Abstract

Defending networks against today’s attackers is especially challenging for modern intrusion detection/prevention systems for two reasons: the sheer amount of state they must maintain, and the possibility of resource exhaustion attacks on the defense system itself. Our work shows how to cope with these challenges in the context of a TCP stream normalizer whose job is to detect all instances of inconsistent TCP retransmissions.
TCP/IP Data Normalization


Index Terms

Computer Science Advances In Computer Application

Keywords
Tcp Ip Data Normalization