


Trafikanalys och Tor

Överblick och relaterad forskning vid KAU

Philipp Winter, Tobias Pulls och Stefan Lindskog

4:e oktober 2018

Vad är ett anonymitetsnätverk?

Att analysera anonymitetsnätverk

- egenskap?
- attackerare?
- antaganden?
- användningsområden?

En global passiv attackerare

Källa: Simon Stålenhag, `simonstalenhag.se` (ursäkta men bilden är för bra!)

Skydd kostar fördröjning och/eller bandbredd

TABLE I

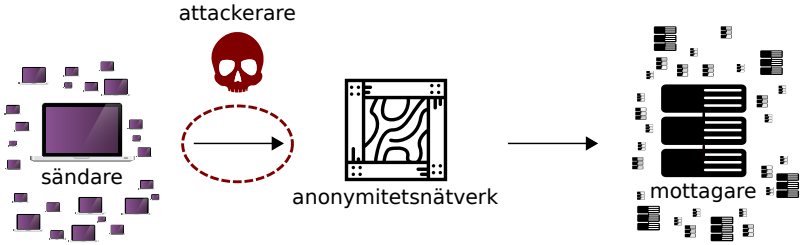
Latency vs. bandwidth vs. strong anonymity of AC protocols, with the number of protocol-nodes K, number of clients N, and message-threshold T, expected latency ℓ' per node, dummy-message rate β.

Protocol	Latency	Bandwidth	Strong Anonymity
Tor [10]	$\theta(1)$	$\theta(1/\mathsf{N})$	impossible
Hornet [47]	$\theta(1)$	$\theta(1/\mathsf{N})$	impossible
Herd [48]	$\theta(1)$	$\theta(\mathsf{N}/\mathsf{N})$	possible
Riposte [49]	$\theta(N)$	$\theta(\mathsf{N}/\mathsf{N})$	possible
Vuvuzula [20]	$\theta(\mathsf{K})$	$\theta(\mathsf{N}/\mathsf{N})$	possible
Riffle [21]	$\theta(\mathsf{K})$	$\theta(\mathsf{N}/\mathsf{N})$	possible
Threshold mixes [14]	$\theta(T \cdot \mathsf{K})$	$\theta(1/\mathsf{N})$	impossible*
Loopix [24]	$\theta(\sqrt{K} \cdot \ell')$	$\theta(\beta)$	possible
DC-Net [15], [46]	$\theta(1)$	$\theta(\mathsf{N}/\mathsf{N})$	possible
Dissent-AT [22]	$\theta(1)$	$\theta(\mathsf{N}/\mathsf{N})$	possible
DiceMix [16]	$\theta(1)$	$\theta(\mathsf{N}/\mathsf{N})$	possible

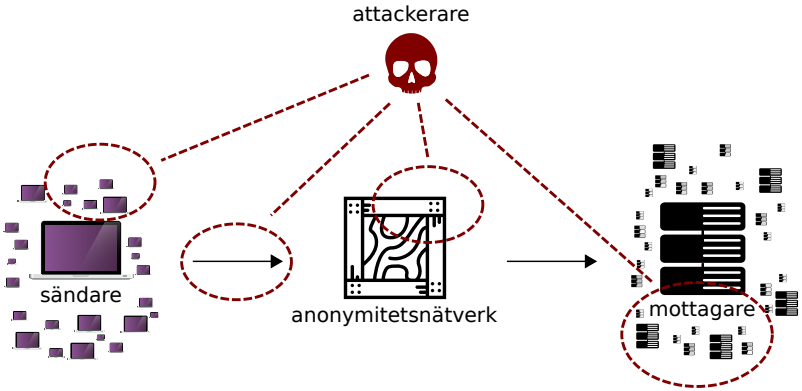
* if T in $o(poly(\eta))$

Källa: "Anonymity Trilemma: Strong Anonymity, Low Bandwidth, Low Latency—Choose Two" av Das et al., 2017

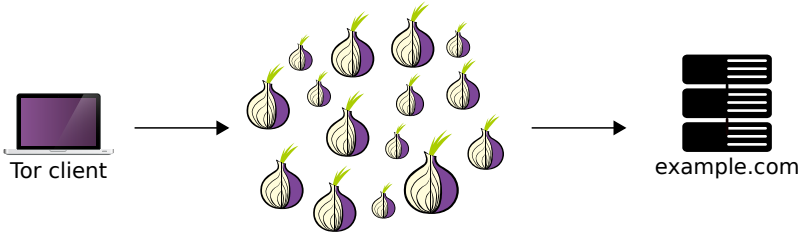
En lokal passiv attackerare



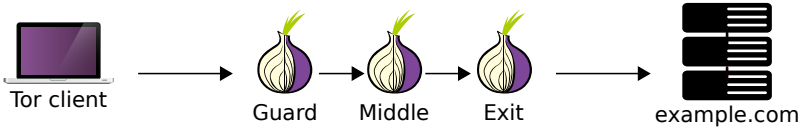
Resten: mittemellan attackerare



Tor – det största anonymitetsnätverket

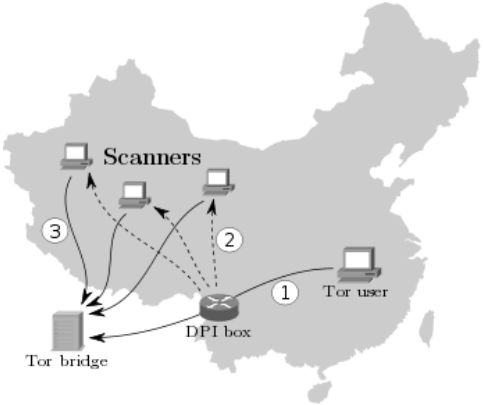


Tor – det största anonymitetsnätverket



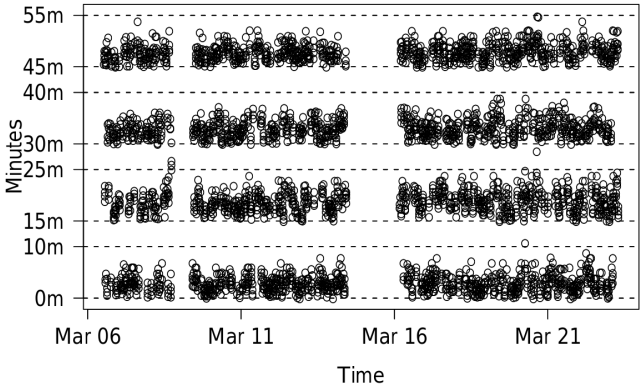
Kinesiska brandväggen

Den kinesiska brandväggen



Källa: “How the Great Firewall of China is Blocking Tor” av Philipp Winter och Stefan Lindskog, 2012

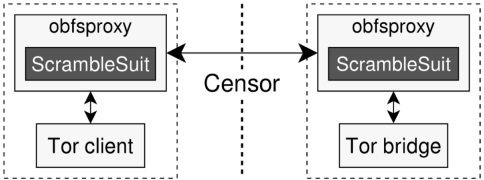
Den kinesiska brandväggen



Källa: "How the Great Firewall of China is Blocking Tor" av Philipp Winter och Stefan Lindskog, 2012

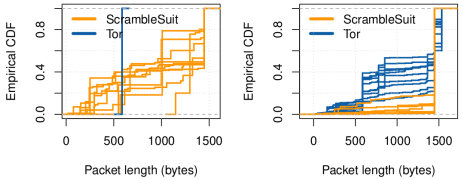
Gå runt censur

Pluggable Transports

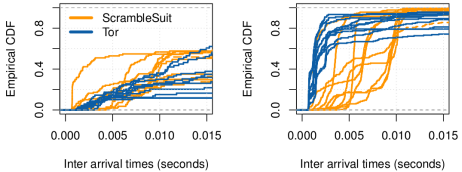


Källa: “ScrambleSuit: a polymorphic network protocol to circumvent censorship” av Winter et al., 2013

ScrambleSuit – ett polymorfiskt protokoll



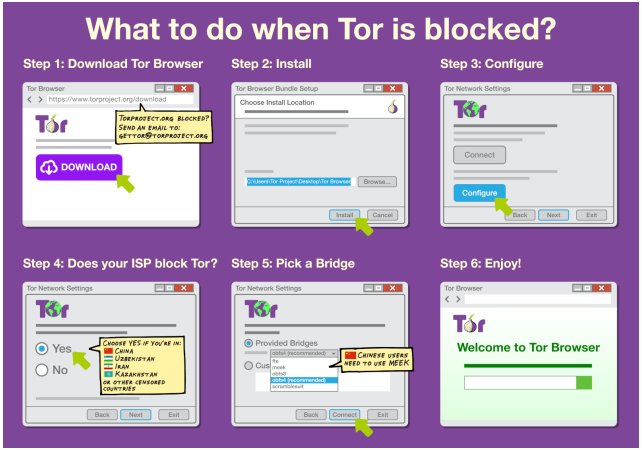
(a) Client-to-server. (b) Server-to-client.



(c) Client-to-server. (d) Server-to-client.

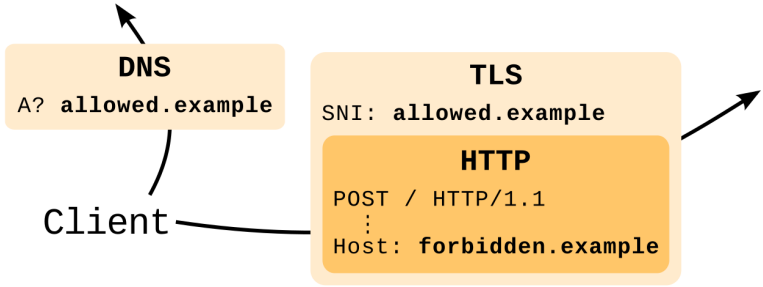
Källor: A Scanner Darkly samt "ScrambleSuit: a polymorphic network protocol to circumvent censorship" av Winter et al., 2013

Obfs4 = ScrambleSuit[2]



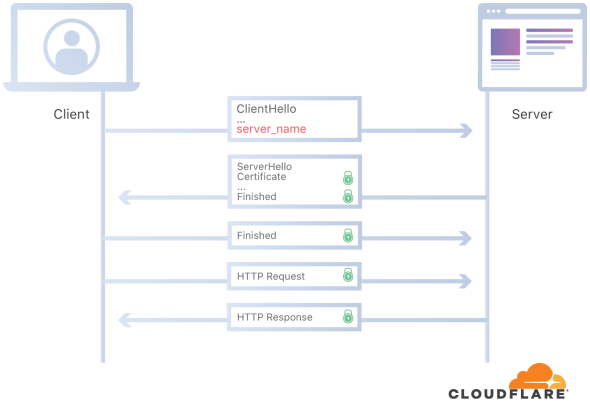
Källa: `https://www.torproject.org/docs/pluggable-transports.html.en`

Meek – domain fronting



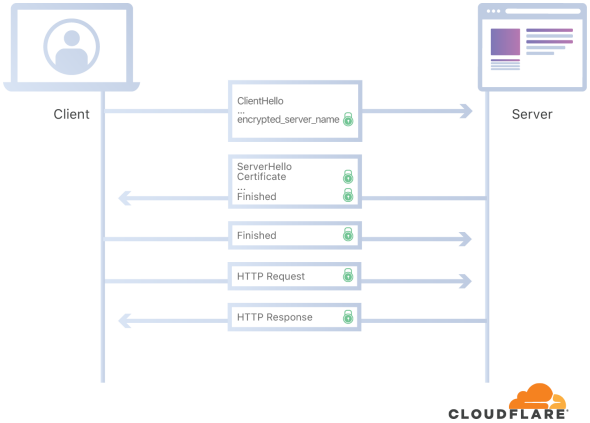
Källa: “Blocking-resistant communication through domain fronting” av Fifield et al., 2015

TLS 1.3 och krypterad SNI (extension)



Källa: https://blog.cloudflare.com/encrypted-sni/

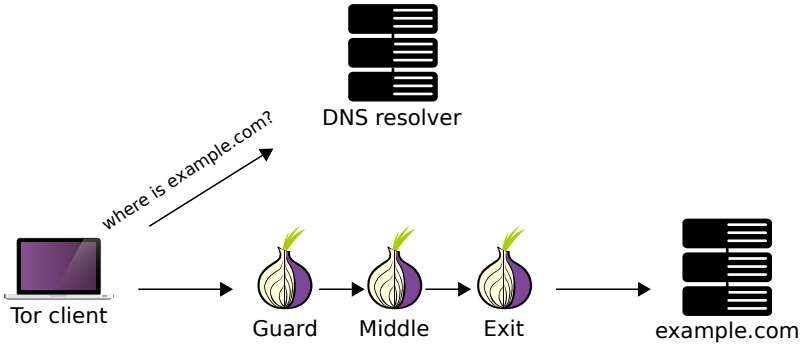
TLS 1.3 och krypterad SNI (extension)



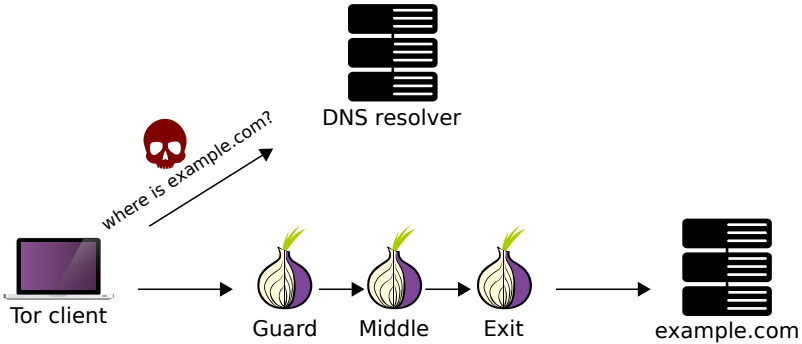
Källa: https://blog.cloudflare.com/encrypted-sni/

Tor och DNS

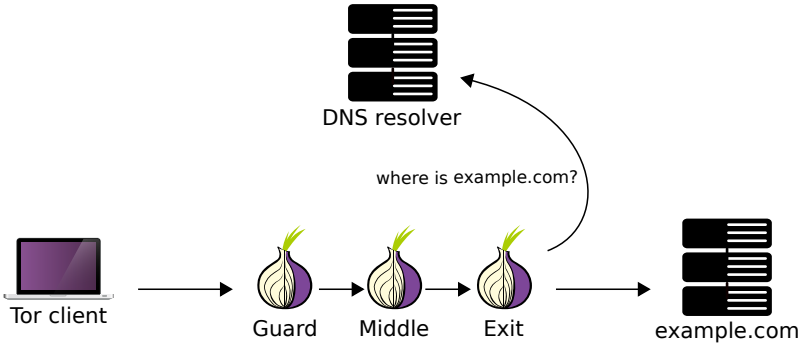
Tor och DNS


DNS resolver
where is example.com?
Tor client
Guard
Middle
Exit
example.com

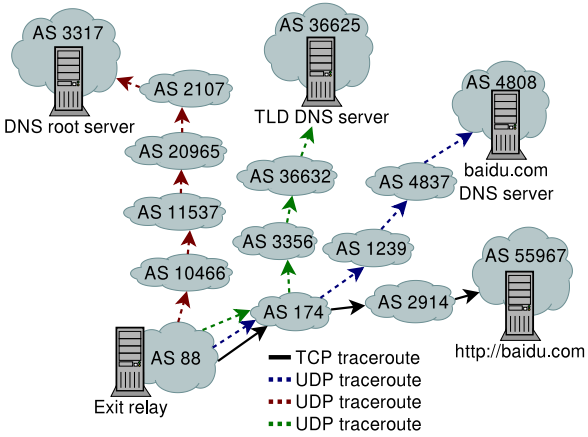
Tor och DNS


DNS resolver
where is example.com?
Tor client
Guard
Middle
Exit
example.com

Tor och DNS


DNS resolver
where is example.com?
Tor client
Guard
Middle
Exit
example.com

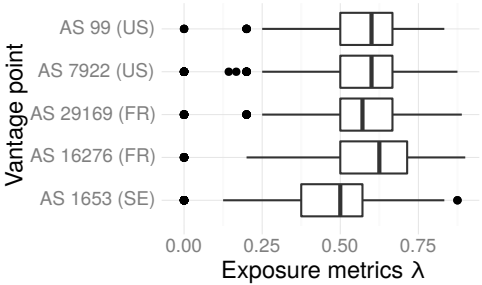
Hur mycket sprider sig DNS trafik?



Källa: "The Effect of DNS on Tor's Anonymity" av Greschbach et al., 2017

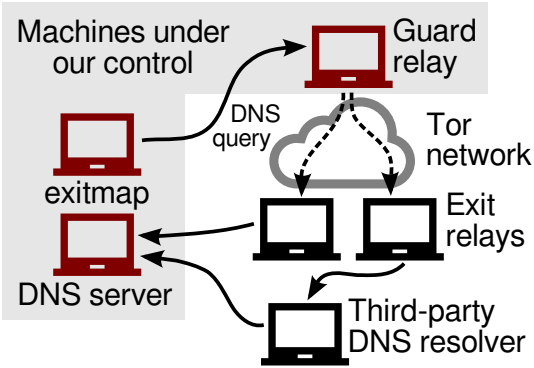
Hur mycket sprider sig DNS trafik?

- Alexa top 1,000
- från olika AS
- mått på utsatthet:
  - högre värde $\rightarrow$ mera DNS trafik
- AS med endast DNS trafik: 56%



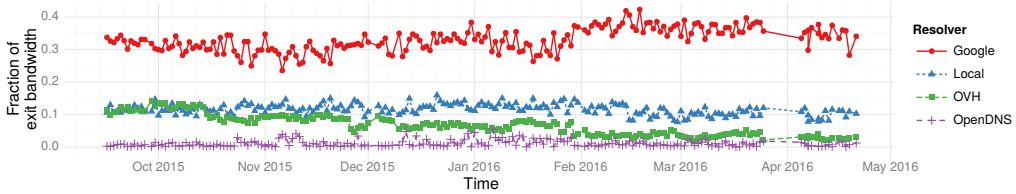
Källa: "The Effect of DNS on Tor's Anonymity" av Greschbach et al., 2017

Hur hanterar exits DNS förfrågningar?



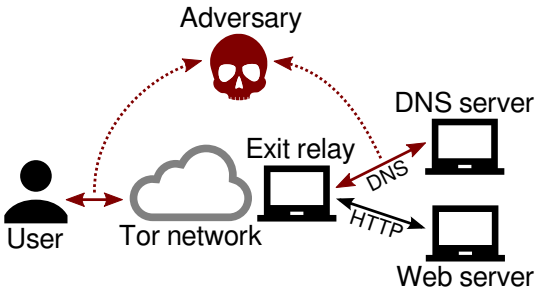
Källa: "The Effect of DNS on Tor's Anonymity" av Greschbach et al., 2017

Hur hanterar exits DNS förfrågningar?



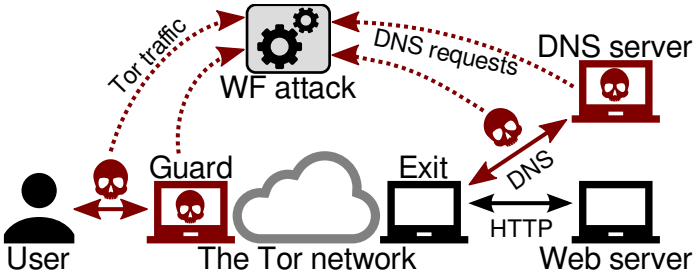
Källa: "The Effect of DNS on Tor's Anonymity" av Greschbach et al., 2017

Hur kan en attackerare använda sig av DNS?



Källa: "The Effect of DNS on Tor's Anonymity" av Greschbach et al., 2017

Hur kan en attackerare använda sig av DNS?



Källa: "The Effect of DNS on Tor's Anonymity" av Greschbach et al., 2017

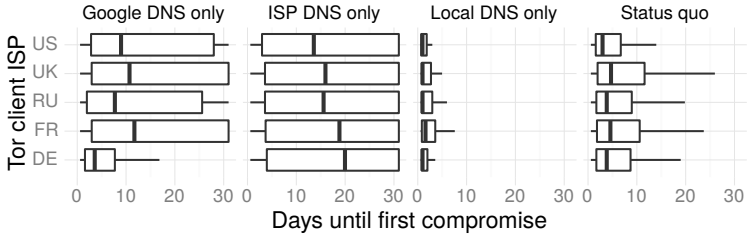
Tid till en AS attackerare vinner?

simulerade 100000 Tor klienter mars 2016, använde TorPS och RIPE Atlas noder

Källa: "The Effect of DNS on Tor's Anonymity" av Greschbach et al., 2017

Tid till en AS attackerare vinner?

simulerade 100000 Tor klienter mars 2016, använde TorPS och RIPE Atlas noder



Källa: "The Effect of DNS on Tor's Anonymity" av Greschbach et al., 2017

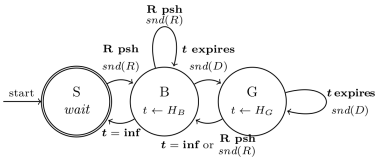
Just nu

Hur Tor ser på försvar

- konstant cellstorlek 512/514 bytes (paddning)
- netflow padding (CELL_PADDING varje 1.5-9.5s)
- från “Lokala säkerhetsarbetet på Kau” av Nicklas Lundqvist igår:

> På gång närmaste tiden
>
> • Test av visibilitetsprogramvara, Netflow test klart innan sommaren, nästa på tur Stealthwatch?

- jobbar på adaptive padding, men skeptiska



Källa: “Toward an Efficient Website Fingerprinting Defense” av Juarez et al., 2016

Projekt just nu på KAU

- CAT (Internetfonden / IIS)
- SURPRISE (SSF)

- Under granskning: PAF5G

pylls.github.io/CAT/

Sammanfattning & tack!