Accessing Web Services Anonymously using P2P

Akmal Khan, Hyunchul Kim, Ted " Taekyoung" Kwon, Yanghee Choi
School of Computer Science and Engineering

Seoul National University, Seoul, Korea

P2P 를 이용한 웹 서비스 익명성 접근

칸 아크말, 김현철, 권태경, 최양희

서울대학교

raoakhan,hkim@mmlab.snu.ac.kr;tkkwon,yhchoi@snu.ac.kr

Abstract 요 약

Peer to peer (P2P) has mainly used for sharing files, VOIP and Video on demand. In this paper, we will investigate the case for using P2P for accessing Web Services anonymously. Anonymous Internet access for different services has been debated for many years but there is lack of publicly available and trusted services/products.

peer to peer(P2P) 시스템은 파일 공유, VoIP, VOD(Video On Demand)에 주로 쓰인다. 본 논문에서는 P2P를 사용한 웹 서비스 익명 접근에 대해 논한다. 수년간 다양한 어플리케이션에 대한 웹 익명성 접근이 논의되어 왔지만, 공개된 데이터나 신뢰성있는 서비스/상품이 없는 실정이다.

Ⅰ. Introduction

Anonymity can mean different to different people and can be used to hide your identity while accessing services like web, blogs, etc. You may want to be anonymous as there are many people wanting to record your Internet traffic and browsing patterns; from governments to commercial advertising networks.

When we talk about " good" and " evil" in the communication protocols domain Peer to Peer (P2P) most of the times end up on the " evil" side. One of the reasons is its usage for possible unethical, illegal activities over the years. It is surprisingly and unfair that TCP/IP is used by all of the crackers/attackers but it mostly end up on the " good" side. Researchers has proposed many P2P schemes over the years like legally sharing files, VOIP or Video on Demand etc. to advocate the importance and utility of such scheme in achieving efficiency ,saving and earning money[2,3,6].

P2PWEB works by searching for the peers who are able to provide the web service. It is kind of voluntary service on the notion of working for each other anonymity. One peer is providing other the anonymity like the same kind of social system where we work voluntary for the benefit of each other.

Ⅱ. Proposed Scheme

Figure 1 provides the high level architecture of Anonymous P2P web access. Normal Web access works by resolving the DNS query for the IP address of server and forwarding the request to the particular web server i.e. SNU web server in our example.

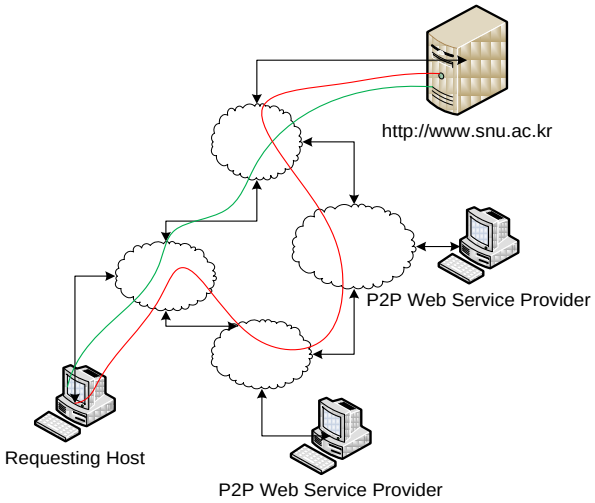

Figure 1: Anonymous P2P Web Access

What most of the web server do is logging the requesters IP address and some time even displaying on their main webpage to let user know about their knowledge of who is accessing their service. The message they simply want to convey to possible malicious users/attackers is that we know who you are. There can be network of volunteer P2P users who provides access of their resources to other users who wants to access web with the goal of achieving anonymity. Figure 1 shows the red line displaying the possible normal web access scenario and the green line to show how web access can work through P2P user providing service to the requester.

There are number of design decisions needed to be considered like scalability, Bandwidth classes, Incentives, caching, etc. For the sake of simplicity, we are not considering at this time the various types of passive and active attacks which can be employed against such volunteer P2P nodes. We are working on the detail design and implementation model for our Anonymous P2PWeb system.

Apart from achieving anonymity numerous other advantages can be achieved by introducing the concept of Network users providing services like Web access. Normally user has no control over the Network paths which his applications are going to use because ISP provides the paths to users based on its contractual relationship with other ISP. On the one hand user can decide which paths he wants to use available through different P2P application service providers based on latency, error rate, etc. There can be economic incentive to giving this service to other users if we consider the dynamic routing design considering the geographic positioning of different networks i.e. using the networks which have less traffic because most of the users are sleeping in that country and there are P2P access providers. We can take example of our PC computer running for whole night without being used most of the time, which can be used as P2P web service provider and you may be even paid if there is a company which uses your PC services. It is understandable to think about the numerous other issues to consider while implementing such services design like price models, how to reduce latencies, fairness etc.

III. Related Work

Chaum's **Mix-Net** design is considered as the first to propose the concept of Anonymous Systems [1].Mix-Net works by hiding the correspondence between sender and recipient by wrapping messages in layers of public-key cryptography, and relaying them through a path composed of " mixes." Intermediate mixes decrypts, delays, and re-orders messages before relaying them onward. Modern Anonymous system designs can be classified into high-latency and low latency designs.

One of the oldest low-latency designs is single-hop proxies such as the **Anonymizer** [2].Users has to contact the trusted anonymizing proxy which strips the data's origin before relaying it but it is vulnerable if the adversary can observe all traffic entering and leaving the proxy.

The low-latency designs [3] handle a variety of bidirectional protocols. They also provide more convenient mail delivery than the high-latency anonymous email networks, because the remote mail server provides explicit and timely delivery confirmation. One of the issues with these systems arises as these designs vulnerable to an active adversary who introduces timing patterns into traffic entering the network and looks for correlated patterns among exiting traffic. Although some work has been done to frustrate these attacks, most designs protect primarily against traffic analysis rather than traffic confirmation.

High-latency System like **Mixminion** [4], **Mixmaster** [5] increases anonymity at the cost of introducing large and variable latencies. High-latency networks resist strong global adversaries, but introduces too much delays for interactive tasks like web browsing, Internet chat, or SSH connections

IV. Conclusion

P2P can be used for accessing web through network of volunteer P2P users. There is lot of issues to consider for such scheme to realistically implemented and usable. There can be numerous economics benefits achievable through this scheme such as " user defined routing" ,User service providers as compared to Cloud computing.

V. References 참 고 문 헌

1. D. Chaum. Untraceable electronic mail, return addresses,and digital pseudo-nyms. *Communications of the ACM*, 4(2),February 1981.

2. http://www.anonymizer.com/

3. http://www.torproject.org/

4. G. Danezis, R. Dingledine, and N. Mathewson. Mixminion:Design of a type III anonymous remailer protocol. In *2003IEEE Symposium on Security and Privacy*, pages 2- 15. IEEE CS, May 2003.

5. U. Moller, L. Cottrell, P. Palfrader, and L. Sassaman. Mixmaster Protocol — Version 2. Draft, July 2003. http://www.abditum.com/mixmaster-spec.txt

6. http://sourceforge.net/projects/ipanon/files/ipanon-0.3/ipanon%200.3/ipanon-0.3.tar.gz/download