P2P File-Sharing in Hell: Exploiting BitTorrent Vulnerabilities to Launch Distributed Reflective DoS Attacks

Florian Adamsky, Syed Ali Khayam, Rudolf Jäger and Muttukrishnan Rajarajan

florian-woot15@adamsky.it
http://florian.adamsky.it/

9th USENIX Workshop on Offensive Technologies

Outline

Table of Contents

2013: DDoS attack record: 300 Gbps

ars technica

MAIN MENU ▾ MY STORIES: 25 ▾ FORUMS SUBSCRIBE JOBS ARS CONSORTIUM

Ars Technica has arrived in Europe. **Check it out!** ×

RISK ASSESSMENT / SECURITY & HACKTIVISM

Spamhaus DDoS grows to Internet-threatening size

More than 300 Gb/s of traffic aimed at the anti-spam site's hosting.

by **Peter Bright** - Mar 27, 2013 8:30pm CET

Share Tweet 268

LATEST FROM ARS TECHNICA/UK

NI HAO MARIO

China finally lifts 15-year ban on manufacture and sale of games consoles

UK government admits that MPs aren't safe from GCHQ's mass snooping

Someone has finally made a portable Bluetooth speaker that doesn't suck

BECAUSE WE CAN

2014: DDoS attack record: 400 Gbps

ars technica

MAIN MENU ▾ MY STORIES: 0 ▾ FORUMS SUBSCRIBE JOBS ARS CONSORTIUM

Ars Technica has arrived in Europe. **Check it out!** ×

RISK ASSESSMENT / SECURITY & HACKTIVISM

Biggest DDoS ever aimed at Cloudflare's content delivery network

Network Time Protocol attack reached 400Gbps.

by **Sean Gallagher** - Feb 11, 2014 6:12pm CET

Share Tweet 59

LATEST FROM ARS TECHNICA/UK

NI HAO MARIO

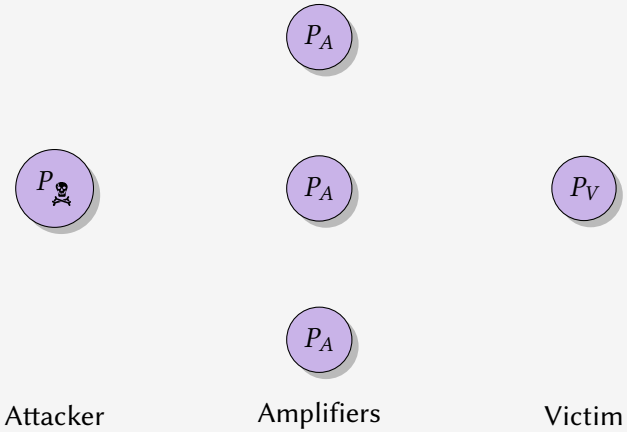
China finally lifts 15-year ban on manufacture and sale of games consoles

UK government admits that MPs aren't safe from GCHQ's mass snooping

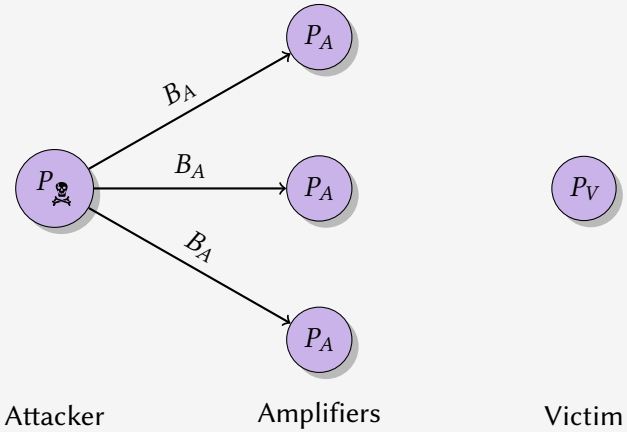
Someone has finally made a portable Bluetooth speaker that doesn't suck

BECAUSE WE CAN

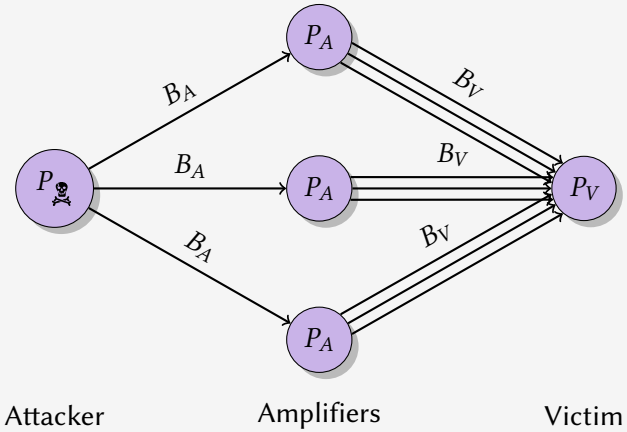
DRDoS Attacks Thread Model



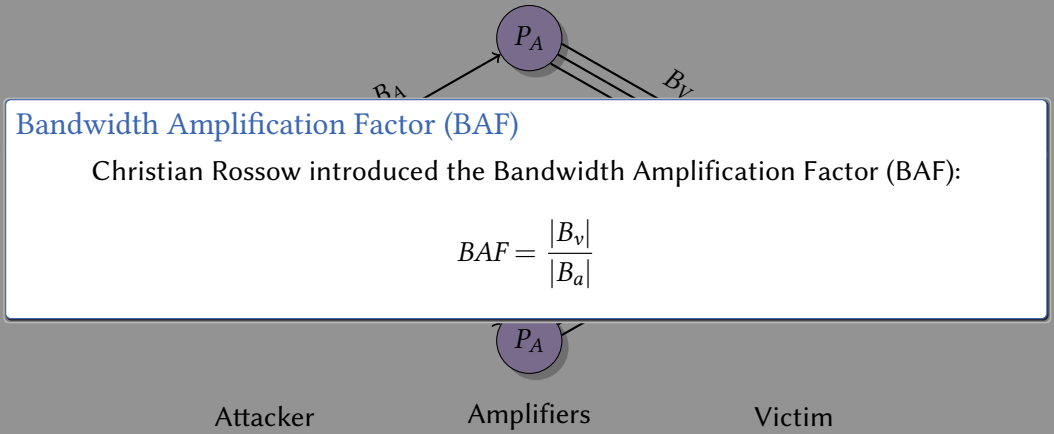
DRDoS Attacks Thread Model



DRDoS Attacks Thread Model



DRDoS Attacks Thread Model

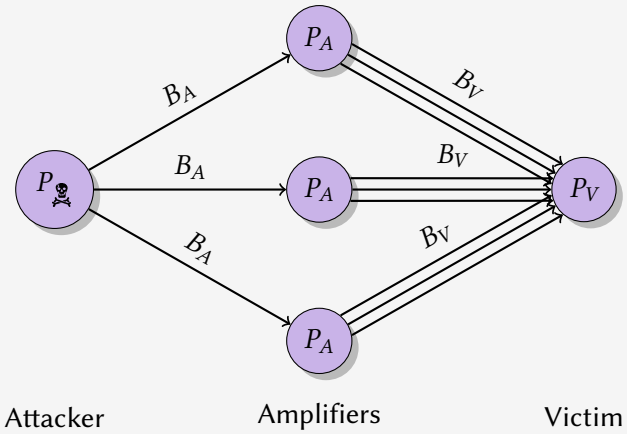


Bandwidth Amplification Factor (BAF)

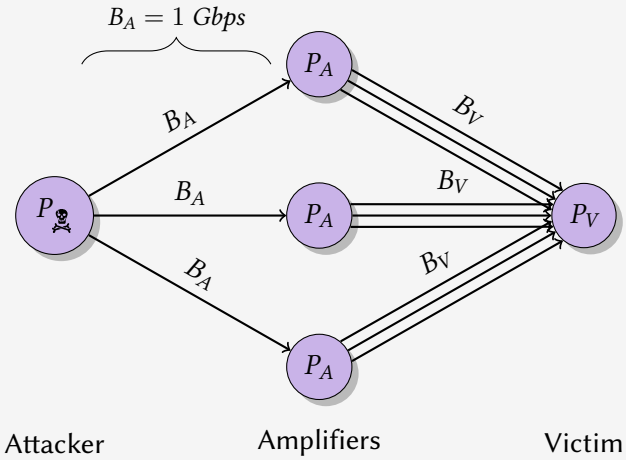
Christian Rossow introduced the Bandwidth Amplification Factor (BAF):

$$BAF = \frac{|B_v|}{|B_a|}$$

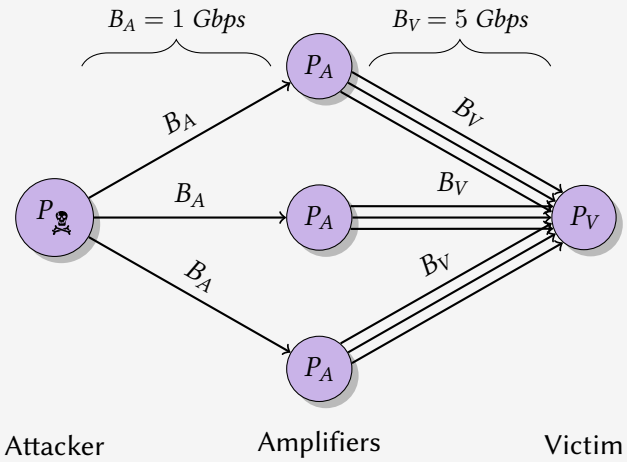
Example: BAF = 5



Example: BAF = 5



Example: BAF = 5



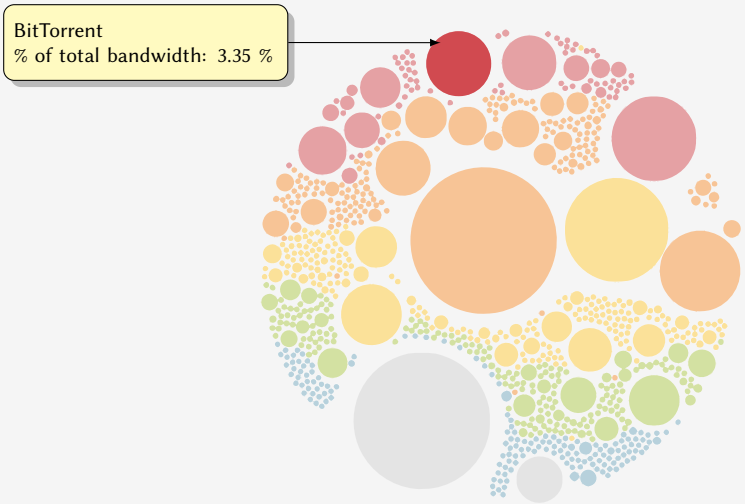
Advantages of a DRDoS Attack

- Attacker hides his own identity
- It can be initiated by a single computer, results in a distributed attack
- Amplifiers send a larger packet to the victim and therefore increase the impact of the attack

Worldwide Application Usage

Source: Paloalto Networks

Worldwide Application Usage



Source: Paloalto Networks

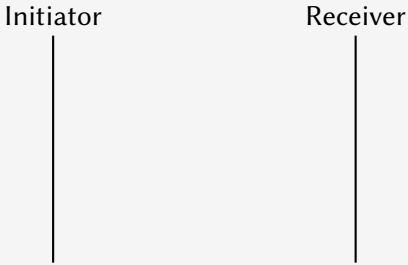
BitTorrent's protocol overview

- Variety of UDP-based protocols are used:
  - Distributed Hash Table (DHT)
  - Micro Transport Protocol (uTP)

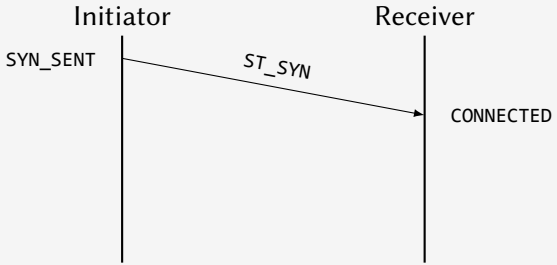
Micro Transport Protocol (uTP)

- uTP is a reliable transport protocol which makes use of UDP
- Similarities to TCP
  - Window based flow control
  - Sequence numbers and ACK numbers
- Differences to TCP
  - Sequence numbers and ACKs refer to packets, not bytes
  - No congestion control (Slow-start, congestion avoidance, ...) $\rightarrow$ LEDBAT
  - Two-way handshake instead of a three-way handshake

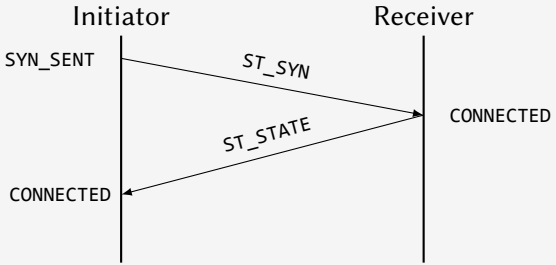
uTP's two-way handshake



uTP's two-way handshake



uTP's two-way handshake



uTP's two-way handshake

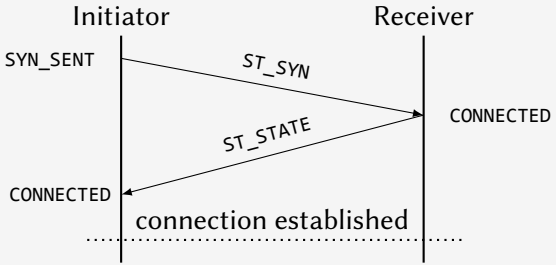


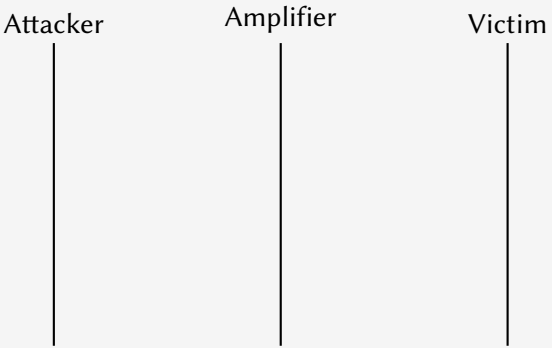
Table of Contents

BitTorrent Handshake

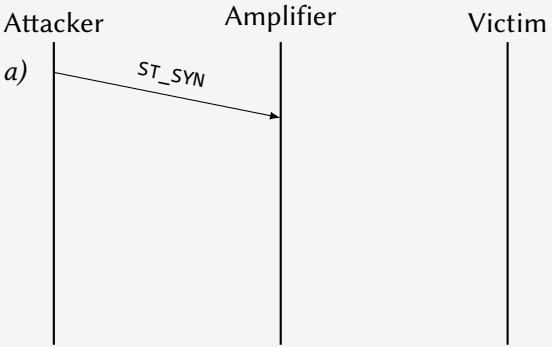
`<pstrlen><pstr><extensions><info_hash><peer_id>`

- `pstrlen` = 19
- `pstr` = *BitTorrent protocol*
- `extensions` 8 bytes reserved
- `info_hash` 20 byte
- `peer_id` 20 byte

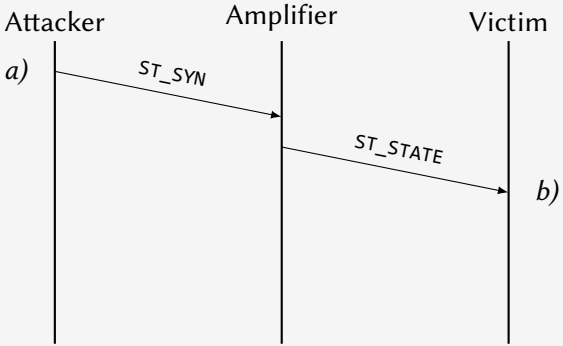
Exploiting uTP's two-way handshake



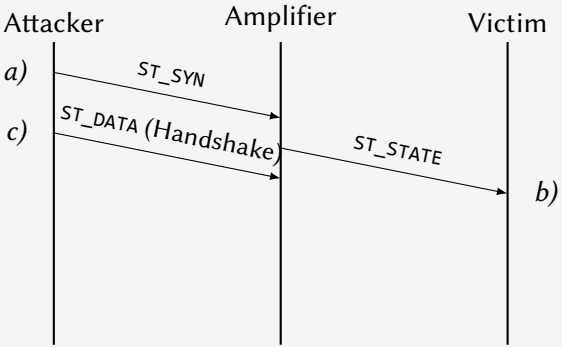
Exploiting uTP's two-way handshake



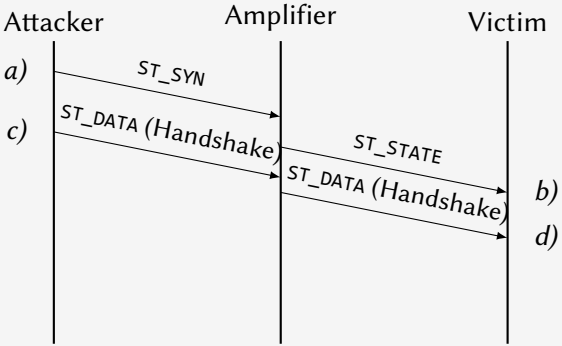
Exploiting uTP's two-way handshake



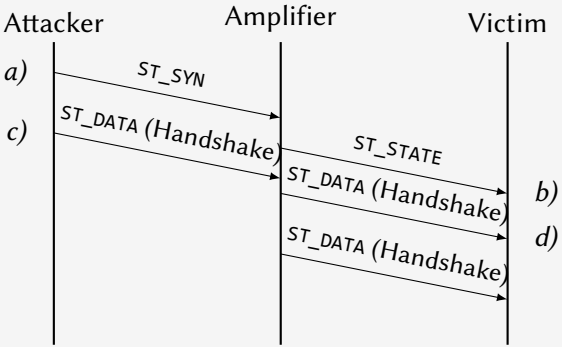
Exploiting uTP's two-way handshake



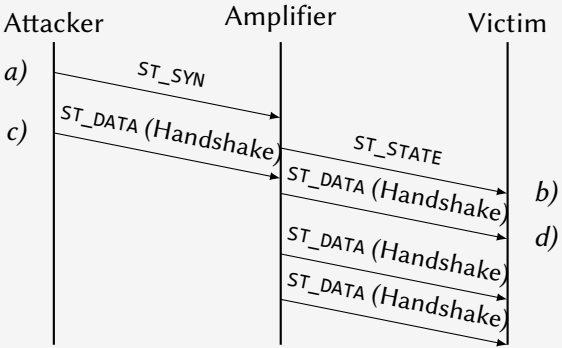
Exploiting uTP's two-way handshake



Exploiting uTP's two-way handshake



Exploiting uTP's two-way handshake



$B_V > B_A$

Definition (Packet Stuffing)

Try to cram as much BitTorrent messages into one packet as possible to minimize the connection establishment protocol flow

Amplification Factors (BitTorrent)

Description	BAF	PAF
ucat	351.5	6
uTorrent w/o extensions	27.6	3.5
Mainline w/o extensions	27.8	3.5
uTorrent with LTEP	39.6	3
Mainline with LTEP	39.6	3
Vuze w/o extensions	13.9	2
Vuze with LTEP	18.7	2
Vuze with AMP	54.3	3.5
Transmission w/o extensions	4.0	3.5
Transmission with LTEP	4.0	3.5
Transmission with AMP	4.0	3.5
Libtorrent w/o extensions	5.2	4
Libtorrent with LTEP	5.2	4

Amplification Factors (BitTorrent)

Description	BAF	PAF
ucat	351.5	6
uTorrent w/o extensions	27.6	3.5
Mainline w/o extensions	27.8	3.5
uTorrent with LTEP	39.6	3
Mainline with LTEP	39.6	3
Vuze w/o extensions	13.9	2
Vuze with LTEP	18.7	2
Vuze with AMP	54.3	3.5
Transmission w/o extensions	4.0	3.5
Transmission with LTEP	4.0	3.5
Transmission with AMP	4.0	3.5
Libtorrent w/o extensions	5.2	4
Libtorrent with LTEP	5.2	4

Amplification Factors (BitTorrent)

Description	BAF	PAF
ucat	351.5	6
uTorrent w/o extensions	27.6	3.5
Mainline w/o extensions	27.8	3.5
uTorrent with LTEP	39.6	3
Mainline with LTEP	39.6	3
Vuze w/o extensions	13.9	2
Vuze with LTEP	18.7	2
Vuze with AMP	54.3	3.5
Transmission w/o extensions	4.0	3.5
Transmission with LTEP	4.0	3.5
Transmission with AMP	4.0	3.5
Libtorrent w/o extensions	5.2	4
Libtorrent with LTEP	5.2	4

Amplification Factors (BitTorrent)

Description	BAF	PAF
ucat	351.5	6
uTorrent w/o extensions	27.6	3.5
Mainline w/o extensions	27.8	3.5
uTorrent with LTEP	39.6	3
Mainline with LTEP	39.6	3
Vuze w/o extensions	13.9	2
Vuze with LTEP	18.7	2
Vuze with AMP	54.3	3.5
Transmission w/o extensions	4.0	3.5
Transmission with LTEP	4.0	3.5
Transmission with AMP	4.0	3.5
Libtorrent w/o extensions	5.2	4
Libtorrent with LTEP	5.2	4

Amplification Factors (BitTorrent)

Description	BAF	PAF
ucat	351.5	6
uTorrent w/o extensions	27.6	3.5
Mainline w/o extensions	27.8	3.5
uTorrent with LTEP	39.6	3
Mainline with LTEP	39.6	3
Vuze w/o extensions	13.9	2
Vuze with LTEP	18.7	2
Vuze with AMP	54.3	3.5
Transmission w/o extensions	4.0	3.5
Transmission with LTEP	4.0	3.5
Transmission with AMP	4.0	3.5
Libtorrent w/o extensions	5.2	4
Libtorrent with LTEP	5.2	4

Amplification Factors (BitTorrent)

Description	BAF	PAF
ucat	351.5	6
uTorrent w/o extensions	27.6	3.5
Mainline w/o extensions	27.8	3.5
uTorrent with LTEP	39.6	3
Mainline with LTEP	39.6	3
Vuze w/o extensions	13.9	2
Vuze with LTEP	18.7	2
Vuze with AMP	54.3	3.5
Transmission w/o extensions	4.0	3.5
Transmission with LTEP	4.0	3.5
Transmission with AMP	4.0	3.5
Libtorrent w/o extensions	5.2	4
Libtorrent with LTEP	5.2	4

Amplification Factors (BitTorrent)

Description	BAF	PAF
ucat	351.5	6
uTorrent w/o extensions	27.6	3.5
Mainline w/o extensions	27.8	3.5
uTorrent with LTEP	39.6	3
Mainline with LTEP	39.6	3
Vuze w/o extensions	13.9	2
Vuze with LTEP	18.7	2
Vuze with AMP	54.3	3.5
Transmission w/o extensions	4.0	3.5
Transmission with LTEP	4.0	3.5
Transmission with AMP	4.0	3.5
Libtorrent w/o extensions	5.2	4
Libtorrent with LTEP	5.2	4

Amplification Factors (BitTorrent)

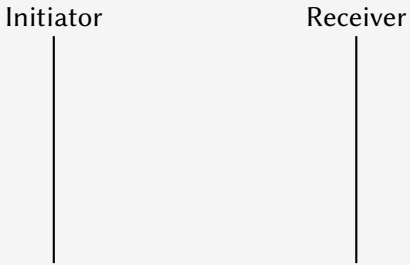
Description	BAF	PAF
ucat	351.5	6
uTorrent w/o extensions	27.6	3.5
Mainline w/o extensions	27.8	3.5
uTorrent with LTEP	39.6	3
Mainline with LTEP	39.6	3
Vuze w/o extensions	13.9	2
Vuze with LTEP	18.7	2
Vuze with AMP	54.3	3.5
Transmission w/o extensions	4.0	3.5
Transmission with LTEP	4.0	3.5
Transmission with AMP	4.0	3.5
Libtorrent w/o extensions	5.2	4
Libtorrent with LTEP	5.2	4

Message Stream Encryption (MSE)

- Aim of MSE is to obfuscate BitTorrent traffic to avoid shaping
- MSE starts a Diffie-Hellman key exchange
- After the key exchange BitTorrent packets are RC4 encrypted

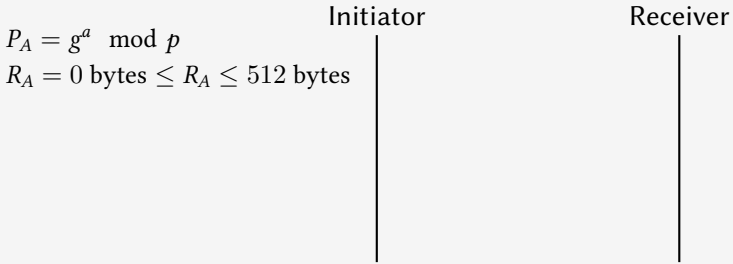
Message Stream Encryption (MSE)

- Aim of MSE is to obfuscate BitTorrent traffic to avoid shaping
- MSE starts a Diffie-Hellman key exchange
- After the key exchange BitTorrent packets are RC4 encrypted



Message Stream Encryption (MSE)

- Aim of MSE is to obfuscate BitTorrent traffic to avoid shaping
- MSE starts a Diffie-Hellman key exchange
- After the key exchange BitTorrent packets are RC4 encrypted

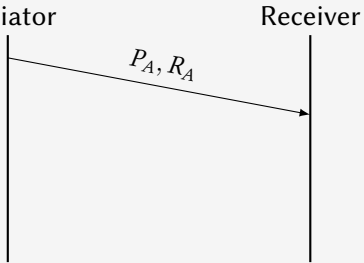


Message Stream Encryption (MSE)

- Aim of MSE is to obfuscate BitTorrent traffic to avoid shaping
- MSE starts a Diffie-Hellman key exchange
- After the key exchange BitTorrent packets are RC4 encrypted

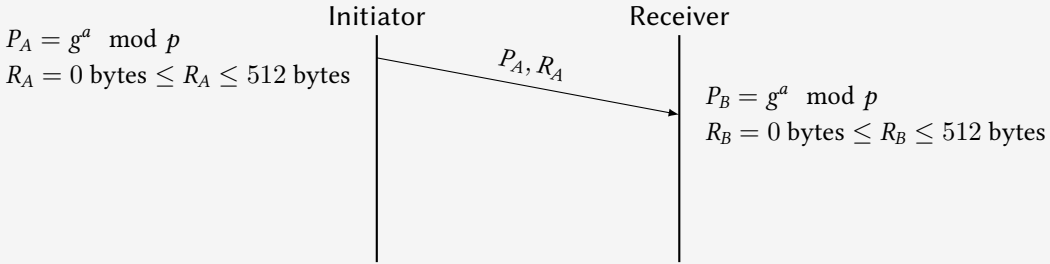
$P_A = g^a \mod p$

$R_A = 0 \text{ bytes} \leq R_A \leq 512 \text{ bytes}$



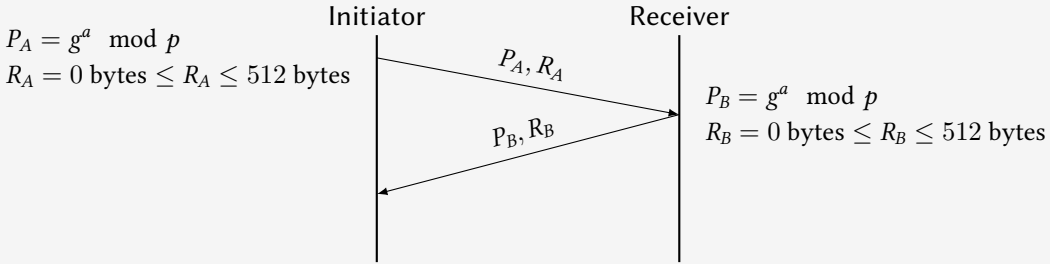
Message Stream Encryption (MSE)

- Aim of MSE is to obfuscate BitTorrent traffic to avoid shaping
- MSE starts a Diffie-Hellman key exchange
- After the key exchange BitTorrent packets are RC4 encrypted



Message Stream Encryption (MSE)

- Aim of MSE is to obfuscate BitTorrent traffic to avoid shaping
- MSE starts a Diffie-Hellman key exchange
- After the key exchange BitTorrent packets are RC4 encrypted

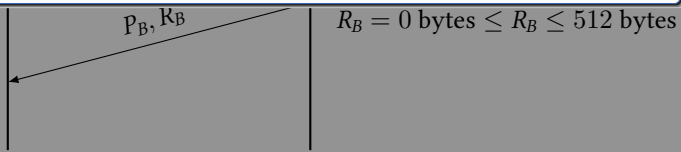


Message Stream Encryption (MSE)

- Aim of MSE is to obfuscate BitTorrent traffic to avoid shaping
- MSE starts a Diffie-Hellman key exchange
- After the key exchange BitTorrent packets are RC4 encrypted

Amplification Factor (MSE)

$$4 \leq BAF_{MSE} \leq 32.5$$



Distributed Hash Table

- DHT implementation in BitTorrent is divided into two protocols:
  - Mainline DHT (MLDHT)
  - Vuze DHT (VDHT)
- MLDHT is by far the biggest overlay network (around 15–27 million users per day)
- Both protocols are not compatible with each other

Amplification Factors (DHT)

Implementation	Description	BAF
MLDHT	`ping`	0.8
	`find_node` with $K = 8$	3.1
	`get_peers` with 100 peers (IPv4)	11.9
	`get_peers` with 100 peers (IPv6)	24.5
	`get_peers` with scrapes	13.4
VDHT	`ping`	0.8
	`ping` with Vivaldi coordinates	14.9

Amplification Factors (DHT)

Implementation	Description	BAF
MLDHT	`ping`	0.8
	`find_node` with $K = 8$	3.1
	`get_peers` with 100 peers (IPv4)	11.9
	`get_peers` with 100 peers (IPv6)	24.5
	`get_peers` with scrapes	13.4
VDHT	`ping`	0.8
	`ping` with Vivaldi coordinates	14.9

Amplification Factors (DHT)

Implementation	Description	BAF
MLDHT	`ping`	0.8
	`find_node` with $K = 8$	3.1
	`get_peers` with 100 peers (IPv4)	11.9
	`get_peers` with 100 peers (IPv6)	24.5
	`get_peers` with scrapes	13.4
VDHT	`ping`	0.8
	`ping` with Vivaldi coordinates	14.9

Amplification Factors (DHT)

Implementation	Description	BAF
MLDHT	`ping`	0.8
	`find_node` with $K = 8$	3.1
	`get_peers` with 100 peers (IPv4)	11.9
	`get_peers` with 100 peers (IPv6)	24.5
	`get_peers` with scrapes	13.4
VDHT	`ping`	0.8
	`ping` with Vivaldi coordinates	14.9

BitTorrent Sync

- Proprietary protocol to synchronize files in a P2P way
- BTSync reached the 1 million users mark in 2013
- BTSync also uses uTP as its transport protocol

Amplification Vulnerabilities (BTSync)

Message	BAF
BTSync handshake	10.8
`ping`	120

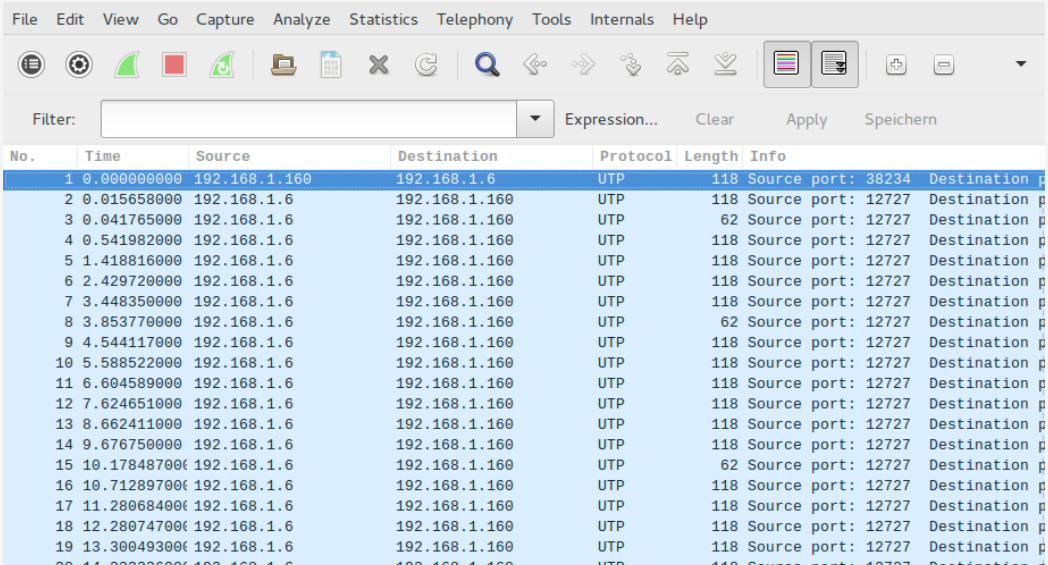
Amplification Vulnerabilities (BTSync)

Message	BAF
BTSync handshake	10.8
`ping`	120

Amplification Vulnerabilities (BTSync)

Message	BAF
BTSync handshake	10.8
`ping`	120

BTSync: ping flood



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.1.160	192.168.1.6	UTP	118	Source port: 38234 Destination p
2	0.015658000	192.168.1.6	192.168.1.160	UTP	118	Source port: 12727 Destination p
3	0.041765000	192.168.1.6	192.168.1.160	UTP	62	Source port: 12727 Destination p
4	0.541982000	192.168.1.6	192.168.1.160	UTP	118	Source port: 12727 Destination p
5	1.418816000	192.168.1.6	192.168.1.160	UTP	118	Source port: 12727 Destination p
6	2.429720000	192.168.1.6	192.168.1.160	UTP	118	Source port: 12727 Destination p
7	3.448350000	192.168.1.6	192.168.1.160	UTP	118	Source port: 12727 Destination p
8	3.853770000	192.168.1.6	192.168.1.160	UTP	62	Source port: 12727 Destination p
9	4.544117000	192.168.1.6	192.168.1.160	UTP	118	Source port: 12727 Destination p
10	5.588522000	192.168.1.6	192.168.1.160	UTP	118	Source port: 12727 Destination p
11	6.604589000	192.168.1.6	192.168.1.160	UTP	118	Source port: 12727 Destination p
12	7.624651000	192.168.1.6	192.168.1.160	UTP	118	Source port: 12727 Destination p
13	8.662411000	192.168.1.6	192.168.1.160	UTP	118	Source port: 12727 Destination p
14	9.676750000	192.168.1.6	192.168.1.160	UTP	118	Source port: 12727 Destination p
15	10.17848700(	192.168.1.6	192.168.1.160	UTP	62	Source port: 12727 Destination p
16	10.71289700(	192.168.1.6	192.168.1.160	UTP	118	Source port: 12727 Destination p
17	11.28068400(	192.168.1.6	192.168.1.160	UTP	118	Source port: 12727 Destination p
18	12.28074700(	192.168.1.6	192.168.1.160	UTP	118	Source port: 12727 Destination p
19	13.30049300(	192.168.1.6	192.168.1.160	UTP	118	Source port: 12727 Destination p

Evadability

	DNS'13	NTP'14	BTH	MLDHT	VDHT	BTSync	MSE
SPI firwall	X	X					
DPI firewall			X	X	X	X	

Table of Contents

Experimental Evaluation

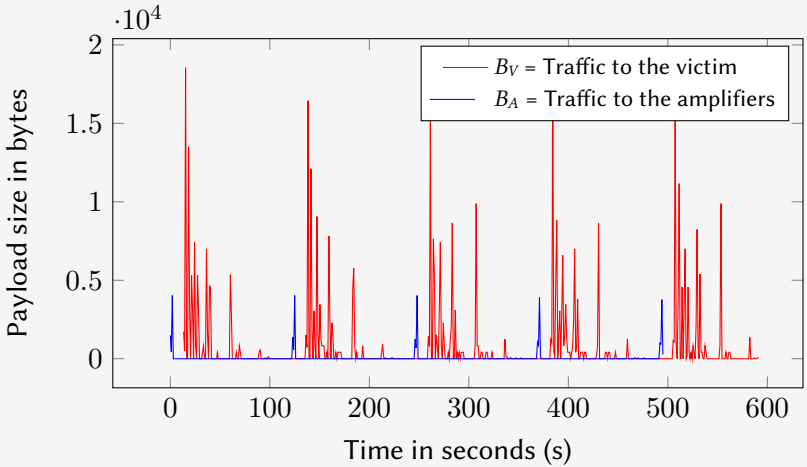
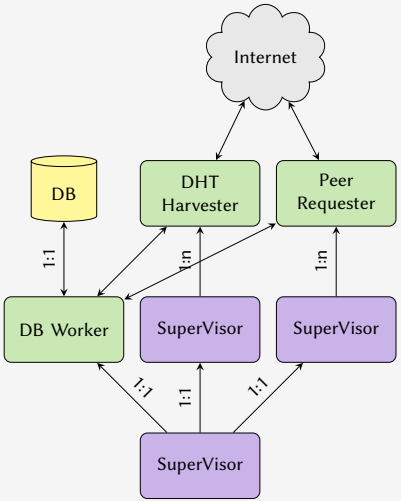


Figure: Amplification attack with 1 attacker, 31 amplifiers and 1 victim.

BitTorrent Crawler

- We wrote a BitTorrent Crawler in Elixir
- Used PirateBay magnet link database from Feb 2012
- We collected overall 9.6 million peers via MLDHT
  - Beginning from 1st January 2015 until 1st February 2015.



Payload size from the DHT responses

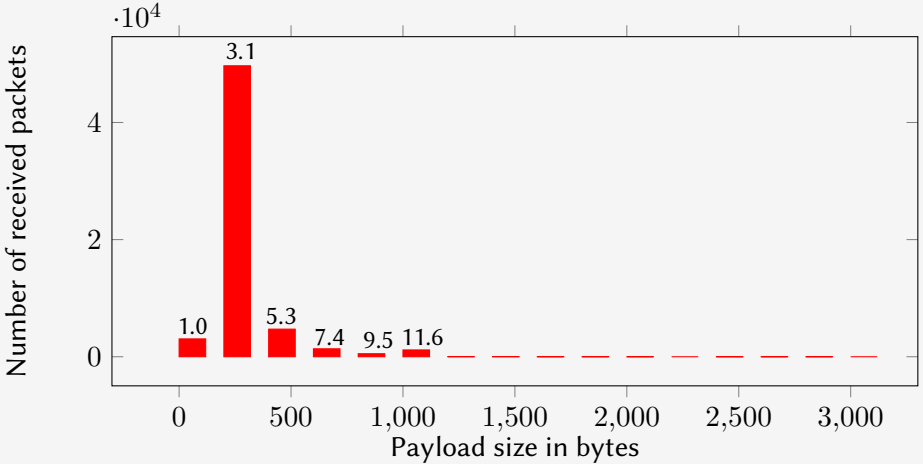


Figure: Histogram of the payload size from the DHT responses which are caused by `get_peers` requests. The numbers on top of the bars are the average BAF values.

BitTorrent handshake size from the uTP responses

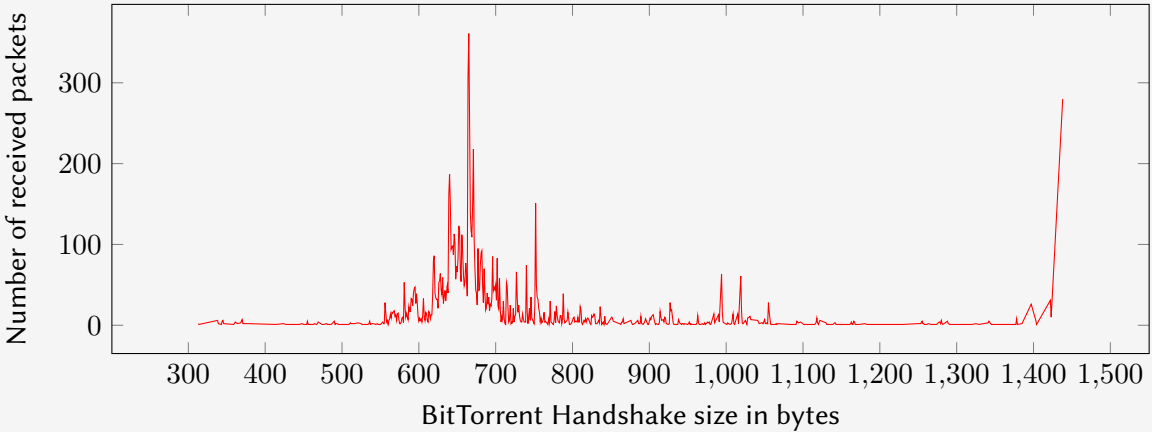


Figure: Histogram of the BitTorrent handshake size from the uTP responses.

BitTorrent handshake size from the uTP responses

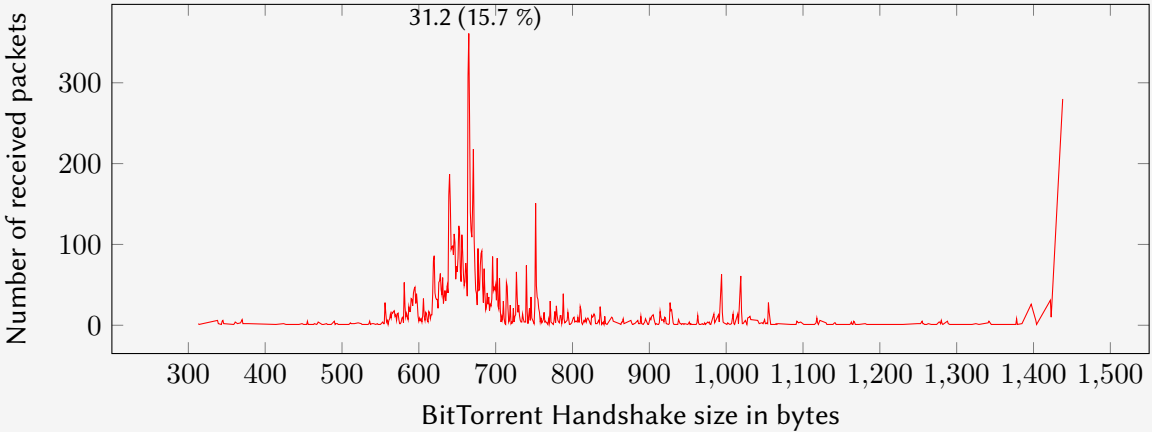


Figure: Histogram of the BitTorrent handshake size from the uTP responses.

BitTorrent handshake size from the uTP responses

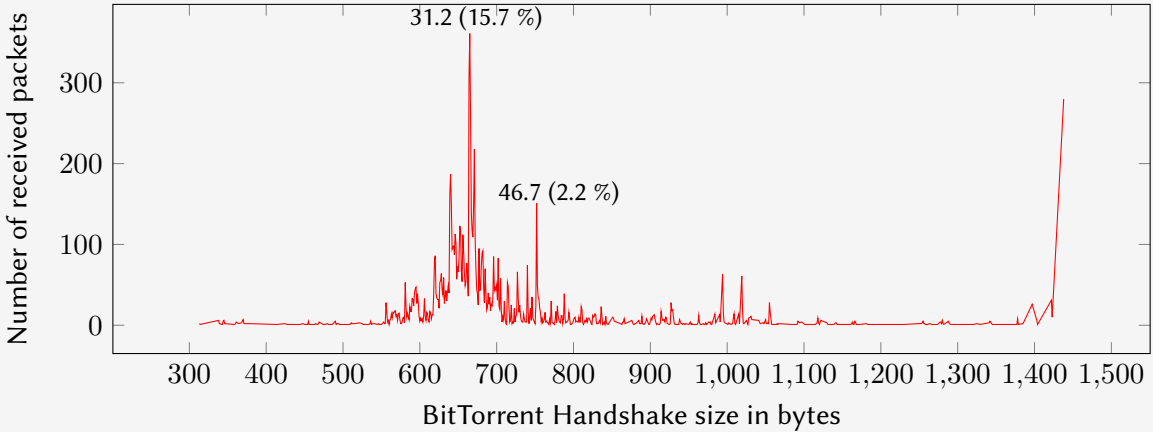


Figure: Histogram of the BitTorrent handshake size from the uTP responses.

BitTorrent handshake size from the uTP responses

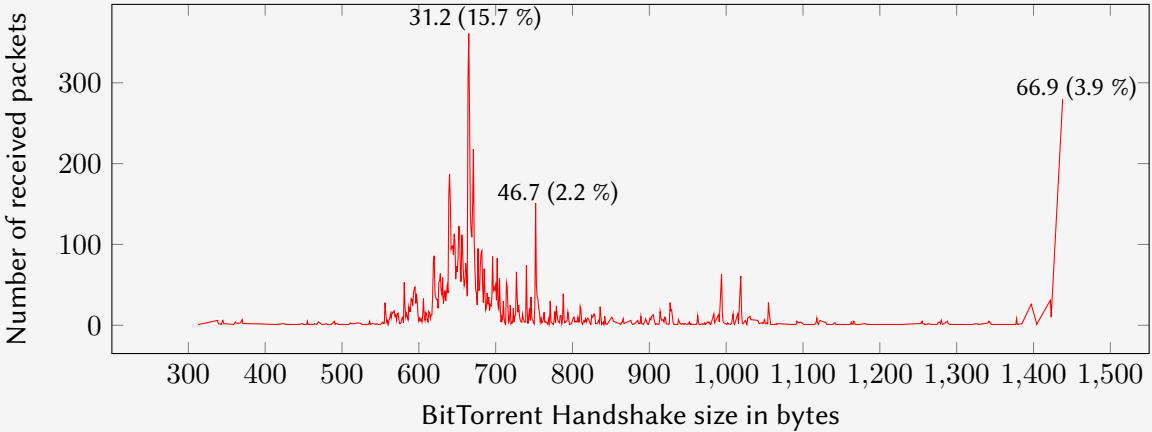


Figure: Histogram of the BitTorrent handshake size from the uTP responses.

Table of Contents

Coutermeasures

ISP side

- BCP 38 (ingress filtering)
  - 2015: more than 70 % of the public networks deployed BCP 38

Coutermeasures

ISP side

- BCP 38 (ingress filtering)
  - 2015: more than 70 % of the public networks deployed BCP 38

Protocol side

- uTP
  - Three-way handshake
  - Verify the second acknowledgment
- DHT
  - Token scheme (similar to `announce_peer`)

Conclusion

- BitTorrent and BitTorrent Sync are vulnerable to DRDoS attacks
- Attacker is able to amplify traffic up to 50 times and with BTSync up to 120 times
- With Trackers, DHT and PEX, an attacker can collect millions of amplifiers
- Hard to circumvent, as the found vulnerabilities can only be defended with a DPI firewall
  - in case of MSE it is even harder

Conclusion

- BitTorrent and BitTorrent Sync are vulnerable to DRDoS attacks
- Attacker is able to amplify traffic up to 50 times and with BTSync up to 120 times
- With Trackers, DHT and PEX, an attacker can collect millions of amplifiers
- Hard to circumvent, as the found vulnerabilities can only be defended with a DPI firewall
  - in case of MSE it is even harder

Responsible Disclosure

uTorrent 3.4.4 49854 (beta) is released today!

Thank You

Questions?

florian-woot15@adamsky.it
http://florian.adamsky.it/

Institutions:

CITY UNIVERSITY LONDON

PLUMgrid

THM
TECHNISCHE HOCHSCHULE MITTELHESSEN