har börjat detektera och blockera vanliga Tor-bryggor med hjälp av nätverkssignaturer. Därför har nya protokoll utvecklats, så kallade "pluggable transports and obfuscated bridges", som inte upptäcks av de gamla signaturerna. Kapplöpningen är svår att vinna, men underlättas av många bryggor.

DFRI fick under 10 veckor möjlighet själva förfoga över en 100 Mb/s internetlina med ett tillhörande nät. Samtliga 255 IP-adresser på nätet konfigurerades på en gammal laptop, varefter slumpmässiga portar och IP-nummer med hjälp av en lokal brandvägg dirigerades om till en och samma Tor-process, konfigurerad som en obfuskerad brygga version 2 och 3.

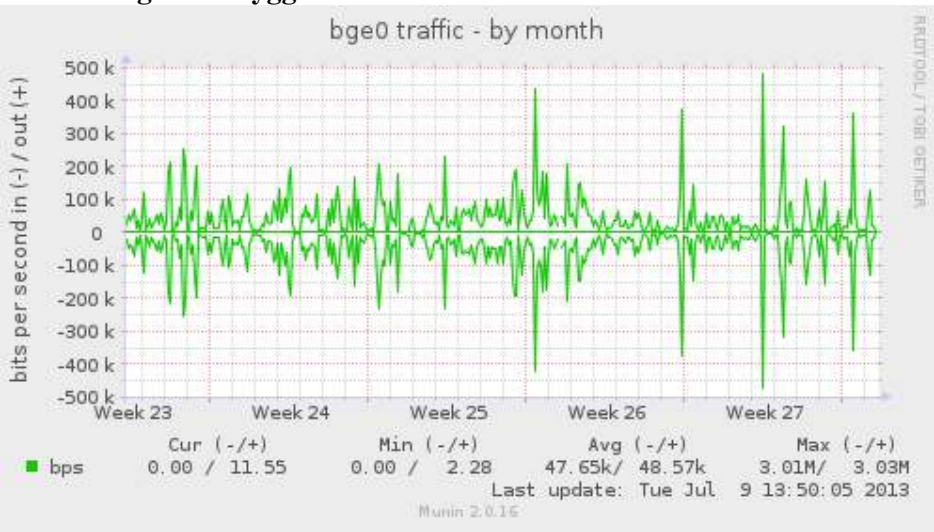
Syftet var att undersöka hur mycket bandbredd bryggorna skulle ta, men också för att Tor-projektet precis bett om fler bryggor. De slumpade kombinationerna av ip:port skickades sedan till Tor-projektet. Se "[tor-relays] A call to arms for obfuscated bridges" [1]

I konfigurationen ställdes följande in:

```
BridgeRelay 1
ServerTransportPlugin obfs2,obfs3 exec /usr/local/bin/obfsproxy managed
```

[1] https://lists.torproject.org/pipermail/tor-relays/2013-April/002089.html

Trafikmängd för bryggor



Bilden ovan visar att bara en bråkdel av de 100Mb/s som fanns att tillgå utnyttjades, och att CPU-användningen var obetydlig, även för en gammal dator.

Hur mycket trafik bryggorna skulle komma att förbruka var omöjligt att förutse. Det är enkelt att begränsa Tor till att bara använda en viss mängd bandbredd, men så skedde inte i det här fallet eftersom mängden bandbredd ändå var obegränsad. Mängden trafik beror på hur många som får bryggan tilldelad sig, användningen, samt hur länge bryggan fortsätter att vara nåbar.

I bästa fall skulle varje brygga bara användas av enstaka personer som anonymt fått den tilldelad sig, men bristen på bryggor gör att varje brygga delas ut till många individer och förr eller senare blir blockerade. Antingen manuellt, baserat på ipadress:portnummer, för att de delats ut till en part som vill begränsa tillgången till Tor-nätverket, eller med hjälp av till exempel nätverkssignaturer.

Bristen på IPv4 adresser gör det svårt att driva många bryggor och samtidigt hålla dem dolda. Det går även att köra bryggor på IPv6, och här finns det stora möjligheter att i framtiden flytta runt bryggorna för att det inte ska gå att testa sig fram till dem.

Nätarkitektur, bakgrund och utformning

Varför eget nätblock?

Den som driver Tor-exittrafik riskerar att felaktigt hållas ansvarig för trafik som Tor-användare skickar och tar emot över internet. Därför har DFRI sett till att skaffa ett eget nätblock.

DFRI anser också att en förening med ett uttalat mål att stärka integritetsskyddet på internet och driva Tor-trafik bör ha större möjlighet att resonera med den som anser sig utsatt för oegentligheter än vad en privatperson har.

Tydlighet gentemot övriga aktörer på internet är ett övergripande mål för DFRI:s verksamhet. Allt sker öppet och i enlighet med hur internet administreras. Föreningens styrelse är ytterst ansvarig för driften av nätet.

Genom att vara sin egen internetoperatör kan DFRI även köpa transit från och arrangera trafikutbyte med andra operatörer, vilket gör att Tor-trafiken sprids över flera punkter. Detta är en fördel ur säkerhetssynpunkt, eftersom "low-latency-nätverk" som Tor är sårbara för övervakning med korrelering av ingående och utgående trafik.

En annan effekt av s.k. trafikutbyte (peering) är att den trafik som "peeras av" inte kostar något. DFRI peerar idag av ca 10% av sin trafik. Arbetet med att öka siffran fortgår.

Utformning av nätet

DFRI har idag utrustning på fyra sajter i Stockholm. Dessa binds samman i ett L2-nät sponsrat av Teknikbyrån i Sverige AB. Trafiken routas i tre stycken routrar anslutna till tre transitleverantörer, två IXP:er och ett fåtal privata peering-anslutningar. En av transitleverantörerna sponsrar även DFRI med gratis transit.

Totalt sex stycken servrar är anslutna till nätet. Förutom Tor-relän och bryggor så används servrarna till andra tjänster, som DNS, mejl, web och testnät för Tor.

Det har visat sig svårt att balansera trafiken på ett sådant sätt att DFRI inte "drar över" hos någon av transitleverantörerna. I och med att det nätblock som DFRI använder är det minsta som routas på internet så går det inte att annonsera olika delar av DFRI:s nät hos olika transitleverantörer.

DFRI har heller inte tillgång till avancerad utrustning för trafikstyrning, vilket medför att föreningen istället får lägga tid på att försöka styra om trafiken för bästa balans.

DFRI har idag för låg redundans vad det gäller routrarna. I synnerhet en av routrarna utgör en ”single point of failure” på ett sätt som försvårar driften av nätet och gör nätet sårbart för bortfall samt oväntade hård- och mjukvarufel.

Abuse och Abusehantering

Ett av DFRI:s mål med att drifta exit-noder är att se hur det fungerar ur rättslig synpunkt och få en bild av de vanligaste abuse-ärendena och ta fram strategier för att hantera dem.

En av effekterna av att DFRI har ett eget nätblock är att det ger föreningen kontroll över en egen abuse-adress. En abuse-adress är den e-postadress som fungerar som kontaktpunkt för den som har ett klagomål att framföra till ägaren av ett nätblock.

Att DFRI själva hand om abuse-mejlen är värdefullt av flera anledningar. Många internetleverantörer väljer idag att stänga av användare som genererar mycket klagomål, något DFRI undviker genom att vara sin egen internetleverantör. Föreningen riskerar inte heller att en annan internetleverantör misstolkar eller ignorerar inkomna klagomål, vilket skulle kunna resultera i onödig eskalering av ärendet hos avsändaren, samt att ärendet inte hanteras korrekt.

Mellan 1:a februari och 15 oktober 2012 har 91 tydliga fall av abuse-ärenden rapporterats till DFRI. Antalet abuse har sedan dess ökat, dels för att DFRI:s exit-bandbredd ökat, men främst för att antal abuse som rör upphovsrättsskyddat material skjutit i höjden. Siffran för perioden 16 oktober 2012 – 31 augusti 2013 är 884.

DFRI har tagit fram ett antal proaktiva åtgärder för att underlätta för administratörer av en tjänst som utsatts för abuse. Den första åtgärden är att göra det så tydligt som möjligt att src-adressen tillhör en exit-nod genom att alltid namnge PTR-recordet tor-exitN-readme.dfri.se. På adressen finns även webbsida som förklarar att trafiken kommer från en Tor-exit router.

DFRI har även upprättat ett tekniskt beredskapsschema där den person som har beredskap också svarar på abuse-ärenden. Om det finns möjlighet försöker DFRI också ge råd och hjälp vid olika typer av ärenden.

Typer av abuse som sker från DFRI:s exit-trafik

De första sex månadernas Tor-drift visar att de vanligaste formerna av abuse som genereras från föreningens exit-noder har handlat om automatiserade scanningar av sårbarheter, samt scraping. Utöver dessa har det även förekommit fall av webbspam och skräppostningar till forum. Sedan början av 2013 har föreningen även tagit emot en stor mängd abuseärenden rörande copyrightskyddat material.

Scraping

Under den tid som DFRI kört exit-trafik har 41 scraping-ärenden hanterats. Rapporterna har dock endast kommit från ett automatiserat system som informerat om att en temporär blockering upprättats. Då ingen svarat på adressen har DFRI har inte lyckats informera om att klienten varit en exit-nod.

Intrångsförsök och sårbarhetsscanningar

Flera abuse-meddelanden rör sårbarhetsscanners eller intrångsförsök, där vad som ser ut att vara automatiserade script försöker använda SQL- eller PHP injections på olika webbplatser. Det har även förkommit ett fall där servrar temporärt varit mål för samordnade attacker från vad rapportören ansåg vara hackarnätverket Anonymous. Det förekommer också att försök till så kallade brute force-attacker sker genom DFRI:s exit, oftast i försök att logga in på tjänster så som IMAP, FTP och SSH.

I samtliga fall har rapportören misstänkt att komprometterade system funnits på DFRI:s nät och begärt att få dem åtgärdade. Tyvärr lyckas DFRI sällan upprätta någon form av dialog med ägarna av de system som blir attackerade, men har mötts av förståelse i de fall som lyckats. I ett fall hade rapportören god kännedom om Tor och valde att vitlista samtliga DFRI:s exit-noder från abuse-generering.

Det är viktigt att förstå att attackerna från DFRI:s nät hittills upptäckts automatiskt av honungsfällor eller IDS-system. Men mer kvalificerade attacker skulle förmodligen inte upptäckas av automatiserade system. Det är också troligt att flera av attackerna från DFRI:s nät är så kallade ”false positives”, där det handlat antingen om en IDS-motor som haft fel signatur, eller att trafiken varit för att testa ett IDS-system.

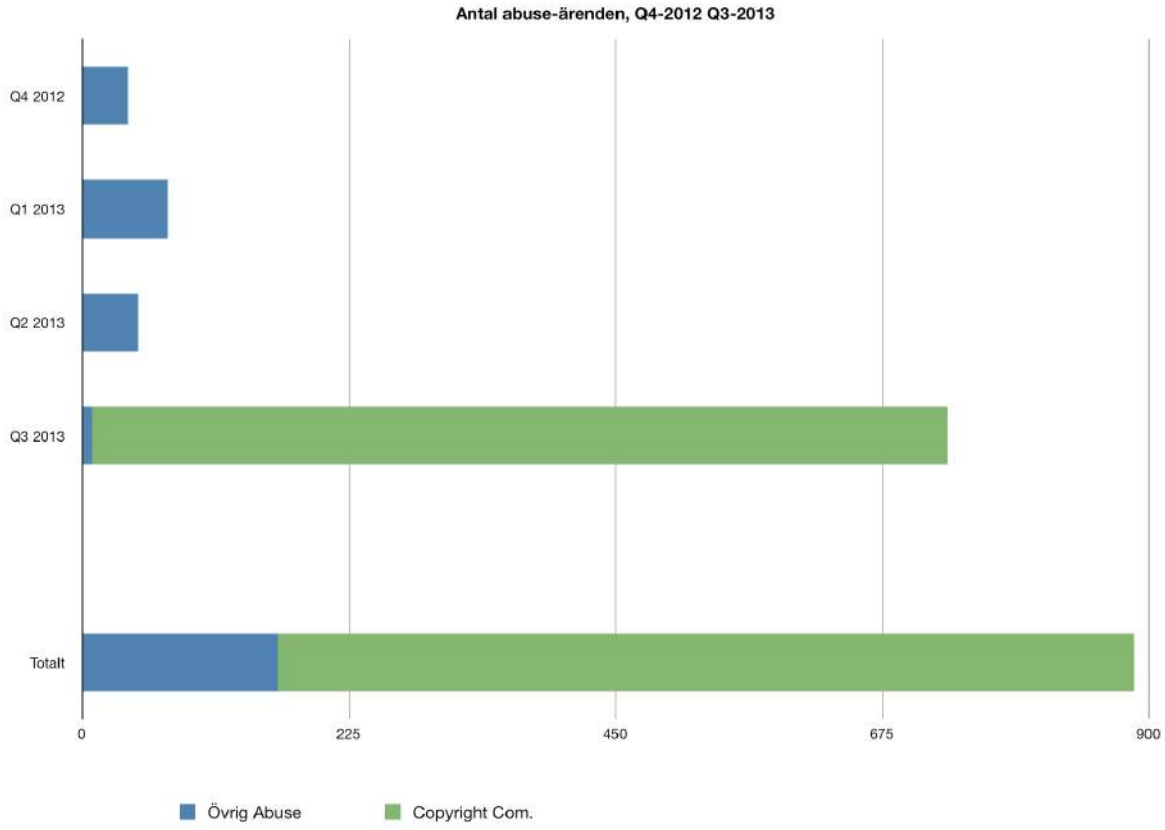
Spam
Den oönskade reklam som genereras från DFRI:s nät sker främst i form av forumspam, där skräpposter med affiliatelänkar skapas. Vid ett tillfälle ville rapportören blockera access från DFRI:s system till det forum rapportören administrerade. I detta fall frågade DFRI om det var möjligt att istället genomföra en mer långsiktig lösning för att bekämpa spam, i detta fall genom att implementera captchas för nya användare. Dessvärre återkom aldrig rapportören.

Fildelning av copyrightskyddat material
DFRI har valt att försöka begränsa möjligheten att använda exit-noderna för delning av copyrightskyddat material. Detta genom att blockera ett antal portar som används för fildelning, vilket går att se i exitpolicyn.

Men nyare fildelningsprotokoll, så som Bittorrent, kan använda vilka TCP-portar som helst, vilket medför att blockering inte är möjligt utan att göra DPI, eller deep packet inspection, alltså djupare trafikanalys. DFRI har dock avstått från denna typ av trafikanalys, eftersom det direkt skulle påverka integriteten för exit-nodens användare.

Under perioden 2013-04-06 till 2013-08-31 tog DFRI emot 754 abuseärenden. Bakom 722 av dessa låg företaget Irdeto USA Inc., som den 30 juli 2013 började skicka abuseärenden till DFRI rörande copyrightskyddat material.

DFRI svarade på det första meddelandet, men fick inget svar från avsändaren. Föreningen ansåg det ändå vara korrekt att fortsätta svara företaget, och implementerade därför en funktion för autosvar på första mailet i varje givet abuseärende. Hittills har DFRI autosvarat på 157 mail från Irdeto.



För detaljer per månad, 2012-09 och framåt, se appendix Abuse-graphs.

Framtida utveckling av abuse-rapportering
DFRI avser att utveckla abuserapporteringen genom att bättre kategorisera vilken typ av abuse som kommer in, samt antal abuse per Mbit per månad. Målet är att redovisa detta i aggregerad form på DFRI:s webbplats, dels av transparensskäl, men också för att hjälpa personer som forskar i ämnet.

Jämförelser med resten av nätet

Det är svårt att ge exakta siffror på hur stor del av Tor-nätet DFRI bidrar med i form av exits och bandbredd. Anledningen är att det ständigt tillkommer och faller bort noder i nätverket, och att noderna ändrar hastighet.

När denna rapport skrevs fanns det totalt 4202 noder i Tor-nätet, jämfört med de 3075 som observerades vid föreningens halvtidsrapport för projektet. Även om antalet noder ökat i nätet så har mängden bandbredd minskat. Det går också tydligt att se att antalet exit-noder inte ökar i samma takt som reläer.

	Halvtidsrapport	Slutrapport
Antal Tor-noder	3075	4202
Antal exits	842	934
Bandbredd i nätet MB/s	2160	988
DFRI:s totala exit vid kontrolltillfället (MB/s)	26.5	37
DFRI:s bidrag	1.20%	3.70%

Dessa siffror är framtagna vid halvtidsrapporten 9 december 2012, och vid slutrapporten den 24 september 2013 från webbplatsen blutmagie[2]. Då många av siffrorna fluktuerar kraftigt gjordes ytterligare en kontroll 14 oktober, som visade mer rimliga siffror:

	Halvtidsrapport	Slutrapport	Kontrolltillfälle
Antal tor-noder	3075	4202	4605
Antal exit-noder	842	934	910
Bandbredd i nätet (MB/S)	2160	988	2647
DFRI:s totala exit vid kontrolltillfället (MB/S)	26.5	37	18
DFRI:s bidrag	1.20%	3.70%	0.6%

Att DFRI:s bidrag är så lågt vid kontrolltillfället beror delvis på att en av DFRI:s exit-noder temporärt saknas från nätet på grund av hårdvarufel. Det är också intressant att konstatera att trots den stora ökningen av noder i nätet har bandbredden inte ökat dramatiskt. Detta kan delvis förklaras med att många noder inte kan nyttjas till sin fulla kapacitet på grund av att ett botnät[3] nyttjar Tor för sin kommandokanal på ett mycket prestandakrävande sätt.

Exitpolicy

En exitpolicy är en lista på portar och destinationsnät där Tormjukvaran tillåter utgående trafik. Även om det är önskvärt att tillåta trafik till samtliga nät och portar så finns det anledningar till begränsningar. DFRI:s exitpolicy är en kompromiss mellan att tillhandahålla så mycket tillgänglighet som möjligt, och samtidigt begränsa utgående trafik för att förhindra missbruk.

Nedan återfinns DFRI:s exitpolicy och motivering

Policy	Destination	Anledning
Neka	0.0.0.0/8:*	RFC1700, endast tillåtet som src.
Neka	169.254.0.0/16:*	RFC3927, linklocal
Neka	127.0.0.0/8:*	RFC5735, loopback
Neka	192.168.0.0/16:*	RFC1918, privata adresser
Neka	10.0.0.0/8:*	RFC1918, privata adresser
Neka	172.16.0.0/12:*	RFC1918, privata adresser
Neka	171.25.193.0/24:*	DFRI:s eget nät
Neka	*:25	SMTP, förhindra spam
Neka	*:119	nntp (news)
Neka	*:135-139	Netbios/cifs/msrpc
Neka	*:445	MS-DS
Neka	*:563	Nntps (news)
Neka	*:1214	KaZaa (p2p)
Neka	*:4661-4666	eDonkey(p2p)
Neka	*:6346-6429	Gnutella (p2p)
Neka	*:6699	WinMX(p2p)
Neka	*:6881-6999	Bittorrent
Tillåt	*:*	

DFRI:s policy blockerar alltså tillgång till vissa nät, till exempel RFC1918-adresser, eller

[2] https://torstatus.blutmagie.de.
[3] https://blog.torproject.org/blog/how-to-handle-millions-new-tor-clients

loopback. DFRI blockerar också tillgång till sitt eget nät, dels för att förhindra att accesskontroller kringgås, men också för att skydda klienten, då den inte kan veta vad som återfinns på en RFC1918-adress som är nåbar från DFRI:s nät.

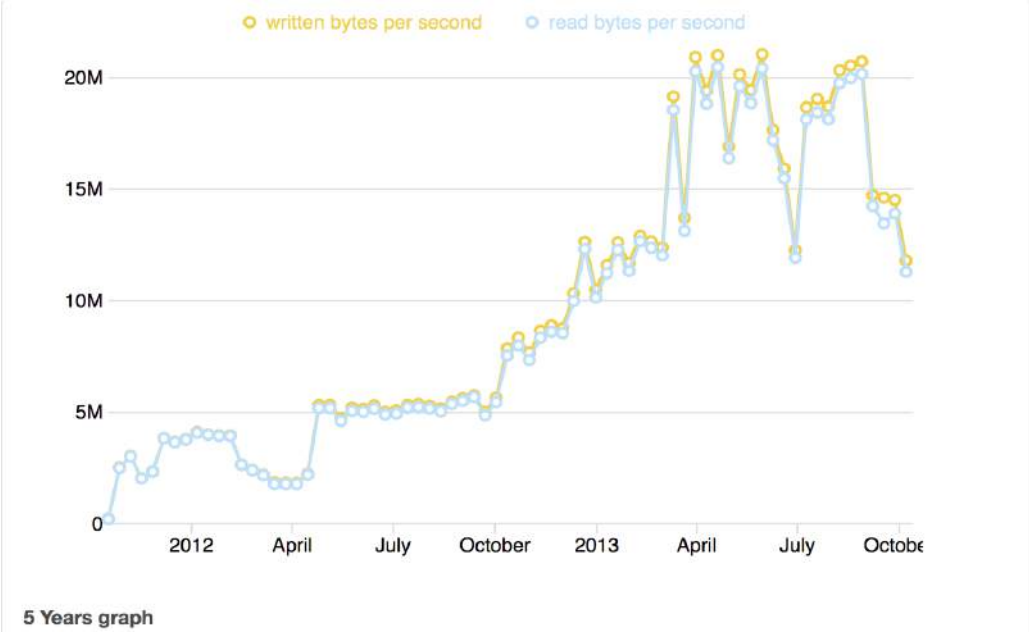
DFRI har också valt att blockera typiska p2p-tjänster, då detta är standardinställningen för Tor-exits, samt SMTP, och portar nåbara på Windowssystem som saknar härdning. SMTP och Windows-portarna blockeras främst för att förhindra abuse. Tillgången till p2p-tjänster är reducerad för att många p2p-tjänster läcker avsändarens riktiga IP-adress i protokollet, och för att bespara DFRI abuseärenden relaterade till copyright.

Trafikgrafer

Följande grafer redovisar hur DFRI:s fyra noder DFRI0[4], DFRI1[5], DFRI2 [6]och DFRI3[7] utnyttjat bandbredd under ett år. Graferna kommer från https://atlas.torproject.org

I takt med att DFRI fått tillgång till fler datahallar har nya noder tillkommit, varför DFRI3 bara har 3 månaders data. DFRI har samarbeten med ISP:erna Portlane, Atrato och Teknikbyrån, och nodernas bandbredd har justeras för att DFRI:s kostnader för bandbredd ska bli så låga som möjligt.

Trafikgraf DFRI 0

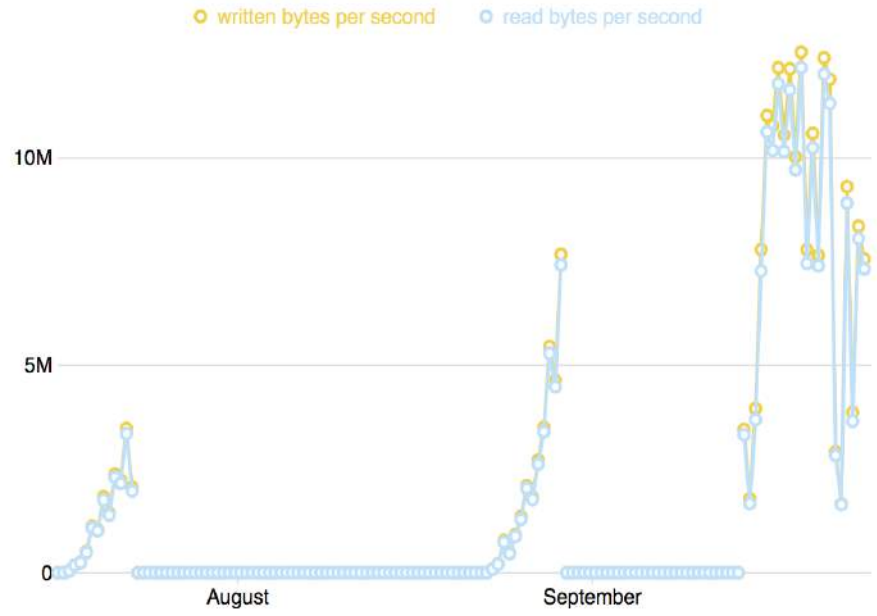


[4] https://atlas.torproject.org/#details/DD8BD7307017407FCC36F8D04A688F74A0774C02
[5] https://atlas.torproject.org/#details/A10C4F666D27364036B562823E5830BC448E046A
[6] https://atlas.torproject.org/#details/75EEE757E2941ADA4CBF89BAFA21B218F795BC97
[7] https://atlas.torproject.org/#details/4BAF6B9AA7D00BB142D611CFE897CB4FBE2943FF

Trafikgraf DFRI 1

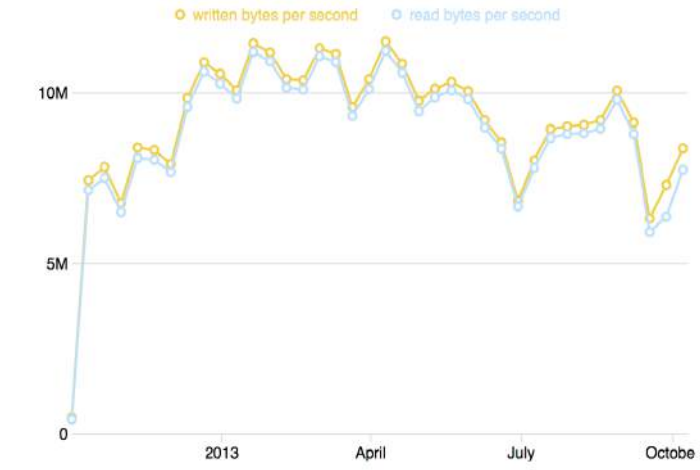
5 Years graph

Trafikgraf DFRI 2



3 Months graph

Trafikgraf DFRI 3



5 Years graph

Tor och IPv6

Bakgrund IPv6 och Tor

IPv6-stödet i Tor består Arbetet med att öka den siffra fortgårav flera olika delar. Klienter skall kunna kontakta förstahoppsrelän över IPv6, och dessa relän skall kunna acceptera inkommande koppel över IPv6. Relän skall kunna prata med varandra över IPv6, och exit-relän skall kunna kontakta tjänster på internet över IPv6.

Den första fasen av IPv6 för Tor inkluderade IPv6-stöd för klienter och privata bryggrelän. I nästa fas adderades stöd för bryggrelän vars adresser distribueras av Tor-projektet.

Nästa steg var att göra det möjligt för alla relän att annonsera en IPv6-adress, utöver sin vanliga IPv4-adress. Nätets "directory authoritites" utökades med funktionalitet att rösta på IPv6-adresser och nätets "konsensus", det vill säga det dokument som definierar nätet, kunde nu inkludera IPv6-adresser.

Det senaste tillskottet till IPv6-stöd i Tor innebar att exit-relän kunde börja koppla upp sig mot IPv6-adresser. Mer detaljer om de olika faserna finns i Tor:s ärendehanteringssystem[8].

Testnät för Tor

DFRI körde under utvecklingsperioden ett testnätverk [9] som användes för att göra tidiga tester av IPv6-stödet i Tor. Framför allt användes detta under hösten 2012 när det behövdes ett separat nät för att testa den nya konsensusmetod som tillåter att relän annonserar IPv6-addresser[10]. Testnätet har också varit värdefullt under testningen av det utökade stödet av exit till IPv6-adresser.

[8] https://trac.torproject.org/projects/tor/wiki/org/roadmaps/Tor/IPv6
[9] https://trac.torproject.org/projects/tor/wiki/org/roadmaps/Tor/IPv6/PrivateIPv6TestingNetwork
[10] Se metod 14 i https://gitweb.torproject.org/torspec.git/blob_plain/HEAD:/dir-spec.txt

Kontinuerlig drift av nya funktioner

I och med att DFRI konfigurerar sina reguljära relän att använda de nya IPv6-funktionerna så hjälper föreningen till att hitta fel i koden. DFRI har god kännedom om hur relän bör bete sig och upptäcker tidigt om något verkar vara fel. Organisationens kunskaper om hur programmet fungerar i detalj gör även att DFRI kan skriva detaljerade buggrapporter som är värdefulla för Tor-utvecklarna. Installationsbasen för IPv6-kapabel Tor är idag ca 65 relän. Av dessa är cirka 10 exit-relän.

DFRI och Raspberry PI

DFRI har även arbetat för att sprida användandet av Tor genom att skapa en kostnadseffektiv kombination av hård-och mjukvara som gör det mycket enkelt att driva mellanrelän för Tor. Allt som behövs är en internetuppkoppling.

Utmaningen var att hitta en hårdvara som kunde fungera som plattform ur ett tekniskt perspektiv, och som gick att göra så estetiskt tilltalande och användarvänlig som möjligt.

Hårdvaruvalet föll på Raspberry PI (RPI), som försågs med ett case av plast och DFRI:s klistermärke. För att underlätta installationen för mottagarna lades även en nätverkskabel och en strömadapter till i paketet.

Med hjälp av några tekniska föreningsmedlemmar skapades en testbädd för att se om plattformen höll måttet för Tor. Kontentan blev att enheterna kunde förmedla trafik i hastigheterna kring 5 Mbit/s utan problem, och ännu mer med rätt förutsättningar och lite överklockning.

Atlas dfri

Show 10 entries

Nickname	Bandwidth	Uptime	Country	IP	Flags	ORPort	DirPort
DFRI0	25.69 MB/s	23h 19m		171.25.193.20		443	80
DFRI1	3.15 MB/s	23h 20m		171.25.193.21		443	80
DFRI2	11.89 MB/s	1d 5h		171.25.193.131		443	80
DFRI3	13.11 MB/s	1d 3h		171.25.193.235		11443	1180
DFRIfriendlyPi	633.92 KB/s	11d 5h		83.255.60.115		443	0
ElofTor01DFRIraspPi	650.09 KB/s	69d 5h		90.225.80.219		9001	9030

DFRI anser att 5 Mbit/s är en rimlig hastighet för den genomsnittliga svenska internetuppkopplingen. Det vill säga, om användaren har en 10 Mbit/s uppkoppling används inte hela för Tor. Enheten gör dessutom en enkel mätning av bandbredden vid uppstarten, och riskerar därmed inte att ta för mycket av den.

Ett annan utmaning var administrationen kring enheterna, och möjligheten att uppdatera mjukvaran. Därför beslutade DFRI att:

- Använda en färdig distribution för Raspberry PI, valet blev Raspbian[11]
- Sätta upp script som automatiskt uppdaterar och underhåller "DFRI:s RPI" ute hos användarna, framför allt för att undvika säkerhetshål.
- Sätta upp script som modifierar en Raspbian-image till att bli en dfri-rpi-image.
- Publicera alla script[12] publikt för att visa på vad som finns på enheterna. På så sätt kan vändaren se att enheten gör det DFRI hävdar.
- Göra DFRI:s image [13]och procedur tillgänglig, så att vem som helst kan skapa en egen enhet.

[11] http://www.raspbian.org
[12] https://github.com/DFRI/dfri-rpi-tor
[13] https://dfri.se/projekt/tor/rpi

Varje RPI kan administreras från nätverket den placeras på genom att logga in över SSH med det lösenord som finns på undersidan av enheten. Det går även att koppla enheten till en skärm med hjälp av HDM20I.

Tester av enheten genomfördes under projektets gång, men dessvärre hann den inte delas ut till medlemmarna. I skrivande stund har samtliga 23 enheter delats ut, och DFRI arbetar med att samla statistik från användningen[14].

Föreningen undersöker bland annat

- Om det går att öka användandet och Tor-trafiken
- Om det går att få en större spridning av reläer
- Huruvida Tor-trafiken påverkas av RPI:erna

I första fasen körs enheterna bara som mellanrelän. Men i framtiden kommer fler lägen att introduceras, som användaren själv kan ställa in. Det finns också planer på att göra RPI till en "anonymiseringsenhet”, som kan tas med var som helst, till exempel på resor.

[14] https://atlas.torproject.org/#search/dfripi