Anonymous Connections and Onion Routing

Michael G. Reed, Paul F. Syverson, and David M. Goldschlag

Abhishek Srivastava
Student ID: 861307778

May 26, 2017
CS 204, Spring 2017

Review:

This paper presents methodology called onion routing which can be used to protect and prevent the anonymity of the end-users from variety of internet services against both eavesdropping & traffic analysis from both inside and outside the networks. Onion routing provides a bi-directional and real-time communication which is similar to TCP/IP connections. Onion routing can be used for anonymous web browsing, anonymous communication etc.

In onion routing instead of making socket connections directly to target machine/network, connections are made through sequence of machines called *onion routers*. All connections are anonymous in *onion routing network* between initiator and responder. All identifying information is removed from data stream before sending it over anonymous connection. Onion network uses permanent socket connections and over this packets are multiplexed. Sequence of onion routers are defined at connection setup but each onion router only identify its previous and next hops in route. Data passed along connections are different at each router and cannot be used tracked since routers donot cooperate correlating data stream they see.

Initiating application makes socket connection to *application proxy* which then connects to *onion proxy* whose job is to define route and construct *onion* layered data structure whic is then to be passed to *entry funnel* and then it is multiplexed over onion routing network. An *onion router* when receives an *onion* peel off it layer, identify next hop and send embedded onion to that route and last router forward it to *exit funnel* which pass data between onion routing network and responder. Each onion layer also carry key seed materials from which keys are generated for crypting data send to forward and backward along anonymous connection. It has advantage over link crypting.

Onion routers only keep track of received onino until they expire and are never forwarded so cannot be used to uncover route information.Paper also proposes multiple configuration which should be done for onion routing such as Firewall configuration, Remote proxy configuration and Customer-ISP configuration.

Comments:

- This is a well written paper that proposes an interesting way to solve the anonymous routing problems, but like all systems, it are prone to certain weaknesses. The major weakness of onion routing size of the onion reduces when destination is near hence it can be inferred by compromised onion router.

- Packet delivery is also not ensured by onion routing in case when an onion router fails on the way and message will never reach destination and new connection will be needed to setup.

- Packet delivery will be slow since at each onion router for both forward and backward packet transmission we need to decrypt and encrypt data. But that's not bad trade for securing anonymity/connection.