Weekly Report 1

Pankaj More (Y9227402)

25th Feb, 2013

Papers Read

- Radhakrishnan, Sivasankar, et al. “TCP fast open.” Proceedings of the Seventh Conference on emerging Networking EXperiments and Technologies. ACM, 2011.

Summary

TCP handshakes are a significant source of delay in short-lived tcp requests since data cannot be transmitted until the 3-way handshake is complete. This paper deals with a new protocol called the TCP Fast Open which allows data transfer even before the handshake is complete thereby decreasing page load time by up to 40 %

The main idea in the paper is the use of a security token to prevent attacks based on sending data before handshake completion. The security token is basically an encrypted byte string containing the client’s IP address. When the client initiates a tcp connection for the first time, the server generates a security “cookie” for the client and sends it with the ACK. The client caches the cookie and uses it for subsequent connections. On the server side, the server will verify that the cookie is “correct” and then accepts the data packet and delivers it to the server application. If the cookie validation fails, the data is dropped and a SYN-ACK is sent only acknowledging the SYN sequence number. The connection then proceeds through a regular 3WHS.

Since the main goal of TCP Fast Open is to allow data exchange during the initial handshake without introducing any security vulnerabilities, the paper talks about various attacks and how their protocol takes care of those attacks.

The simplicity in its design and its reasonable defense against various DOS attacks has made it easily deployable. In fact, since Linux kernel 3.7 as of November,2012 , TCP Fast Open support has already been added and it is being used in real-world.