Toward Unobservable Data Sharing in Overlay Networks

Qingfeng Tan[1,2], Jinqiao Shi[1,2], Xiaojun Chen[1,2], Fanwen Xu[3], and Shoufeng Cao[4]

[1]Chinese National Engineering laboratory for Information Security Technologies

[2]Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China

{tanqingfeng, shijinqiao, chenxiaojun}@iie.ac.cn

[3]Department of Computer Science, Beijing University of Posts and Telecommunications, Beijing, China

[4]National Computer Network Emergency Persons Technical Team/Coordination Center of China

ABSTRACT

With increasingly concerned with of erosion of privacy, privacy preserving and censorship-resistance techniques are becoming more and more important. Anonymous communication techniques offer an important method defense against Internet censorship, but don't hide the fact that the users are using them.

We present an efficient anonymous and unobservable communication protocols with steganography in overlay network. It secretly exchanges messages from users to innocent-looking destinations by mirroring and forwarding a special traffic. The covert communication is indistinguishable from normal network communication to any adversaries without secret key.

Categories and Subject Descriptors

C.2.0 [**Computer-Communication Network**]: General-Security and protection(e.g., firewalls)

General Terms

Security

Keywords

Covert communication; Censorship-resistant; unobservability

1. INTRODUCTION

Nowadays, the Internet has become a primary tool for routine work and entertainment. With the development of the Internet and the growing desire of privacy and free expression, Internet censorship attracts more and more attentions. However, many users face surveillance of their Internet communication, the prevalence of Internet censorship has become a serious threat to privacy and free of speech.

Traditional anonymous communication systems (such as Tor[1]) are particularly vulnerable to traffic analysis[2]. In fact, researchers have demonstrated that it is easy to monitor and block such systems. The primary problems of these schemes are that these entry points can easily be found and blocked by a censor. In addition, the use of encrypted tunnels between a user and the entry point is suspicious of an attacker; as a result, censors can detect and block the user's connection to those entry points. Furthermore, the systems' communication behavior and traffic pattern is detectable, which doesn't hide the fact that the users are using these technologies.

Censorship-resistant systems such as Telex[3] and Cirripede[4] provide a new approach for defending against Internet censorship without relying on entry points distributed. However, a key difference between our scheme and the Telex approach is that, the goal of Telex system is to make access to censored data, but our goal is to publish or share passively censored data to untraceable destinations; Furthermore, Telex and Cirripede use Diffie-Hellman over an elliptic curve, However, our system opts to use symmetric-key cryptography for achieving better scalability; Finally, it is difficult to deploy accurately such Telex station on the paths between the client and the Non-Blocked.com for all packets of the client's connection pass through it without government participation, whereas our system architecture allow friendly ISPs to deploy deflecting router on any paths between censors'networks and a large number of innocent users, and then transparently mirror part of all traffic it sees to the receiver.

In this paper, we propose a new unobservable communication method in overlay network to circumvent Internet monitoring and censorship. We describe how to leverage covert internet traffic in order to exchange censored data, while maintaining plausible deniability against publishing data. The main challenge in the design of the system is ensuring unobservability and providing a level of usability. Our idea is to construct covert channels based on symmetric cryptography. Consequently, a cryptographic handshake protocol is proposed to ensure that the covert channel in P2P traffics can only be recognized by the deflecting router, whereas anyone else cannot distinguish them from regular traffic without a shared secret. In the downstream direc-

tion, the publishers response content by hiding censored data in uncensored popular p2p content (e.g.,text, photos, and videos) as the cover medium.

2. DESIGN OVERVIEW

2.1 Architecture Overview

As shown in Fig. 1, we show our system architecture. The main components are as follow:

Publisher: the publisher, running on a user's computer, wants to share targeted resource with a covert destination in unobservable communication manner.

Firewall: a censor, monitoring or filtering the publisher's traffic, attempt to detect a client who is the publisher and trace the recipient.

Innocent Users: some P2P users who want to search some interesting resources for fun in P2P network.

Recipient: a user who aims to exchange secretly message with a publisher.

Deflecting router: the Internet router provides for mirroring the covert traffic.

Backend Server: a backend server end for processing the traffic mirrored by Deflecting router.

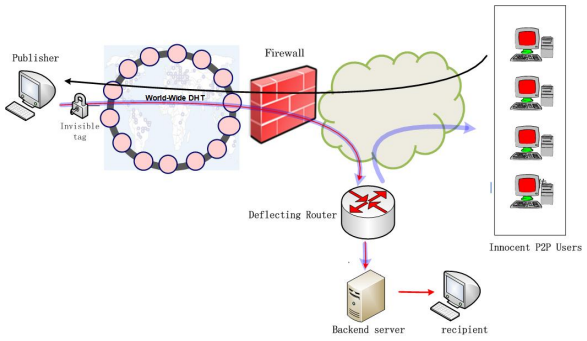

Figure 1: System Architecture

The system is designed to allow users to exchange securely data in unobservable manner, and preserve the users'privacy. The basic idea of our design is that, entry points can easily be found and blocked by a censor, but it is difficult to filter an in-network device, follow this insight, the system architecture is provided in Fig. 1, a publisher behind in censorship network wish to exchange message with recipient secretly, but don't reveal this recipient's identity. The unobservable communication is divided into two main phase: steganographic handshake and data channel. steganographic handshake allows both parties to authenticate the group membership of one another and establish a secure channel. data channel consists of message transmissions from a publisher to the real recipient.

To use this system, it needs deploy the deflecting router on the paths between senders and recipients, to secretly share resources, the sender construct a covert channel in the P2P packet header makes it difficult for an adversary to detect and block these flows. Innocent users behind the vast deployment of deflecting router search some interesting resources, and then download them. If the download flows is the special covert flow, then the router mirrors part of all download traffics it sees to real destinations. From the perspective of adversaries, a user of using the system is making a regular network traffic, while the user is actually sharing messages to untraceable destinations that are monitored by a censor.

2.2 Steganographic Handshake

Steganographic handshake protocol plays a key role in the hidden communication in the overlay network. There are many methods that the publisher could covertly talk to the deflecting router. In this paper we propose that an encrypted magic value embedded within the 160-bits node ID that is indistinguishable from other node IDs. We assume that the each peer shares a secret with the deflecting router. The secret that is used to generate random key to encrypt magic value are from recipient via out-of-band. The modified node id protocol is as follows:

The publisher generates n bytes of strong random seed: RS(n) and then computes the m-bits random key: MAC(shared secret, RS(n)), which is the hash of the concatenation of the shared secret and RS(n). Finally, the random key is used to encrypt the 32-bits magic value by an AES symmetric encryption and placed in the node id. Therefore, the first 8 bytes of a node id is random seed, and the last 4 bytes of a node id is the encrypted magic values. Upon a deflecting router detects a packet that contains the magic value at the node id, and then mirrors it and the remaining packets in the flow to a recipient.

2.3 Data Channel

Data Channel consists of a sequence of download requests and responses. The downstream communication consists of four steps for sending a message: (1) divide a message into many erasure-encoded "shares", (2) embed these shares into popular p2p resources(e.g., images, videos, text), (3) construct a covert channel embedded in 160-bits node ID, and (4) share the content back to the innocent p2p users.

In order to mirror packets from publishers to the real destinations, First, the deflecting router monitors only packet headers of P2P downstream direction. Once a deflecting router detects a packet that contains a special "tag" (magic value)at lookup response traffic, and then inserts a unique 4-tuple consisting of source and destination IP addresses and port numbers to matched IP rule table. Second, the deflecting router uses the ip rules to match all the source IP addresses and ports and mirrors it and the remaining packets in the flow to a real destination.

After making a download request form any one of innocent users, the publisher steganographically embed "tag" in responses which its flows should be mirrored by deflecting router, and then hide censored messages in a cover medium makes it difficult for an adversary to detect and block these tagged flows, because a popular P2P resource typically serves the same content to many different peers (and even to the same user multiple times). Receivers then retrieve a subset of these blocks to recover the original message by decoding these cover media.

3. ACKNOWLEDGEMENT

This work was supported by National Natural Science Foundation of China (Grant No. 61100174) and National High Technology Research and Development Program of China (Grant No. 2011AA010701)

4. REFERENCES

[1] R.Dingleding, N.Mathewson, and P. Syverson. Tor: The second-generation onion router. In Proc. 13th USENIX Security Symposium, San Diego, CA, Aug. 2004.

[2] S. J. Murdoch,, and G. Danezis, Low-cost traffic analysis of Tor. In Proceedings of the 2005 IEEE Symposium on Security and Privacy. May 2005.

[3] E. Wustrow, S. Wolchok, I. Goldberg, and J. A. Halderman. Telex: Anticensorship in the Network Infrastructure. In Proceedings of the 20th USENIX Security Symposium, 2011.

[4] A. Houmansadr, G. T. Nguyen, M. Caesar, and N. Borisov. Cirripede: Circumvention Infrastructure using Router Redirection with Plausible Deniability. In Proceedings of the 18th ACM conference on Computer and communications security, CCS '11, pages 187-200, 2011.