SPID

och
identifiering av obfuskerade protokoll

Erik Hjelmvik
< erik . hjelmvik [at] gmail . com >

Swedish Network Users' Society
Stockholm, 2010-09-29

Nätneutralitet #1

Definition #1 av nätverksneutralitet:

*Internetoperatören ska inom ramen för samma Internetaccesstjänst inte manipulera eller **nedprioritera datatrafiken** för en användare beroende på **innehåll**, ursprung eller destination,*

Källa: PTS-ER-2009:6 ”Nätneutralitet”

Nätneutralitet #2

Definition #2 av nätverksneutralitet:

*… den som tillhandahåller nättjänster **inte bör få blockera (eller ens prioritera)** enskilda **applikationer** eller innehåll.*

*Det handlar (i de flesta länder) inte huvudsakligen om censur utan snarare om att en Internetleverantör skulle spärra, eller försvåra möjligheterna för en konsument att konsumera konkurrerande innehållstjänster, exempelvis **försvåra för konsumenten att använda en IP- telefoni eller hyrvideotjänst** som konkurrerar med den som internetleverantören erbjuder i egen regi.*

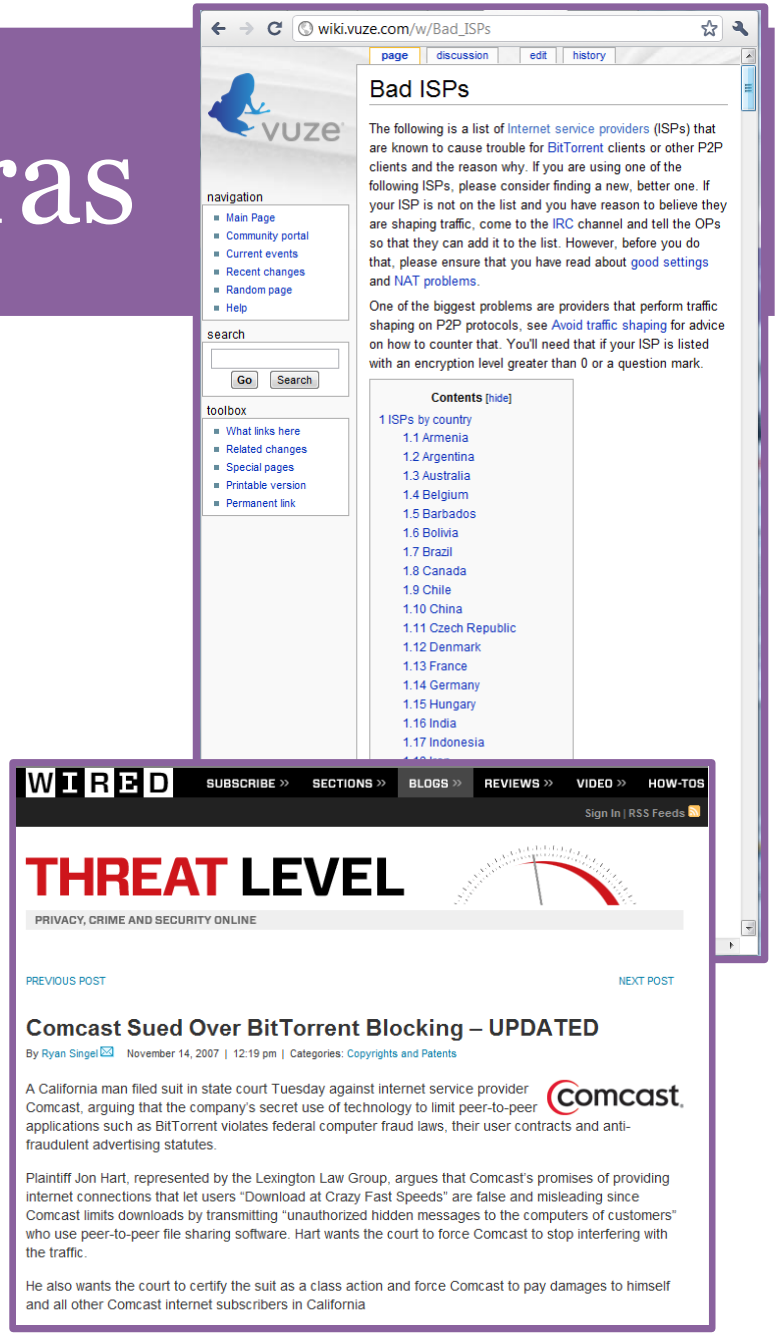
Källa: ”Nätverksneutralitet i Sverige – En summering av ett Teldok 2.0 seminarium”

Skype blockeras

- T-mobile:s blockering av Skype i Tyskland avslöjades 2009
- Många länder och företag köper utrustning för att blockera VoIP-trafik
  - Saudi Telecom
  - Giza Systems (Cairo)
  - Sydamerika
  - Asien
  - Europa

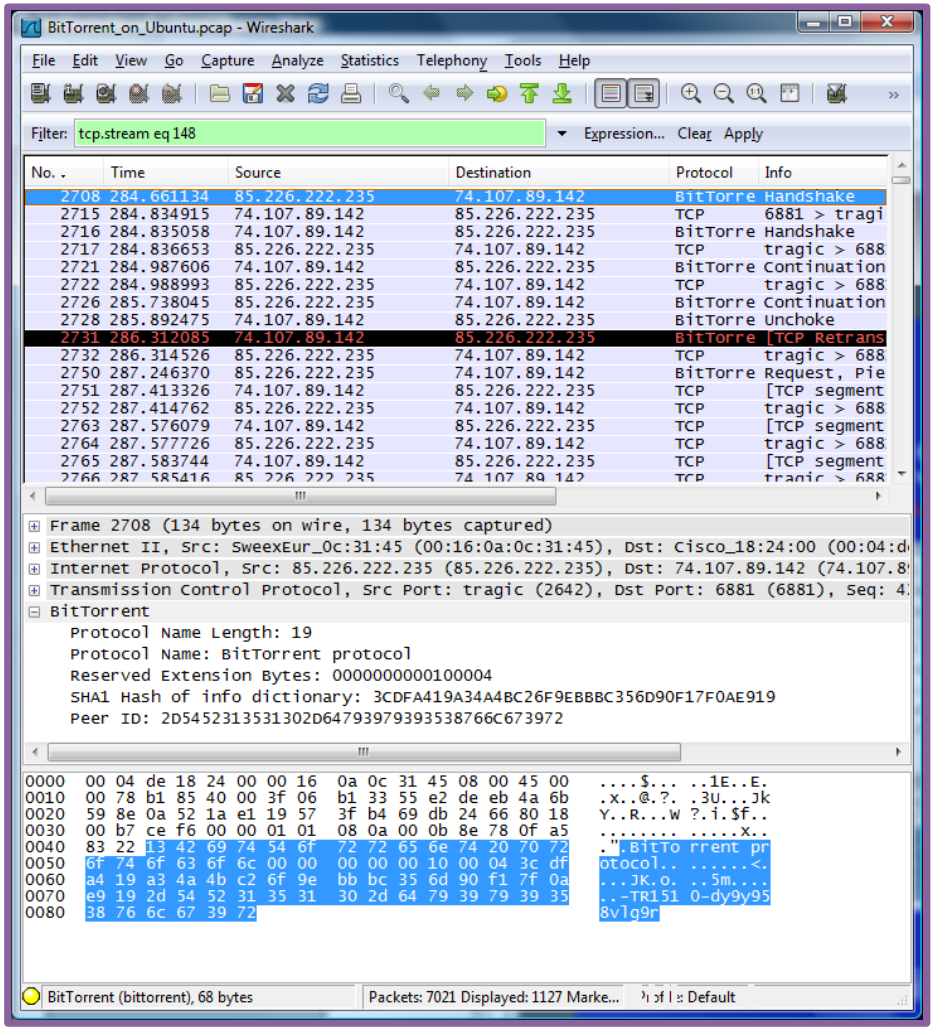
BitTorrent blockeras

- Över 70 ISP:er uppges begränsa BitTorrent-trafik i sina nät
- Comcast ”dödade” BitTorrent-trafik med TCP RST-paket under 2007



Traffic Classification

- Payload-signaturer med kända byte-sekvenser

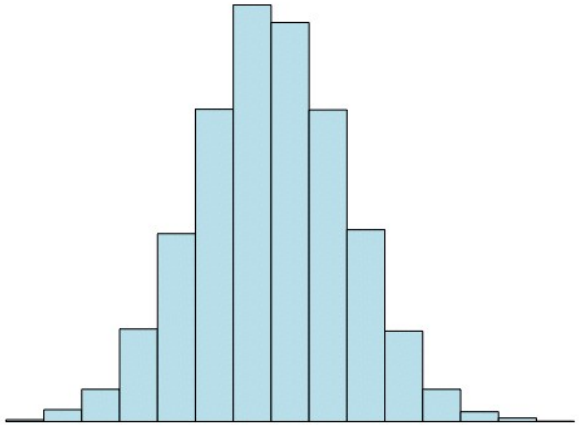


Motreaktion: obfuskerade protokoll

- Protokoll:
  - BitTorrents ”Message Stream Encryption” (MSE), även känt som ”Protocol Header Encryption”
  - eMule:s ”protocol encryption”
  - Skype använder ett obfuskerat protokoll
- Obfuskeringsmetoder:
  - Kryptera payload
  - Injicera BLOB:ar av slumpmässiga storlekar
  - Fragmentera data i TCP-paket med slumpmässig storlek

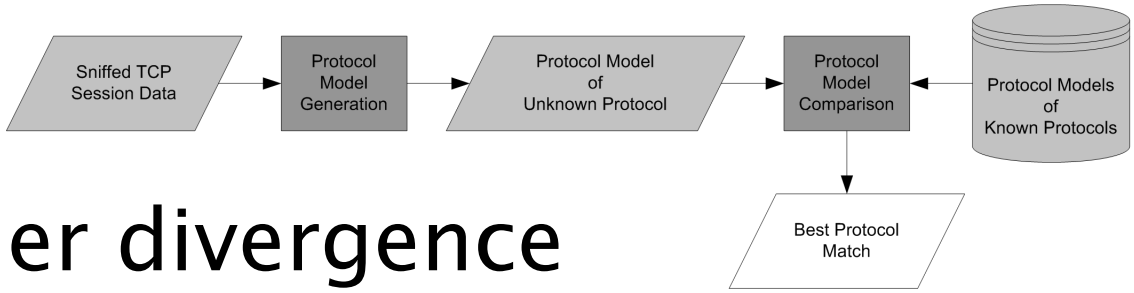
SPID?

Statistical Protocol IDentification



- Mäter 30 olika ”attribut” i nätverkstrafiken
  - Paketstorlekar
  - Riktningar på paket
  - Tid mellan paket
  - Payload i paket
  - Vanliga bit-sekvenser i payloaden
- Skapar statistiska ”fingerprints” för varje attribut
  - Sannolikhetsfördelningar av måtten
- Protokollmodel = Alla 30 fingerprints
- Jämför statistiska modeller från kända protokoll med observerade sessioner

Vaddå jämföra modeller?



- Kullback-Leibler divergence
  - Mäter ”avståndet” mellan två sannolikhetsfördelningar

$$D_{KL}(P_{attr}||Q_{attr,prot}) = \sum_i P_{attr}(i) * log \frac{P_{attr}(i)}{Q_{attr,prot}(i)}$$

P = observation
Q = modell

- Protokollmodellen med det minsta KL-avståndet är ”best match”

Analyserade protokoll

Protokoll	Källkod	Obfuskeringsmetod
MSE (Vuze + µTorrent)	Open Source	Obfuskerat Krypterat
Skype (TCP och UDP)	Proprietär	Krypterat *Obfuskerat?*
eDonkey Protocol Obfuscation (TCP och UDP)	Open Source	Obfuskerat Krypterat
Spotify (Server och Streaming)	Proprietär	Krypterat

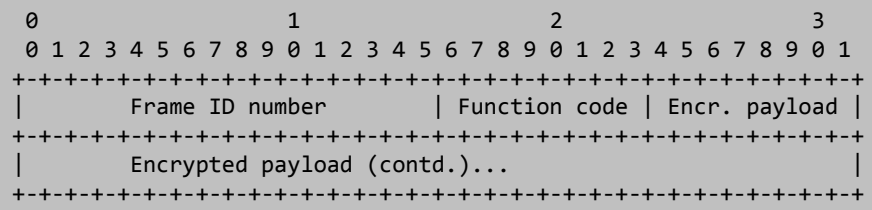
Klassificeringsresultat

Protocol	MSE	Skype TCP	Skype UDP	Spotify P2P	Spotify Server	Edonkey TCP Obfuscation	Edonkey UDP Obfuscation	13 other protocols	Unknown
MSE	0.963	0	0	0	0	0.002	0.003	0	0.032
Skype TCP	0.051	0.653	0	0	0.010	0.031	0.194	0.020	0.041
Skype UDP	0	0.001	0.767	0	0	0	0.001	0.001	0.230
Spotify P2P	0	0	0	0.913	0.039	0	0	0	0.049
Spotify Server	0	0	0	0	0.933	0	0	0	0.067
Edonkey TCP Obfuscation	0.047	0	0	0	0.002	0.910	0.005	0.009	0.026
Edonkey UDP Obfuscation	0.001	0.002	0.001	0	0	0.001	0.973	0.001	0.021

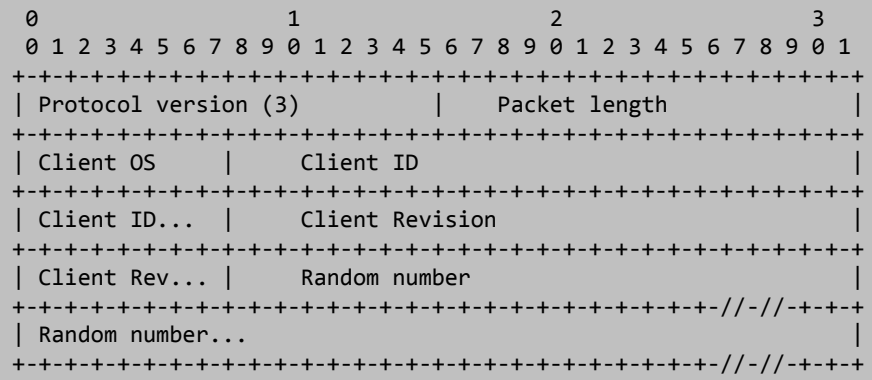
Vilka attribut kan mätas?

- Payload-meters funkade bra för protokoll med ingen eller dålig kryptering
  - Exempelvis Skype UDP och Spotify Server
- Paketstorlekar och riktningar fungerade bäst för obfuskerade protokoll
  - Bättre padding hade gjort detta omöjligt

Skype UDP:



Spotify Server (första paketet):



Reflektioner och tankar

- Bättre metoder för identifiering kommer att finnas även i kommersiella produkter
- Fler och bättre obfuskerade protokoll kommer att utvecklas
- Obfuskering försvårar även för andra
  - Internetforskning
  - Forensisk analys
  - Nätsäkerhetsprodukter: IDS / IPS
  - Utvecklare (komplex felsökning)

Länkar...

Ladda ner och prova SPID proof-of-concept:

http://sourceforge.net/projects/spid/

Läs min och Wolfgangs rapport ”Breaking and Improving Protocol Obfuscation”:

http://www.iis.se/docs/hjelmvik_breaking.pdf