Combining Bittorrent with Darknets for P2P privacy

Öznur Altintas Niclas Axelsson

Abstract

Over the last few years, traditional downloading of programs and application from a website has been replaced by another medium - peer to peer file sharing networks and programs. Peer- to-peer sharing has grown to tremendous level with many networks having more then millions of users to share software's, music files, videos and programs etc. However, this rapid growth leaves privacy concerns in its awake.

P2P applications disable clients to limit the sharing of documents to a specific set of users and maintain their anonymity. Using P2P applications like BitTorrent exposes clients' information to the other people. OneSwarm is designed to overcome this privacy problem. OneSwarm is a new P2P data sharing system that provides users with explicit, configurable control over their data. In this report, we will discuss briefly Darknets and privacy terms, and mainly how OneSwarm solves privacy problem while providing good performance.

Introduction

For a better understanding of this report, we begin with the explanation of some terms such as Darknets and privacy and brief background information underlies the idea of OneSwarm.

Darknet—a collection of networks and technologies used to share digital content. The darknet is not a separate physical network but an application and protocol layer riding on existing networks. Examples of Darknets are peer-to-peer file sharing, CD and DVD copying and key or password sharing on email and newsgroups. When used to describe a file sharing network, the term is often used as a synonym for "friend-to-friend", both describing networks where direct connections are only established between trusted friends.

Privacy—the protection of information from unauthorized disclosure—is a long-standing concern of computer system design. Privacy has become of particular concern as users become authors of content, rather than passive consumers, sharing their content and their interests with overlapping sets of people. At a technical level, privacy is easy to accomplish with centralized solutions. If the user data is stored on a server in a data center, user directives about distribution can be easily enforced, and data about user interests can be carefully limited or disabled on user request. However, in reality many web services force users to trade off privacy and service. Many sites see no harm in to collect, store, and share personal data of their users.

Peer-to-peer (P2P) data sharing systems potentially provide an option for achieving scalability and privacy without relying on centralization. With P2P systems, user still leaves aside the privacy for the sake of usability. For instance, systems like BitTorrent are high performance and robust, but everyone's activities are visible to anyone who cares to look. On the other hand, anonymization systems like Tor and Freenet emphasize privacy but at the cost of poor performance and robustness, in part because of misaligned incentives and inefficient protocol choices such as single path routing. A privacy-preserving file sharing service called OneSwarm, intended to bring these two features -privacy and usability- together. Remainder of this report continues with a detailed explanation of OneSwarm system.

OneSwarm

OneSwarm is a privacy-preserving P2P client based on the Azureus bittorrent client. It was released 2009. The main goal with this protocol was to create something that could transfer files in a secure and efficient way preserving privacy of the sender/receiver.

A cloud of clients

In a OneSwarm network is the client connected to a set of friends. Each entity in this set is connected to another set. This way it's possible to create many small sets, connected to eachother by some common friend. The privacy is keept by preventing users to get knowledge about their friends sets.

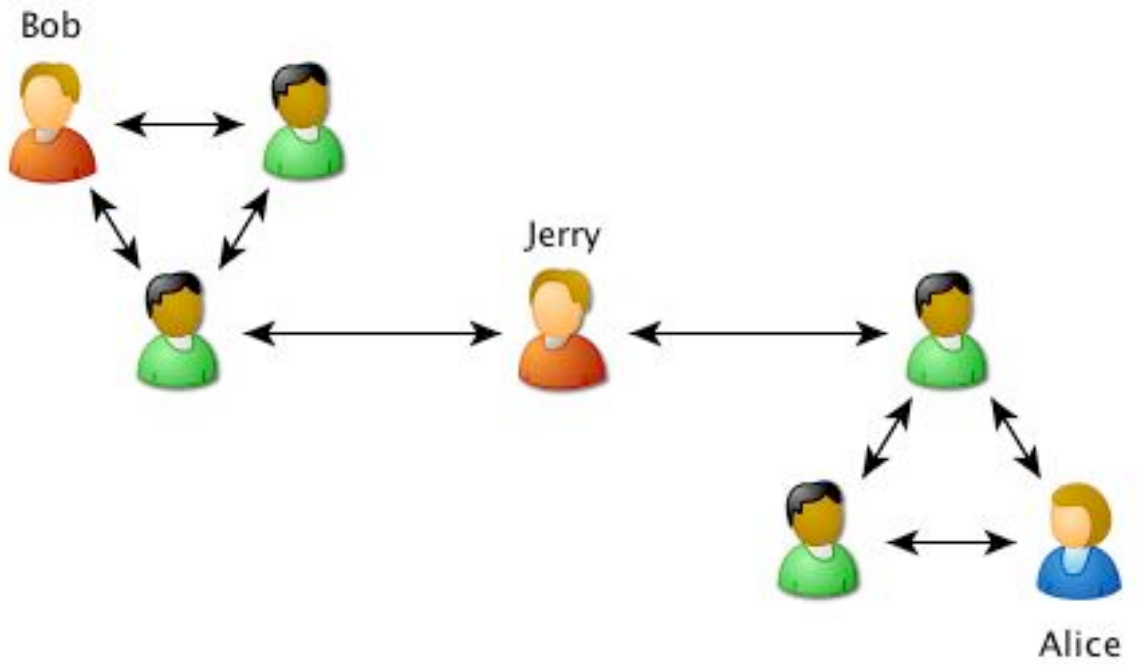

Fig 1. Bob and Alice are connected to two different sets of friends, but can reach eachother through their common friend Jerry.

File transfers
The file transfers is inspired by the Bittorrent protocol, it supports multi-source download but instead of using a centralized tracker OneSwarm uses a flooding algorithm when searching for files. Shared files are indexed with a compressed XML file, containing attributes describing the name, size, and other metadata. If a file is in a private share, the metadata in the XML also contains a 512 bit capability used as a symmetric encryption key during transfer. The index-file is exchanged between users in the initial connection between them.

When a user is searching for a file, it sends a search query to its friends and if they doesn't have it they forwards this message to their friends. To preserve the privacy, all clients does a short delay (Usually 150ms) before forwarding messages. Because of this can not the reciever get any information about the sender (Like if the sender is the datasource for a specific file).

OneSwarm is using the bittorent protocol when transfering files ,but instead of connecting directly to the source, it uses the path as a source. If you look at Fig 2, *Alice* are sending a search query to the network (The filled line), and if the user receiving this request do not have the file, he forwards the request to his friends. When the request reaches a user who shares this file, the user responds with a search reply message (Dotted line) containing a search identifier, hashes that identifies the matching file(s), file metadata and a *path identifier*. This identifier is a unique ID which identifies a path (Look at Fig 2).

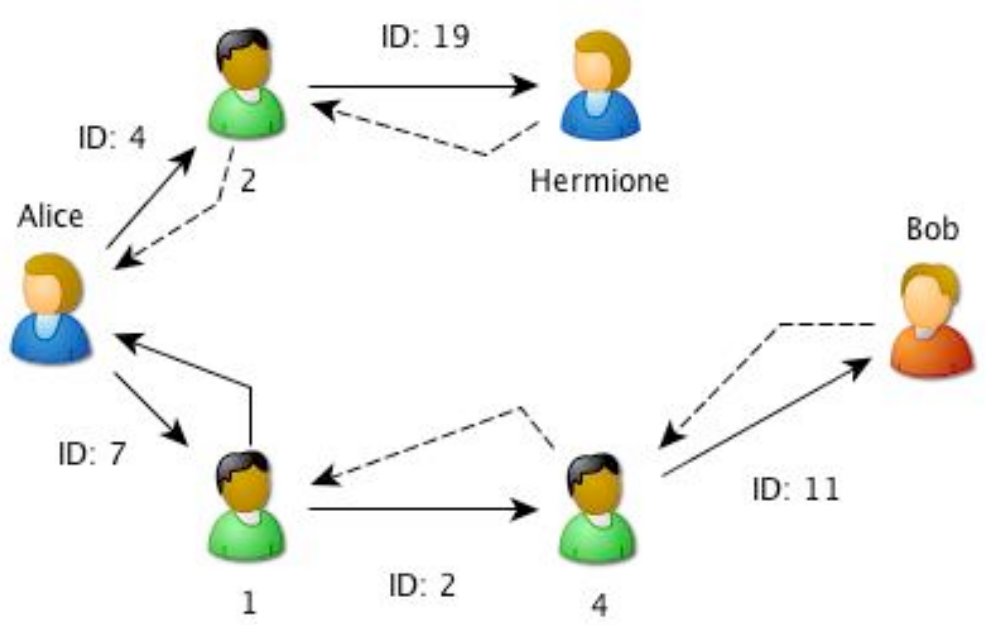

Fig 2. Example of a search query in OneSwarm

Conclusion

What we have learnt about this topic so far:

- Currently popular peer-to-peer networks suffer from a lack of privacy.
- OneSwarm, a file sharing system designed to reduce the cost of privacy to the average user.
- OneSwarm is built on (and backwards compatible with) BitTorrent.
- Novel techniques are developed for efficient, robust, and privacy-preserving lookup and data transfer.
- Flexible control over their privacy by defining sharing permissions and trust at the granularity of individual data objects and peers is provided for users.
- Privacy-preserving downloads on OneSwarm are roughly as fast as a direct Internet transfer between the two nodes, and an order of magnitude faster than using Tor for the same operation.
- OneSwarm is available for Linux, Mac OS X, and Windows.
- Finally, OneSwarm is research software that is still under active development. For strong anonymity, OneSwarm warns their thousands of users.

References

Combining BitTorrent With Darknets For P2P Privacy. (n.d.). *Slashdot: News for Nerds. Stuff that Matters.* Retrieved March 7, 2010 from *http://www.slashdot.org*

Darknet (file sharing). (2010, March 3). *In Wikipedia, the free encyclopedia*. Retrieved March 7, 2010, from *http://en.wikipedia.org/wiki/Darknet_%28file_sharing%29*

Peter Biddle, Paul England, Marcus Peinado, and Bryan Willman, "The **Darknet** and the Future of Content Distribution," *Digital Rights Management conference*, November 22, 2002

Tomas Isdal, Michael Piatek, Arvind Krishnamurthy, Thomas Anderson, “Privacy-preserving P2P data sharing with OneSwarm,” http://oneswarm.cs.washington.edu/