Bittorrent Security and Privacy

Samuel Cheng
Tanay Gavankar

Overview

- What is Bittorrent?
- How it Works
- Benefits Over Traditional Download
- Bittorrent in the Real World
- Privacy and Security
- Legality Issues

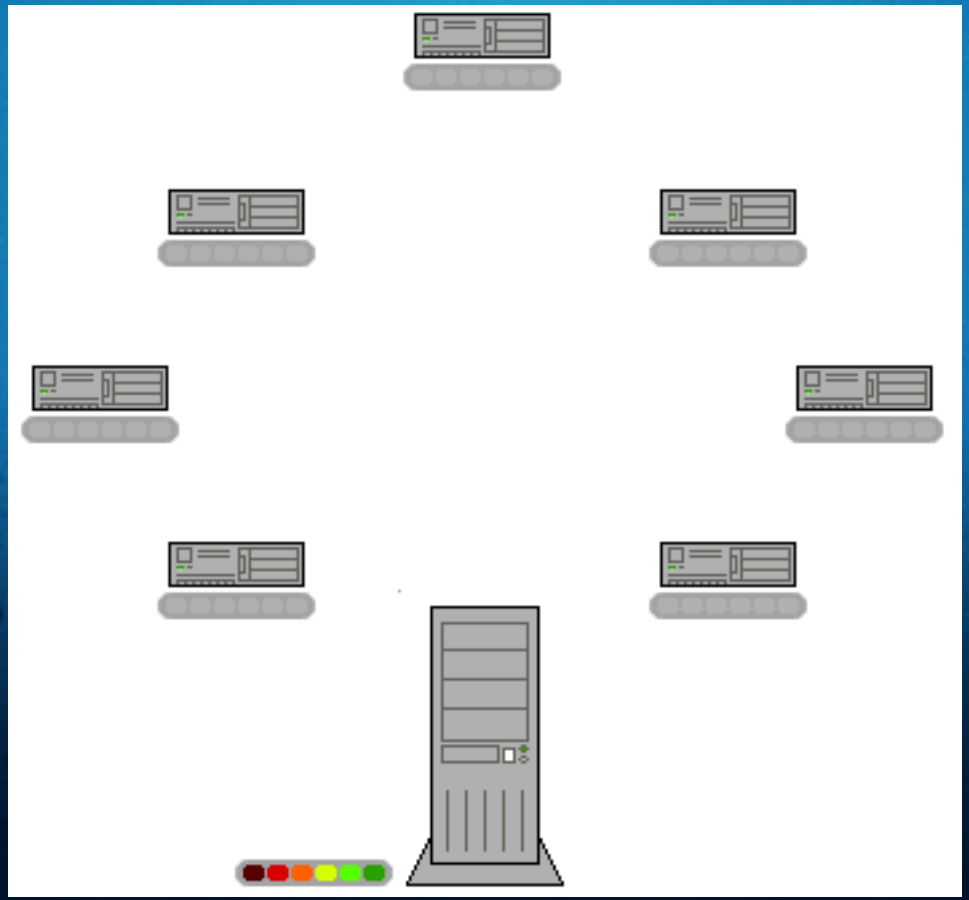
What is Bittorrent?

- Peer-to-peer file sharing protocol
- Used for large files
- No central source server
- Distributed with simultaneous upload/download
- Terminology:
  - Seed - client user who has the complete file (all pieces)
  - Peer - client user who has the incomplete file (some/no pieces)
  - Swarm - collection of seeds and peers
  - Tracker - central server that coordinates swarm

How it Works

- File is split into pieces.
- Pieces are cryptographically hashed and stored into torrent file.
  - Used to prevent accidental/malicious corruption.
- Seed distributes torrent file through conventional means.
  - HTTP, email, etc
- Peers use torrent file to contact tracker and get swarm info.
- Peers randomly select pieces to download from swarm.
  - May be from seeds OR peers
- Peers become seeds once complete file has been downloaded.

How it Works



Source: Wikipedia

Benefits

- Lower cost to initial provider
  - Most bandwidth cost is offset to swarm (other seeds/peers)
- Higher redundancy
  - Hashes allow corruption identification
  - Swarm is one big backup
- Resistant to abuse or load spikes
  - High volume of requests get distributed across swarm
  - Higher volume makes a larger swarm, so it's self-sustaining

Real World

- Blizzard Entertainment
  - All game content and patches
- Open source and freeware projects
  - Linux!
- Web server update distribution
  - Facebook
  - Twitter
- UK government
  - Distributes details of tax money spending
- Pirates

Privacy and Security Issues

- You are not anonymous
- Swarm can see a lot
  - Files
  - IP Address
    - Location
    - ISP
- Protocol header analysis
  - Network eavesdroppers can distinguish torrent traffic
  - ISPs use this to throttle/ban P2P users

Privacy and Security Issues (cont.)

- Distributed trackers
  - No central tracker. Each peer acts as a tracker.
  - Implemented using Distributed Hash Tables (DHT)
    - (key,value) pairs are stored and can be accessed by any node
  - Decreased vulnerability to DDOS attacks
  - Increased scalability and robustness

- Torrent Poisoning
  - Uploading fake or corrupt torrent files
  - Often used to gather IP addresses of downloaders

Encryption

- Protocol Header Encryption
  - Encrypts only header
  - Still allows detection of torrent usage

- Protocol Encryption
  - Encrypts entire message
  - Uses Diffie-Hellman key exchange and infohash of torrent to establish RC4 encryption key
    - Key exchange minimizes eavesdroppers
    - Infohash avoids man-in-the-middle attacks
    - RC4 chosen for speed
      - Stream cipher
      - Used in SSL, WEP, etc

Legality Issues

- Digital Millennium Copyright Act (DMCA)
  - Criminalizes technology, services and attempts to circumvent U.S. copyright law
- Bittorrent technology is legal.
- File sharing copyrighted material is illegal
- Pressure from mostly RIAA and MPAA
  - Want to shut down Bittorrent trackers
  - IPs are easily obtainable
  - Issue subpoenas to force ISPs to reveal identity of users
  - Often issue cease-and-desist notices

Questions?