文章编号:1005-0523(2009)05-0070-05

BitTorrent安全体系结构设计

王 珏,周 莉

(华东交通大学 信息工程学院,江西 南昌 330013)

摘要:BitTorrent文件分发模型得到普遍应用,但结点缺乏控制、资源缺乏认证等安全性问题也日益突出。针对BitTorrent模型的技术特点,在其基本框架和关键技术的基础上,结合基于SSL的认证技术和多层的安全隧道技术,建立了BitTorrent模型的安全体系结构,在系统层面上为BitTorrent应用提供综合可控的安全服务,实现对网络中各种实体提供统一的安全管理,建立有序可信的网络环境。

关 键 词:BitTorrent;体系结构;双向认证;安全通信
中图分类号:TP393.09 **文献标识码**:A

近几年,一种被称为BT下载的P2P的文件分发模型应用越来越广泛。BT即BitTorrent的缩写,是一种基于混合式网络的P2P应用,它以资源为中心组织P2P网络,网络中结点行为的自主性受到监控中心的监控和管理,但资源的分发与共享的过程并不受到任何干涉。与"纯粹"的P2P应用相比,BitTorrent文件分发模型(以下简称"BT模型")增加了结点的控制和管理,从一定程度上降低了结点行为对整个网络造成的不良影响。然而,由于设计和应用上的问题,BT模型仍然存在着诸多安全隐患,对P2P网络乃至整个Internet的安全都带来了威胁。

针对BT模型的安全问题,当前主要是研究资源的安全性,例如非法访问、篡改、计算机病毒等,或者是将其他P2P应用的安全技术简单应用于BT模型。这些安全措施显得过于片面和僵化,没有从BT模型的特点和整体考虑其安全[1~3]。所以,必须以BT模型结构为基础,充分研究其协议和相关技术,结合成熟的网络安全技术,建立一套系统的安全体系结构。

1 BT文件共享模型

1.1 BT模型概述

BT模型以三个部分——BT网站、.torrent文件和Tracker服务器为核心,基于一套独有的编码规则和协议,控制和帮助P2P网络中的结点共享文件。BT模型的结构如图1所示。

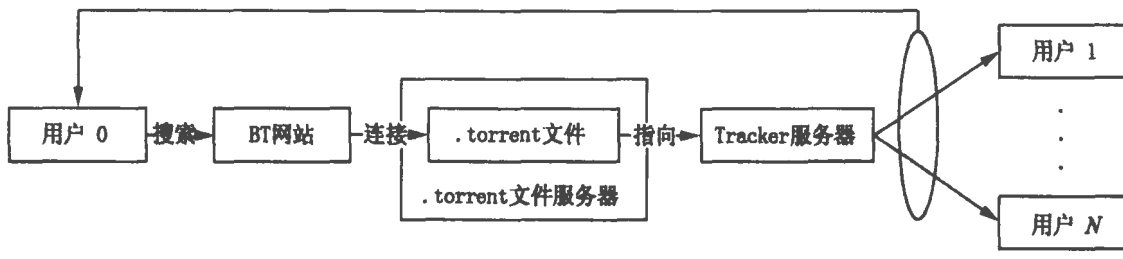

图1 BT模型结构图[4]

用户是BT网络中的结点,其中用户0是共享文件的完整拥有者(被称为"种子"),在结构中负责发布原始文件。其他用户是下载者,同时也是文件的上传者,一旦文件下载完毕,用户即成为"种子",只负责文件的上传。

收稿日期:2009-06-18
基金项目:江西省教育厅科技项目(GJJ08255)
作者简介:王 珏(1978-),男,江西南昌人,讲师,硕士,主要研究方向为计算机网络与信息安全。

中国知网 https://www.cnki.net

BT网站是一系列提供.torrent文件搜索的Web服务器,从一个BT网站可以搜索到一部分.torrent文件,但文件本身可以位于其它的HTTP服务器上。

每个.torrent文件包括一个文件列表,其中包含每个文件的文件名、文件大小、"种子"数、下载该文件的用户数和文件的散列值等。除此之外,还包括Tracker服务器的位置。

Tracker服务器是BT网络和用户信息的维护者,其职责是帮助用户互相发现对方,下载同一个文件的所有用户围绕Tracker形成一个独立的子网。Tracker跟踪所有下载某个文件的用户,并实时地将这些用户信息发给其中任何一个,它控制着BT网络上某个或某些文件的下载和用户之间的协同工作[5]。

BT模型拥有以下关键技术[6]:

1) 对象统一按照B编码(BEcoding)的明文编码规则进行编码,.torrent文件,Tracker服务器对结点请求的响应报文,以及结点之间传输的报文都按照B编码的规则进行描述;

2) 结点间依靠基于TCP的应用层协议——结点线路协议进行消息的协商与资源的上传与下载;

3) 资源的分发是按照分片机制进行的,将文件分隔为固定大小的片段,用户必须知道其它用户拥有的片段,从而能够采用"(片段拥有)最少者优先"的策略选择片段进行下载;

4) BT模型关键机制是所有用户必须进行文件片段的交换——下载的同时提供上传。BT模型通过"针锋相对(tit-for-tat)"来保证该机制的运转,即只向上传文件片段的用户提供该文件其它片段的下载。所以,只有提供高速上传的用户才可能高速下载。而完成下载的用户成为"种子"只进行上传,以保证整个网络中文件资源的持续存在。

1.2 BT模型的安全问题

BT模型的安全问题主要有以下几个方面:

1) 结点缺乏有效的认证机制,所以无法解决下列问题:结点提供错误的结点信息造成BT网络的管理失效;结点向Tracker服务器或其它结点进行拒绝服务攻击造成Tracker服务器或者其它结点无法工作;结点对Tracker进行非授权访问篡改结点信息或资源信息;一个结点提交多个身份控制一个BT网络的极大部分破坏P2P网络的冗余性[7]。

2) Tracker服务器缺乏认证机制,这样一来,恶意站点通过扮演Tracker服务器,并通过.torrent文件发布,使得BT用户能够加入不安全的BT网络,从而对正常BT网络中的结点和资源造成破坏。

3) 结点间的通信缺乏安全保障。结点间的协商、数据上传和下载仅有基本的完整性验证,缺乏保密性、抗抵赖性等安全防护。

(4) 穿越防火墙:BT软件经过特殊设计,能够通过防火墙使内外网用户建立连接,这就像是在防火墙上开放了一个秘密通道,使得内网直接暴露在不安全的外部网络环境下。

2 BitTorrent安全体系结构的设计

2.1 BT安全体系结构基本框架

BT安全体系结构的基本框架如图2所示。

该框架在BT模型原有安全机制的基础上提供了3个层次的安全服务:

1) 结点双向认证。对加入BT网络的结点进行认证,防止恶意结点加入造成的安全隐患,同时,对Tracker服务器进行认证;

2) 安全通信。保障结点间通信消息的机密性、完整性等以及维护结点间链路的稳定性;

3) 其他安全服务。针对特定的环境提供各类安全服务,例如文件分发中的资源评价、完整性、不可抵赖等安全机制。

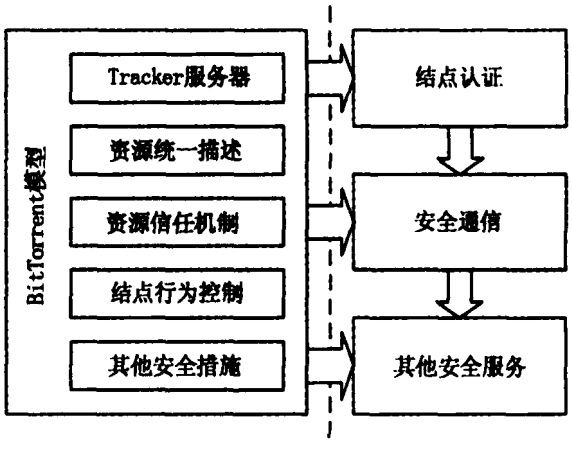

图2 BitTorrent安全体系结构基本框架

中国知网 https://www.cnki.net

上述安全服务在BT安全体系结构中被组织为层次结构,下层服务的实现依赖于上层服务,所有安全服务的实现依赖于BT模型的核心安全机制和技术。

2.2 BT模型安全机制

BT模型自身提供了一些安全机制保障BT网络的安全运行:

1) Tracker服务器的设立。Tracker服务器承担了结点查询、资源发布等工作,避免了"纯粹的"P2P网络中因为结点和资源查询造成的"查询洪泛"问题;另外,Tracker服务器的存在也使得BT网络拥有结点行为的监控和管理中心,能够有效进行结点行为控制;

2) 资源统一描述。BT网络中的资源信息采用B编码进行描述,B编码使得BT网络中的实体与网络外的实体区分开来,成为一个相对独立的实体域,从一定程度上阻止了伪造、仿冒、篡改等攻击行为;

3) 资源下载和上传的策略。BT模型采用"针锋相对"策略来保证结点在下载的同时必须提供上传,以上传作为结点享受P2P对等权利的基本前提;

4) 资源的信任机制。资源的信任机制主要包括数据校验和内容评估两方面:

(1) .torrent文件中声明的资源片段都有唯一的SHA1散列值,如果片段没有通过基于该散列值的校验,则不会发布到BT网络中[6];

(2) 为了减低资源的"污染"等级,新发布的资源必须首先被仲裁,以判断是否包含伪造内容。如果资源中包含"低质量"的内容,或者资源的命名不合法,则被禁止发布[4];

5) 其它安全措施[1]。BT模型还应用了其它安全机制来保证信息的安全:

(1) Tracker服务器与结点通信中采用校验机制。在通信过程中设定一个校验码,以确认通信信息在传送的过程中没有经过修改;

(2) 结点的TCP包过滤机制。当结点有效连接已经达到上限的时候,过滤其它所有的连接请求,也停止该结点向其它结点发送连接请求,以防止结点试图连接过多的结点造成的洪泛;

(3) 动态安全策略。当结点成为"种子"的时候,将启动一个类似防火墙的模块,这个模块将为结点提供比较严格的网络安全策略,让结点拥有更为安全的网络环境。

BT模型的安全机制是BT安全体系结构的基石,确定了安全体系结构的拓扑结构、实体描述、信任机制和网络传输策略等内容,在此基础上,引入认证、安全通信等安全技术,结合BT模型安全机制采用的协议、算法和策略等,构建BT安全体系结构丰富和稳定的上层安全服务,同时也为安全服务的实施提供了基础性的保障。

2.3 双向认证

利用Tracker服务器在BT网络中的中心地位建立认证中心,负责向用户分发密钥以及验证来自用户的密钥。同时,结点在连接Tracker服务器时也必须对Tracker服务器的合法性进行验证,以防止连接到恶意站点。因此,可以在结点与Tracker服务器之间建立基于SSL的双向验证[8]。

2.3.1 Tracker服务器认证

结点认证Tracker服务器的过程如下:

1) 结点向Tracker服务器发送一个开始信息"Hello"以便开始一个新的会话连接;

2) Tracker服务器根据结点的信息确定是否需要生成新的主密钥,如需要则Tracker服务器在响应结点的"Hello"信息时将包含生成主密钥所需的信息,如协议版本、加密算法等;

3) 结点根据收到的Tracker服务器响应信息,产生一个主密钥,并用Tracker服务器的公开密钥加密后传给Tracker服务器;

4) Tracker服务器用公钥恢复该主密钥,并返回给结点一个用主密钥认证的信息,以此让结点认证Tracker服务器。

2.3.2 结点认证

结点认证之前必须确保Tracker服务器已经通过了认证,这一阶段主要完成对结点的认证。经认证的

中国知网 https://www.cnki.net

Tracker服务器发送一个数字证书请求给结点,结点则将请求摘要和其公开密钥形成的数字证书返回给Tracker服务器,从而向Tracker服务器提供认证。

2.4 安全通信

在P2P安全模型中,结点间的安全通信需要建立结点间的安全隧道。在BT模型中,结点线路协议基于TCP协议。因此,可将基于网络层和传输层的安全协议应用于P2P网络中结点之间的安全通信。

2.4.1 网络层安全协议——IPSec

IPSec定义了用于网络层的两个协议:AH协议和ESP协议。AH设计用来提供完整性,将传输层报文的摘要值写入AH首部,并插入IP首部与传输层报文之间。ESP提供保密性以及完整性和报文鉴别,由ESP首部、ESP尾部和ESP鉴别数据三部分组成。ESP尾部填充传输层报文并保留报文协议首部,将报文与ESP尾部加密后,在IP首部与加密报文之间加入ESP首部,然后将ESP首部、加密后的报文和ESP尾部生成ESP鉴别数据,置于ESP尾部之后。

IPSec支持多种加密算法及散列算法,能够对传输的IP数据包提供加密和完整性保护,从而在网络层建立一个安全隧道[9]。

P2P网络中结点间的通信都基于IP协议,因此,在P2P网络中应用IPSec进行安全通信无须对P2P使用的上层协议进行修改,在本文提出的基于BT的P2P安全模型中,IPSec的应用不会影响基于结点线路协议的P2P通信。

2.4.2 传输层安全协议——TLS

传输层安全)TLS(Transport Level Security是建立在TCP协议之上的安全标准。包括两层协议:TLS记录协议和TLS握手协议。TLS记录协议位于TCP首部之上,用于封装TCP报文。TLS记录协议通过对称加密提供通信的保密性,并提供安全哈希功能保证通信数据的完整性。TLS握手协议允许通信的双方在应用程序协议传输和接收其第一个数据字节前彼此之间相互认证、协商加密算法和加密密钥。

TLS的最大优势就在于:TLS独立于应用协议。因此,BT模型使用的结点线路协议可以透明地应用在TLS之上。

2.5 其他安全服务

其他安全服务是针对不同的应用环境提供的各类安全服务。利用BT模型提供的资源统一描述、结点行为控制、资源信任机制等行为以及统一的认证和安全通信机制,在特定的应用环境中提供信息的保密性、完整性、不可抵赖性等安全机制,并对BT网络中的不同实体(包括结点、资源、信息等)提供授权与权限管理、信任评价、安全管理等安全机制。

3 安全体系结构的应用环境

本文提出的BT安全体系结构为一个理论框架,其安全服务的实现依赖于现有的成熟网络安全技术,例如授权机制、安全访问机制等,在应用上不存在技术上的阻碍。除此之外,安全服务在模型中的应用还依赖于BT模型中的实体或相关技术,现有的BT应用尽管在功能和具体实现上存在差异,但基本框架和协议仍然大同小异,在应用的广泛性上有很好的前景。

因此,无论是在架构应用上,还是在安全技术的应用上,该理论框架都能够应用于当前流行的BitTorrent应用与开发,例如BitComet,BitSpirit和Azureus等,在不改变其极有结构和功能的基础上提供文中提出的各种安全服务。

4 结语

BT模型由于其协议的高效性和应用的多样性,日益成为P2P网络中一种重要的技术,然而由于各方面原因,其安全建设相对于其应用显得较为落后。本文在介绍BT文件共享模型的基础上,利用该模型的安全服务和网络机构,结合基于SSL的认证技术以及不同协议层的安全隧道技术,提出了一种系统的、可

中国知网　https://www.cnki.net

控的安全体系结构。该安全平台的建立,对于 BT 网络乃至于 P2P 网络的安全建设和安全管理,都有较好的应用价值。

参考文献:

[1] 文 龙. BitTorrent 安全性研究[D]. 成都:电子科技大学,2006. 74 - 75.
[2] 熊 皓,姚 丽,王志鸿. 综合信誉对等体制模型及其安全性的研究[J]. 福建电脑,2008,24(11):94 - 95.
[3] 蔡方萍. 点对点网络及其安全问题分析[J]. 萍乡高等专科学校学报,2008,25(3):56 - 58.
[4] J A Pouwelse, P Garbacki. An introduction to the BT Peer-to-Peer File-Sharing System[R]. The Netherlands: Delft University of Technology, 2004. 15.
[5] 陈贵海,李振华. 对等网络:结构、应用与设计[M]. 北京:清华大学出版社,2007. 35 - 44.
[6] Elliott Mitchell. BT protocol specification v1.0[EB/OL]. http://wiki.theory.org/BTSpecification, 2007 - 01 - 12.
[7] 周亚建,杨义先. 与 P2P 技术相关的信息安全问题[J]. 电信工程技术与标准化,2006,19(5):127 - 129.
[8] 陆荣杰,刘知贵,郑晓红. 基于 HTTPS 隧道技术的统一认证平台研究与实现[J]. 计算机应用与研究,2006,(12):168 - 170.
[9] 叶润国,宋 成,吴 迪,等. P2P 网络中对等结点间安全通信研究[J]. 微电子学与计算机,2004,21(6):95 - 99.

Design of BitTorrent Security Infrastructure

WANG Jue, ZHOU Li

(School of Information Engineering, East China Jiaotong University, Nanchang 330013, China)

Abstract: The BitTorrent file-distribution model gets universal application, but there are security problems including shortage of nodes control and resources authentication. According to the characteristics of Bittorrent model, this thesis establishes the security infrastructure based on its basic frame and key techniques, combining the SSL authentication and the multi-layer secure tunnel techniques. The infrastructure can provide general and controllable security service at the system level to implement the unified security management of the units in the network. Consequently it can establish reliable network environment.

Key words: BitTorrent; infrastructure; mutual authentication; security communication

(责任编辑:刘棉玲)

中国知网 https://www.cnki.net