

SPIID

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 Internetaccessstjänst 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



IEEE Spectrum INSIDE TECHNOLOGY MAGAZINE MULTIMEDIA
AEROSPACE BIOMEDICAL COMPUTING CONSUMER ELECTRONICS ENERGY

TELECOM / INTERNET
The VoIP Backlash
Internet-based telephony saved traditional carriers—but new services are making per-minute calls more expensive.
By STEVEN CHERRY / OCTOBER 2009

World children's festivals!
Kate Nash, an American girl singer, is in Germany.

News Travel Lifestyle Restaurants NEW Galleries Jobs Dating Discussion
National Business & Money Politics Sci & Tech Society Sport Offbeat Opinion

Sign up for the editor's weekly newsletter

The Local
GERMANY'S NEWS IN ENGLISH

T-Mobile 3G
SMS
21:30
2

T-Mobile blocks Skype for German iPhones
Published: 31 Mar 09 17:03 CET

German telecommunications giant T-Mobile will not allow its customers to use the new Skype application for the iPhone, the company told The Local on Tuesday.

- Government ministers warned not to use BlackBerrys and iPhones - Science & Technology (8 Aug 10)
- Deutsche Telekom Q2 hit by loss of T-Mobile UK - Business & Money (5 Aug 10)
- Minister demands Apple transparency - National (26 Jun 10)

The internet telephony (VoIP) service Skype allows users to make telephone calls for free, or at least significantly more cheaply than traditional telephone providers. There have been several unofficial applications for mobile devices in use for some time, but the first official iPhone application for the service launched on Tuesday – free of charge – to a host of excited media chatter.

BitTorrent blockeras

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



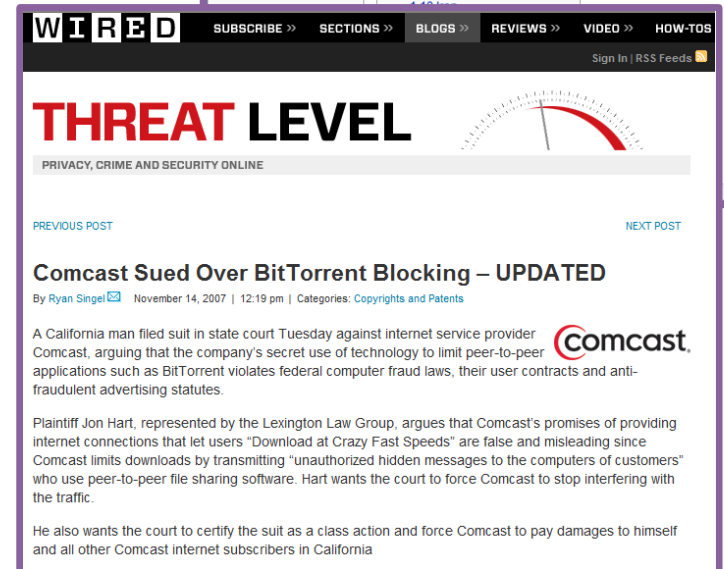
Bad ISPs

The following is a list of [Internet service providers](#) (ISPs) that are known to cause trouble for [BitTorrent](#) clients or other P2P clients and the reason why. If you are using one of the following ISPs, please consider finding a new, better one. If your ISP is not on the list and you have reason to believe they are shaping traffic, come to the [IRC](#) channel and tell the OPs so that they can add it to the list. However, before you do that, please ensure that you have read about [good settings](#) and [NAT problems](#).

One of the biggest problems are providers that perform traffic shaping on P2P protocols, see [Avoid traffic shaping](#) for advice on how to counter that. You'll need that if your ISP is listed with an encryption level greater than 0 or a question mark.

Contents [hide]

1 ISPs by country
1.1 Armenia
1.2 Argentina
1.3 Australia
1.4 Belgium
1.5 Barbados
1.6 Bolivia
1.7 Brazil
1.8 Canada
1.9 Chile
1.10 China
1.11 Czech Republic
1.12 Denmark
1.13 France
1.14 Germany
1.15 Hungary
1.16 India
1.17 Indonesia



WIRED SUBSCRIBE >> SECTIONS >> BLOGS >> REVIEWS >> VIDEO >> HOW-TOS

Sign In | RSS Feeds

THREAT LEVEL

PRIVACY, CRIME AND SECURITY ONLINE

PREVIOUS POST NEXT POST

Comcast Sued Over BitTorrent Blocking – UPDATED

By [Ryan Singel](#) November 14, 2007 | 12:19 pm | Categories: [Copyrights and Patents](#)

A California man filed suit in state court Tuesday against internet service provider Comcast, arguing that the company's secret use of technology to limit peer-to-peer applications such as BitTorrent violates federal computer fraud laws, their user contracts and anti-fraudulent advertising statutes.

Plaintiff Jon Hart, represented by the Lexington Law Group, argues that Comcast's promises of providing internet connections that let users "Download at Crazy Fast Speeds" are false and misleading since Comcast limits downloads by transmitting "unauthorized hidden messages to the computers of customers" who use peer-to-peer file sharing software. Hart wants the court to force Comcast to stop interfering with the traffic.

He also wants the court to certify the suit as a class action and force Comcast to pay damages to himself and all other Comcast internet subscribers in California

Traffic Classification

- Payload-signaturer med kända byte-sekvenser



IPOQUE



No.	Time	Source	Destination	Protocol	Info
2708	284.661134	85.226.222.235	74.107.89.142	BitTorre	Handshake
2715	284.834915	74.107.89.142	85.226.222.235	TCP	6881 > tragic
2716	284.835058	74.107.89.142	85.226.222.235	BitTorre	Handshake
2717	284.836653	85.226.222.235	74.107.89.142	TCP	tragic > 688
2721	284.987606	74.107.89.142	85.226.222.235	BitTorre	Continuation
2722	284.988993	85.226.222.235	74.107.89.142	TCP	tragic > 688
2726	285.738045	85.226.222.235	74.107.89.142	BitTorre	Continuation
2728	285.892475	74.107.89.142	85.226.222.235	BitTorre	Unchoke
2731	286.312085	74.107.89.142	85.226.222.235	BitTorre	[TCP Retrans]
2732	286.314526	85.226.222.235	74.107.89.142	TCP	tragic > 688
2750	287.246370	85.226.222.235	74.107.89.142	BitTorre	Request, Pie
2751	287.413326	74.107.89.142	85.226.222.235	TCP	[TCP segment
2752	287.414762	85.226.222.235	74.107.89.142	TCP	tragic > 688
2763	287.576079	74.107.89.142	85.226.222.235	TCP	[TCP segment
2764	287.577726	85.226.222.235	74.107.89.142	TCP	tragic > 688
2765	287.583744	74.107.89.142	85.226.222.235	TCP	[TCP segment
2766	287.585416	85.226.222.235	74.107.89.142	TCP	tragic > 688

Frame 2708 (134 bytes on wire, 134 bytes captured)
Ethernet II, Src: SweexEur_Oc:31:45 (00:16:0a:0c:31:45), Dst: Cisco_18:24:00 (00:04:d...
Internet Protocol, Src: 85.226.222.235 (85.226.222.235), Dst: 74.107.89.142 (74.107.8...
Transmission Control Protocol, Src Port: tragic (2642), Dst Port: 6881 (6881), Seq: 4...
BitTorrent
Protocol Name Length: 19
Protocol Name: BitTorrent protocol
Reserved Extension Bytes: 000000000100004
SHA1 Hash of info dictionary: 3CDF419A34A4BC26F9EBBC356D90F17F0AE919
Peer ID: 2D5452313531302D64793979393538766C673972

```
0000 00 04 de 18 24 00 00 16 0a 0c 31 45 08 00 45 00 ....$....1E..E.  
0010 00 78 b1 85 40 00 3f 06 b1 33 55 e2 de eb 4a 6b .x.@.?..3U...Jk  
0020 59 8e 0a 52 1a e1 19 57 3f b4 69 db 24 66 80 18 Y..R...W?.i.$f..  
0030 00 b7 ce f6 00 00 01 01 08 0a 00 0b 8e 78 0f a5 .....X..  
0040 83 22 13 42 69 74 54 6f 72 72 65 6e 74 20 70 72 ..BitTo rrent pr  
0050 6f 74 6f 63 6f 6c 00 00 00 00 00 10 00 04 3c df otocol.....<  
0060 a4 19 a3 4a 4b c2 6f 9e bb bc 35 6d 90 f1 7f 0a ...JK.o...5m...  
0070 e9 19 2d 54 52 31 35 31 30 2d 64 79 39 79 39 35 ..-TR151 0-dy9y95  
0080 38 76 6c 67 39 72 8vl9r
```

Motreaktion: obfuskerade protokoll

- Protokoll:

- BitTorrents "Message Stream Encryption" (MSE), även känt som "Protocol Header Encryption"
- eMule:s "protocol encryption"
- Skype använder ett obfuskerat protokoll

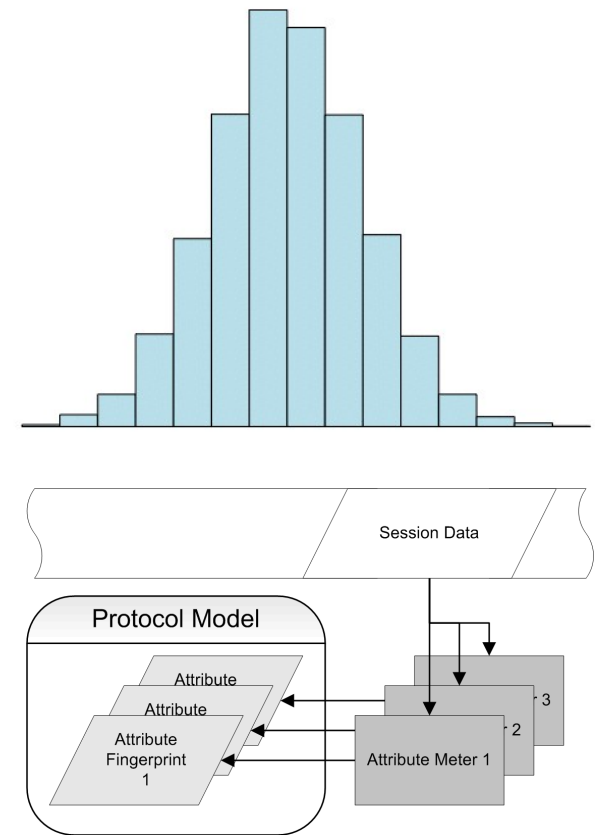
- Obfuskeringsmetoder:

- Kryptera payload
- Injicera BLOB:ar av slumpmässiga storlekar
- Fragmentera data i TCP-paket med slumpmässig storlek

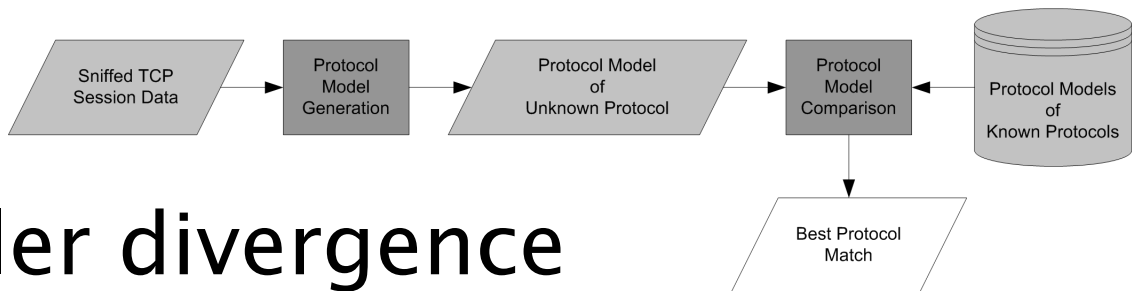
SPID?

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
- Protokollmodell = 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 <i>Obfuskerat?</i>
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:

```
0                               1                               2                               3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+++++-----+-----+-----+-----+-----+-----+-----+-----+
|           Frame ID number           | Function code | Encr. payload |
+++++-----+-----+-----+-----+-----+-----+-----+-----+
|           Encrypted payload (contd.)...           |
+++++-----+-----+-----+-----+-----+-----+-----+-----+
```

Spotify Server (första paketet):

```
0                               1                               2                               3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+++++-----+-----+-----+-----+-----+-----+-----+-----+
| Protocol version (3)           | Packet length |
+++++-----+-----+-----+-----+-----+-----+-----+-----+
| Client OS           | Client ID |
+++++-----+-----+-----+-----+-----+-----+-----+-----+
| Client ID...       | Client Revision |
+++++-----+-----+-----+-----+-----+-----+-----+-----+
| Client Rev...     | Random number |
+++++-----+-----+-----+-----+-----+-----+-----+-----+
| Random number...   |
+++++-----+-----+-----+-----+-----+-----+-----+-----+
```

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