The Arms Race in P2P

Tactics and Counter-Tactics in the War Between Peer-to-Peer File Sharers, Copyright Holders, and ISPs

Kevin Bauer    Dirk Grunwald    Douglas Sicker

University of Colorado
Context: The Rise of Peer-to-Peer

1993-2000: Early Internet saw mostly web traffic

2000-: Peer-to-peer (P2P) protocols like Gnutella, FastTrack, Napster, & BitTorrent becoming popular for file sharing

2006-Present: P2P traffic now most common

Source: CacheLogic Research
January 2006
Content Dissemination Models

• Traditional client/server model
  – Users (*clients*) contact a **centralized server** to retrieve content (webpage)

• Peer-to-peer (P2P) model
  – Users (*peers*) contact **each other** to retrieve content
  – *Advantages*: Decentralization, fault-tolerance, content availability, fast data dissemination
  – Common applications: Streaming media, voice-over-IP (VoIP), and **file sharing**
Current P2P Landscape

P2P still most common protocol class today

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Southern Africa</th>
<th>South America</th>
<th>Eastern Europe</th>
<th>Northern Africa</th>
<th>Germany</th>
<th>Southern Europe</th>
<th>Middle East</th>
<th>Southwestern Europe</th>
</tr>
</thead>
<tbody>
<tr>
<td>All P2P</td>
<td>65,77%</td>
<td>65,21%</td>
<td>69,95%</td>
<td>42,51%</td>
<td>52,79%</td>
<td>55,12%</td>
<td>44,77%</td>
<td>54,46%</td>
</tr>
<tr>
<td>Ares</td>
<td>0,29%</td>
<td>42,63%</td>
<td>0,00%</td>
<td>2,24%</td>
<td>0,84%</td>
<td>0,16%</td>
<td>0,11%</td>
<td>1,80%</td>
</tr>
<tr>
<td>BitTorrent</td>
<td>48,34%</td>
<td>30,02%</td>
<td>80,83%</td>
<td>74,51%</td>
<td>70,77%</td>
<td>48,94%</td>
<td>78,85%</td>
<td>58,20%</td>
</tr>
<tr>
<td>DirectConnect</td>
<td>0,01%</td>
<td>0,00%</td>
<td>17,87%</td>
<td>0,08%</td>
<td>0,85%</td>
<td>0,00%</td>
<td>0,12%</td>
<td>0,30%</td>
</tr>
<tr>
<td>eDonkey</td>
<td>2,48%</td>
<td>25,99%</td>
<td>1,16%</td>
<td>7,70%</td>
<td>24,22%</td>
<td>47,17%</td>
<td>15,37%</td>
<td>35,99%</td>
</tr>
<tr>
<td>Gnutella</td>
<td>18,60%</td>
<td>0,36%</td>
<td>0,14%</td>
<td>14,21%</td>
<td>1,75%</td>
<td>1,66%</td>
<td>5,00%</td>
<td>2,75%</td>
</tr>
<tr>
<td>iMesh</td>
<td>13,60%</td>
<td>0,02%</td>
<td>0,00%</td>
<td>0,47%</td>
<td>0,00%</td>
<td>0,03%</td>
<td>0,00%</td>
<td>0,14%</td>
</tr>
<tr>
<td>Thunder</td>
<td>14,04%</td>
<td>0,80%</td>
<td>0,00%</td>
<td>0,69%</td>
<td>0,77%</td>
<td>1,64%</td>
<td>0,52%</td>
<td>0,62%</td>
</tr>
<tr>
<td>Other</td>
<td>2,64%</td>
<td>0,19%</td>
<td>0,00%</td>
<td>0,10%</td>
<td>0,68%</td>
<td>0,41%</td>
<td>0,03%</td>
<td>0,21%</td>
</tr>
</tbody>
</table>

Source: Ipoque Internet Study 2008/2009

BitTorrent dominates P2P around the world
Problems That P2P File Sharing Causes

• Peers act as both **consumers** and **providers** of content
  – Problem of network management: This behavior consumes a lot of *(upload)* bandwidth
  – **Bad for Internet service providers (ISPs)**

• P2P networks often distribute **copyright-protected content** (illegally)
  – Problem of enforcing copyright: It’s difficult to stop sharing from both a technical and a legal perspective
  – **Bad for copyright holders**

→ ISPs and copyright holders have mutual incentive to mitigate P2P file sharing
Talk Outline

Overview of BitTorrent

The arms race - Phase 1: *De-incentivize P2P*
- ISPs’ past tactics to disrupt BitTorrent
- Copyright holders’ past tactics to reduce file sharing

The arms race - Phase 2: *File sharers’ counter-tactics*
- BitTorrent protocol encryption
- Anonymous communications

The arms race - Phase 3: *Emerging tactics*

Conclusion and Policy Implications
Sharing a File with BitTorrent

• Steps to share a file with BitTorrent

1. Break original file into several fixed-size pieces (i.e., 256 KB or 1 MB)

2. Compute a SHA1 hash for each piece to ensure integrity

3. Create a torrent metafile: Piece size, number of pieces, hashes, URI of tracker server

“Torrent” metadata file

Tracker: http://tracker.host.com:8080/announce
File length: 256 MB
Piece size: 1 MB
Number of pieces: 256
Sharing a File with BitTorrent (2)

• To download the file:
  1. Download the desired torrent file
  2. Contact the tracker and obtain list of other peers

  Who is sharing this file?

128.138.207.2, 182.203.21.4, ...

3. Request pieces from the other peers

I want piece #23
Here’s piece #23

I want piece #94
Here’s piece #94

Peer Tracker server
BitTorrent File Transfer in Detail

**Downloader (“Leecher”)**

I’d like to download part of the file from you

These are the pieces I currently have

I’m interested in some pieces you have

Can I have piece #104?

**Uploader (“Seeder”)**

OK

OK, and these are the pieces I currently have

OK, go ahead and ask for pieces

Ok, here’s piece #104...
Talk Outline

Overview of BitTorrent ✓

The arms race - Phase 1: De-incentivize P2P
• ISPs’ past tactics to disrupt BitTorrent
• Copyright holders’ past tactics to reduce file sharing

The arms race - Phase 2: File sharers’ counter-tactics
• BitTorrent protocol encryption
• Anonymous communications

The arms race - Phase 3: Emerging tactics

Conclusion and Policy Implications
Past ISP Tactics

- Identify BitTorrent application-layer header within packets in the network
  - Easy because BitTorrent usually operates in plaintext

**BitTorrent is easy to identify:**

- Throttle or block BitTorrent traffic using forged TCP reset packets (*i.e.*, “Sandvine”)
BitTorrent manipulation by ISPs is a world-wide phenomenon

How common is BitTorrent traffic manipulation by ISPs?

~100,000 users from around the world tested their ISPs (3/2008 – 1/2009)

Over **4,500** hosts observed BitTorrent blocking by their ISPs **(shown in red)**

[Dischinger et al., ACM Internet Measurement Conference 2008]
Regulators’ Reaction to Protocol Specific Traffic Interference

• Issues of network neutrality, lack of transparency, and potential anti-competitive motives

• In August 2008, the FCC ruled that Comcast “had unduly interfered with Internet users’ right to access the lawful Internet content and to use applications of their choice.”

[FCC Press Release; August 1, 2008]
Past Copyright-Holder Tactics

Copyright holders (MPAA and RIAA) have incentive to mitigate lost revenue resulting from piracy

Conduct investigations to identify peers

1. Investigators query trackers for peers’ IP addresses

2. Issue DMCA take-down notices to each IP address (or pursue legal action)

[Piatek et al., USENIX Workshop on Hot Topics in Security (HotSec) 2008]
Tracker list queries can be inaccurate

• Querying tracker lists can give many false positives
  – *i.e.*, stale tracker information, open wireless access point
• Trackers use a simple HTTP mechanism to register new peers; often possible to register arbitrary IP addresses

Register an arbitrary IP address **A.B.C.D**:

```
wget 'http://torrentstorage.com/announce.php
?info_hash=%E8%BC%89%A4B%24%28%26%269F%3B%265CC%265B%261%267%263%261%265
rpbVcq&port=55746&uploaded=0&downloaded=0&left=366039040&event=started&numwant=50&no_peer_id=1&compact=1&ip=A.B.C.D&key=NfBFoSCo'
```

Source: Piatek *et al.* HotSec ‘08
Talk Outline

Overview of BitTorrent ✓

The arms race - Phase 1: De-incentivize P2P ✓
- ISPs’ past tactics to disrupt BitTorrent
- Copyright holders’ past tactics to reduce file sharing

The arms race - Phase 2: File sharers’ counter-tactics
- BitTorrent protocol encryption
- Anonymous communications

The arms race - Phase 3: Emerging tactics

Conclusion and Policy Implications
Defeating Traffic Shaping with BitTorrent Encryption

- BitTorrent offers **Message Stream Encryption**
  - Obfuscates the protocol header (and payload) to defeat traffic identification and throttling

**Step 1:** Establish shared secret key $S_k$, authenticated by info_hash

**Step 2:** Exchange RC4 **encrypted** protocol messages

**Limitations:**
1. Weak authentication
2. Integrity not verified
Tor provides anonymity for TCP by tunneling traffic through a virtual circuit of three Tor routers using layered encryption.
Can BitTorrent Users Hide with Tor?

• We characterized how Tor is used in practice and observed significant BitTorrent traffic over a four day observation period

[McCoy et al., Privacy Enhancing Technologies Symposium 2008]
Can BitTorrent Users Hide with Tor?

• BitTorrent is using a disproportionate amount of Tor’s available bandwidth

[McCoy et al., Privacy Enhancing Technologies Symposium 2008]
Talk Outline

Overview of BitTorrent ✓

The arms race - Phase 1: *De-incentivize P2P* ✓
• ISPs’ past tactics to disrupt BitTorrent
• Copyright holders’ past tactics to reduce file sharing

The arms race - Phase 2: *File sharers’ counter-tactics*
• BitTorrent protocol encryption
• Anonymous communications

The arms race - Phase 3: *Emerging tactics*

Conclusion and Policy Implications
Virtual Private Network Anonymizers

• One-hop anonymous VPN services (BTGuard, iPredator) are now available for BitTorrent

**Limitations of centralized VPN approach:**
1. Technically feasible to know and disclose both client and destination
2. Vulnerable to legal pressure
BitBlender: Anonymity within BitTorrent

- BitBlender achieves *plausible deniability* for peers who are listed by a tracker → enhances users’ privacy
- Achieved by introducing “relay peers” to proxy piece requests and replies for other peers

[Image of peer-to-peer network with Alice, Robert, Relay, Mallory, MediaDefender, SafeNet, and BAY:TSP]

[Robert is sharing the file]

[Who is sharing?]

[Tracker server]

[Could be a file sharer or a relay – can’t tell]

[Bauer et al., Workshop on Applications of Private and Anonymous Communications 2008]
Plausible Deniability with SwarmScreen

Establish random connections to hide Alice’s *true* downloading habits

- Like BitBlender, attempts to provide privacy by “plausible deniability”, but achieves it by participating in random torrents
- Uses tunable parameter called *(SwarmScreen Protection Factor)* SPF that determines degree of privacy
- Plug-in for Vuze available

F2F File Sharing with OneSwarm

- **Key observation:** P2P participation is public knowledge
- “Friend-to-friend” (F2F) network: Files are shared *only with your friends*, leverages social network relationships
- Request for file is routed through other friends to hide the requestor and data is sent through reverse links to requester to hide data source

[Istdal et al., University of Washington-CSE Technical report. February, 2009]
Speculation: Partnerships Between ISPs and Copyright Holders?

• ISPs and copyright holders have mutual interest in mitigating P2P – Could they join forces?

• France’s new “Three Strike Law”
  – An ISP customer receives three warnings about illegal file sharing
  – Customer must appear before a judge with the power to suspend the customer’s Internet service

• Enforcement challenges
Conclusion and Policy Implications

- P2P file sharing is problematic for ISPs and copyright holders
- Both groups have tried to mitigate P2P
  - Traffic shaping using forged TCP reset packets
    - **Policy issues**: Network neutrality, transparency, acceptable network management
  - P2P investigations aimed at identifying sharers
    - **Policy issues**: Evidence collection, P2P lawsuits, anonymous communications and legal issues
- Consequently, P2P users have started an “arms race” of counter-tactics to avoid these tactics
- Our goal is to overview current state of this “arms race” and encourage further dialogue among policy makers

Questions?
Backup Slides