Review “Anonymous Routing”

Name: Wenhui Zhang
Email: wuz49@ist.psu.edu

Paper Name：

Reed, M. G., Syverson, P. F., & Goldschlag, D. M. (1996, December). Proxies for anonymous routing. In *Computer Security Applications Conference, 1996., 12th Annual* (pp. 95-104). IEEE.

Contribution:

This paper propose onion routing, which is an infrastructure resistant to traffic analysis. Thus this infrastructure achieves anonymous connections.

Motivation:

Internet surveillance techniques such as traffic analysis technique could reveal users’ privacy. Security of corporate and governmental users also hurts. Encryption does not work for this situation, as packet headers could still reveal identities of users. Thus end-to-end anonymity connection technique is needed for public internet.

Related works:

Two extensively used approaches for communication anonymity are mixes and proxies. Mixes randomly permutes and decrypts inputs to prevent adversary from getting information on which ciphertext corresponds to a given message. In mixes, each layer of message requires public key crypto, which is time consuming and not appropriate for low latency apps. Proxy makes channels appear to come from proxy, not true originator, and achieves anonymous connection. However, it suffers from single point of failure.

Methodology:

Onion routing is a distributed anonymous communication service, which achieves anonymous connection using an overlay network. This overlay network allows users to improve their privacy and security on the Internet. To create an onion, the router at the head of a transmission selects a number of onion routers at random and generates a message for each one, providing it with symmetric keys for decrypting messages, and instructing it which router will be next in the path. (1) The client make request to application proxy, and onion proxy gives the order to choose random router based on the encryption algorithm; (2) The sender transmit equal-length messages encrypted with the symmetric keys specified in the onion and deliver the message on path; (3) When message leaves router, it peels off a layer using symmetric key; (4) The last router peels off the last layer and sends the message to the intended recipient; (5) When the connection is broken, all information about the connection is cleared at each Onion Router.

Results:

This implementation uses proxy servers, and is on Sun Solaris 2.4. In this implementation, servers could run in user space. And there is no need to build proxies for every application, as SOCKS compliant TCP. It has flexible exit policies, each node chooses what applications and destinations can emerge from it.

Take away:

Onion routing is a good anonymous communication service technique for building privacy concern P2P system.