Abstract

Macroscope is a network-based intrusion detection system that uses Bottleneck Verification to detect user-to-superuser attacks. Bottleneck Verification (BV) detects novel computer attacks by looking for users performing high privilege operations without passing through legal "bottleneck" checkpoints that grant those privileges. Macroscope's BV implementation models many common Unix commands, and has extensions to detect intrusions that exploit trust relationships, as well as previously installed Trojan programs. Bottleneck Verification performs at a false alarm rate more than two orders of magnitude lower than a reference signature verification system, while simultaneously increasing the detection rate from roughly 20% to 80% of user-to-super-user attacks.