Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

Stealing bandwidth from BitTorrent seeders

Florian Adamsky [a,*], Syed Ali Khayam [b], Rudolf Jäger [c], Muttukrishnan Rajarajan [a]

[a] City University London, London, United Kingdom
[b] PLUMgrid, Inc., Sunnyvale, CA, USA
[c] THM University of Applied Sciences, Campus Friedberg, Germany

ARTICLE INFO

Article history:
Received 6 December 2013
Received in revised form
21 June 2014
Accepted 31 July 2014
Available online 13 August 2014

Keywords:
Peer-to-peer
BitTorrent
Attacks
Countermeasures
Seeding algorithms

ABSTRACT

BitTorrent continues to comprise the largest fraction of Internet traffic. While significant progress has been made in understanding the BitTorrent choking mechanism, its security vulnerabilities have not been investigated thoroughly. This paper presents an experimental analysis of bandwidth attacks against different choking algorithms in the BitTorrent seed state. We reveal a simple exploit that allows malicious peers to receive a considerably higher download rate than contributing leechers, therefore introducing significant efficiency degradations for benign peers. We show the damage caused by the proposed attack in two different environments: a lab testbed comprising 32 peers and a PlanetLab testbed with 300 peers. Our results show that 3 malicious peers can degrade the download rate up to 414.99% for all peers. Combined with a Sybil attack that consists of as many attackers as leechers, it is possible to degrade the download rate by more than 1000%. We propose a novel choking algorithm which is immune against bandwidth attacks and a countermeasure against the revealed attack.

1. Introduction

High market penetration of broadband connectivity in the past decade has catalyzed a fundamental change in user's traffic characteristics with Peer-to-Peer (P2P) file sharing content comprising a considerable fraction of today's Internet traffic (Van Der Sar, 2011a; Van Der Sar, 2012). Simultaneous to widespread usage of P2P software, a global debate continues to take place on copyright violations perpetuated through P2P software. In addition to public litigation, active measurement studies (Dhungel et al., 2008a, 2011) have revealed many attacks on P2P systems, allegedly launched by companies hired by the music and film industries. Hence, at this time it is important to investigate the threat landscape for P2P systems.

Considering the BitTorrent ecosystem, an attacker has four major components to attack: leechers, seeders, peer and torrent discovery. Peer discovery techniques have evolved with the introduction of Distributed Hash Table (DHT) (Loewenstern, 2008), Peer Exchange (PEX) (User, 2008) and Local Peer Discovery (LPD) (Norberg, 2009). Also, the change from major torrent discovery websites (e.g. PirateBay) to magnet links (PirateBay, 2012) makes the torrent discovery process more robust against attacks. Consequently, leechers and seeders represent the most vulnerable parts in this

* Corresponding author.
E-mail addresses: Florian.Adamsky.1@city.ac.uk, fa-elsevier@haktar.org (F. Adamsky), akhayam@plumgrid.com (S.A. Khayam), Rudolf.Jaeger@iem.thm.de (R. Jäger), R.Muttukrishnan@city.ac.uk (M. Rajarajan).
http://dx.doi.org/10.1016/j.cose.2014.07.009
0167-4048/

ecosystem. One attack that is directed against leechers and seeders is the bandwidth attack.

Dhungel et al. (2007) defined a bandwidth attack as a malicious peer who manages to download from the seeder with the highest speed. As a result, the malicious peer allocates a slot from the active peer set. We add a new attack dimension to this vector, where an attacker gets more bandwidth by one of the following scenarios:

- incorrect protocol implementation;
- incorrect protocol specification;
- programming errors in the BitTorrent client; and/or
- implementation errors in the transport protocol (e.g. TCP (Sherwood et al., 2005), Micro Transport Protocol (uTP) (Adamsky et al., 2012)).

In this paper, we investigate the vulnerability of different chocking algorithms in seed state against bandwidth attacks and reveal a vulnerability caused by incorrect specification of the BitTorrent fast extension. This extension was introduced to ramp up the bootstrapping time for new peers. However, a malicious peer can exploit this extension to steal bandwidth even when a peer is choked. We show that this attack can create significant reductions in download rates for all participating peers.

The key contributions of this paper are as follows:

- We evaluate the effectiveness of bandwidths attacks on different chocking algorithms in seed state on a lab testbed system with 32 peers running commonly-used BitTorrent client software.
- We repeat the experiment in a large-scale scenario on PlanetLab with 300 peers to validate the attacks' utility and effectiveness.
- We show how an attacker can exploit a programming error in the choking algorithm to steal large amounts of bandwidth from a seeder.
- We show a vulnerability caused by an incorrect protocol specification, analyze its impact empirically, and propose, implement and evaluate a countermeasure to patch the vulnerability.
- We propose a countermeasure against the allowed fast attack and propose a novel seeding algorithm which is resilient against bandwidth attacks. We evaluate the proposed algorithm for performance, stability and security.

2. Related work

In this section, we discuss the related work that has influenced and inspired this paper.

Adar and Huberman (2000) analyzed the user traffic on Gnutella and found that 70% of all Gnutella users share no files. They argue that free riding is a major threat to P2P networks which leads to degradation of the system performance and introduces vulnerabilities in the system.

Dhungel et al. (2008b) provided the first investigation of bandwidth and connection attacks on BitTorrent. They defined bandwidth attacks as peers who try to allocate an upload slot from the seeder as soon as possible to nip the seeder in the bud. Their measurements showed that bandwidth attacks are rather ineffective, and it is only possible to increase the download time up to 10%. In another work, Dhungel et al. (2011) came to the conclusion that it is not possible to nip the seeder in the bud. The present work, on the contrary, shows that bandwidth attacks can be launched effectively against seeders. The same authors also studied connection and piece attacks against leechers in detail (Dhungel et al., 2009).

Liogkas et al. (2006) designed and implemented three selfish-peer exploits to obtain bandwidth without sharing pieces with other peers. In the first exploit, their client only downloads pieces from the seeder. Seeders can be easily identified as they advertise themselves by sending a HAVE_ALL message or a complete bitfield. The second exploit attempts to download only from the fastest peers. This exploit observes the frequency of the HAVE messages from the victim. This information is exploited to rougly calculate the download rate of the peer. The last exploit introduces false but rare pieces to attract high bandwidth leechers. This attack exploits the vulnerability that a peer can announce pieces which it does not own. They concluded that their exploits delivered significant benefits, but also that BitTorrent proved to be quite robust against them. Extending this work, Locher et al. (2006) developed a selfish BitTorrent client called *BitThief*, which never serves any content to other peers. This client exploits optimistic unchoking and does not perform any chokes or unchokes, and never announces any pieces. The results of this study showed that BitThief succeeded in downloading the complete file in any case. In rare cases, their client even outperformed the mainline client. In both of these works, the focus of the attack was to download the complete file without sharing upload bandwidth. While prior work in this domain focusses on downloading of a complete file, we instead investigate the effectiveness of attackers which are only interested in degrading system efficiency but are not interested in data integrity.

El Defrawy et al. (2007) showed that it is possible to launch a distributed denial-of-service (DDoS) attack on BitTorrent. DDoS belongs to the category of bandwidth attacks. An attacker can set a victim as one of the trackers. All future peers attempt to contact the victim, consequently flooding the victim with BitTorrent packets.

Piatek et al. (2007) performed a measurement of millions of BitTorrent users and showed that the performance and availability of BitTorrent is quite poor. These measurements motivated the authors to design and implement a new one-hop reputation protocol for P2P networks. The idea of this protocol is to encourage persistent contribution incentives and rewarding contributions. Every client maintains a history of interactions, which serve as intermediaries attesting of the behavior of others. While this protocol limits free-riding, it is hard to compare their protocol with the seeding algorithm proposed in this paper (Section 6.2) as one-hop reciprocation changes the standard BitTorrent protocol behaviors.

We have shown in our previous work (Adamsky et al., 2011) that it is possible to exploit the choking mechanism in leech state. This can destabilize BitTorrent's clustering to attack high bandwidth leechers. One disadvantage of this attack is