INNOVATION PARTNERSHIPS
UNIVERSITY OF MICHIGAN

Framework and Methods for Online Network Monitoring, Statistical Analysis and Forensics of Data Streams

TECHNOLOGY NUMBER: 7070

Technology ID
7070

Category
Software
Software & Content

Inventor
George Michailidis
Michael Kallitsis
Stilian Stoev

Further information
Ashwathi Iyer
ashwathi@umich.edu

View online page

OVERVIEW

Predicts, analyzes, and responds to network attacks in a rapid manner

- Allows real-time visualization of large amounts of data
- Runs on inexpensive, commodity hardware

BACKGROUND

Modern internet infrastructure has several weaknesses which can be exploited by malicious groups or individuals. Distributed denial of service (DDoS) attacks, while relatively simple, can compromise government and business servers, costing hundreds of thousands of dollars. There are even services which can be bought for the purpose of DDoS attacks. Protecting against Distributed Denial of Service (DDoS) attacks requires a multi-layered approach involving network infrastructure, software configuration, and proactive monitoring. It is essential to have ways to fight against such attacks and improve network security, and a need exists for more effective and less expensive alternatives to meet these demands.

INNOVATION

Researchers have developed an invention that helps to predict, analyze, and respond to network attacks in a rapid manner. This technology helps to identify incipient and ongoing attacks through the analysis and visualization of network traffic data. Using a powerful new platform, the technology is able to scan all incoming packets at up to 25 Gigabytes per second

on commodity hardware. This approach also allows the identification of the sources and scopes of incoming attacks. While there are some companies which provide similar services, this technology offers substantial advantages by allowing real-time visualization of large amount of data on non-specialized and comparatively cheap hardware. The application may be used for internet traffic monitoring, automatic intrusion detection, or network forensics for rapid identification of attack victims and originators. Furthermore, the software runs on inexpensive, commodity hardware and is therefore orders of magnitude less expensive than existing solutions.

ADDITIONAL DETAILS

The technology is available through a GNU GPL v3.0 license