

Security in P2P File Distribution

By Bram Cohen, author of BitTorrent

bram@bitconjurer.org

<http://bitconjurer.org/BitTorrent/>

Reasons to use P2P

- For distributors, reduced cost
- For downloaders, files not available elsewhere

Types of file distribution

- Web site
- Napster clone
- BitTorrent

Web site architecture

- Users find data with hyperlinks
- Transfers are done directly from server to client

Napster clone architecture

- Users find data by keyword search
- Transfers are done between peers
- Many slight variants

BitTorrent architecture

- Users find data with hyperlinks
- Metainformation is downloaded from a web site
- Bulk transfer is done between peers

Types of attack

- Data reading
- Denial of service
- File corruption
- Remote exploit

Active versus passive attacks

- Passive attacks simply observe, are generally easy to do
- Active attacks require intervention, are harder to accomplish

Common active attacks

- Remotely rooting a machine is easy on an alarming number of sites
- Redirecting DNS is also alarmingly easy
- Altering data sent between two hosts is relatively difficult in practice

Types of data reading

- Finding available data
- Determining who is downloading what ('who' in this case means which IP address)

Types of denial of service

- Direct attack (teardrop)
- Distributed denial of service (DDOS) – attacks from multiple (usually rooted) hosts
- Semantic – flood network with spam or corrupted data

Types of file corruption

- Garbled/unreadable
- Introduction of exploit
- The former usually leads to the latter
(Gobbles will 0wn y00)

Types of remote exploit

- Usually just a direct attack, a very serious (and common!) problem
- Some attacks require the target to initiate a request (many HTTP clients are susceptible)

Data reading on a web site

- Fairly easy if you can sniff
- Can be made harder using HTTPS
- Most sites don't care

Data reading on a Napster clone

- Extremely easy by design
- On many systems, peers run the search engines, so peers can see everything ('teen' is a common search term)

Data reading using BitTorrent

- Access to file contents is the same as on web sites
- Anyone with access to a file can see who else is downloading it
- Most sites don't care

Denial of service on a web site

- Direct attacks are reasonably stoppable if you keep up to date on security patches
- Distributed denial of service unfortunately very easy – Yahoo was taken down by an unskilled script kiddie

Denial of service on a Napster clone

- DDOS generally more difficult due to distributed nature
- Semantic attacks trivial. Rumor has it spamming is common

Denial of service in BitTorrent

- Same as HTTP for original web site
- Peers can be made to waste bandwidth by sending corrupted data, but won't accept it due to secure hashes

The magic of secure hashes

- No two files have the same secure hash
- Cryptographic property – hash collisions obviously must exist but can't be found
- If any collision is found for a hash function people stop using it
- BitTorrent uses SHA1

File corruption on a web site

- Possible to do by active attack
- Can be made more difficult by using HTTPS
- DNS redirection surprisingly easy

File corruption on a Napster clone

- Trivial, any file can be introduced using any name

File corruption in BitTorrent

- Same as for a web site
- Metainfo file contains secure hashes

Remotely exploiting a web site

- HTTP clients and servers are notoriously exploitable
- Constant extension of HTTP and widespread implementation in C exacerbate problem
- Can be kept reasonably under control by keeping up to date with security patches

Remotely exploiting a Napster clone

- Depends on the particular clone
- Clients are generally proprietary, written in C, and use possibly messy unpublished protocols
- Unknown exploits may be rampant

Remotely exploiting BitTorrent

- Metainfo file is on a web server, inherits all of those problems
- Protocol is simple and published, standard implementation is open source, readable, and written in Python. Exploits are unlikely
- Doesn't yet support unicode due to canonicalization concerns (~/.bashrc)
- Underlying OS usually much bigger problem

Conclusions

- Web sites aren't very secure
- Napster clones say 'kick me'
- BitTorrent is only marginally worse than web sites