Title

Fast Content-Based Packet Handling for Intrusion Detection

Authors
Fisk, Mike
Varghese, George

Publication Date
2001-05-07

Peer reviewed

Fast Content-Based Packet Handling for Intrusion Detection

Mike Fisk*
mfisk@lanl.gov
Los Alamos National Laboratory

George Varghese
varghese@cs.ucsd.edu
Computer Science & Engineering Department
University of California San Diego

Abstract

It is becoming increasingly common for network devices to handle packets based on the contents of packet payloads. Example applications include intrusion detection, firewalls, web proxies, and layer seven switches. This paper analyzes the problem of intrusion detection and its reliance on fast string matching in packets. We show that the problem can be restructured to allow the use of more efficient string matching algorithms that operate on sets of patterns in parallel. We then introduce and analyze a new string matching algorithm that has average-case performance that is better than the best theoretical algorithm (Aho-Corasick) and much better than the currently deployed algorithm (multiple iterations of Boyer-Moore). Finally, we implement these algorithms in the popular intrusion detection platform Snort and analyze their relative performance on actual packet traces. Our results provide lessons on the structuring of content-based handlers, string matching algorithms in general, and the importance of performance to security.

The full paper is available by contacting the first author by e-mail at mfisk@cs.ucsd.edu.

[*] This work was supported by the U.S. Department of Energy under contract W-7405-ENG-36 with Los Alamos National Laboratory and a UC MICRO fellowship at UCSD.