San Francisco State University
Department of Computer Science

Technical Report SFSU-CS-TR-06.08

Title: Caching TCP Options With Syn_Cookies in the Linux 2.6 Kernel

Author(s): Jensen Galan

Date: 5/4/06

Abstract:
Syn_cookies are a defense mechanism built-in to the Linux Kernel designed to thwart a SYN Flood Denial of Service (DoS) attack. Syn_cookies circumvent the need to allocate state information by hashing a 32-bit cryptographic challenge that a client requesting a connection must echo in the final part of the 3-way handshake. This enables servers to accept new connections in the midst of a SYN Flood attack. While this 32-bit hash neutralizes the SYN Flood DoS attack, any TCP options negotiated in the 3-way handshake are lost. This leads to a degradation in the Quality of Service (QoS). In order to maintain the TCP options necessary for high performance in today's high bandwidth/high latency networks, this work proposes and implements a BSD-style SYN_Cache in the Linux Kernel. This mechanism is used in conjunction with syn_cookies to cache and retrieve the TCP options negotiated by legitimate clients. A small number of bytes per cache entry are allocated and a global hash table is used for speedy lookups. Standard HTTP Performance Benchmarks show trivial performance degradation during a heavy SYN Flood attack while preserving the TCP options of window scaling, timestamping, and selective acknowledgments (SACK).

Keywords: Linux, Kernel, Linux 2.6 Kernel, syncookies, syn_cookies, SYN Flood, DoS, DDoS, TCP options, SYN Cache, Denial of Service, Distributed Denial of Service, 3-way handshake, Network Security