UNIVERSITY OF MARYLAND
VENTURES
UMVENTURES.ORG

TECHNOLOGY

Detecting DDoS Attacks in Stub Domains

OVERVIEW

Denial of Service (DoS) attack technology is developing in an open-source environment and is evolving rapidly. Technology producers, system administrators, and users are improving their ability to react to emerging problems, but they are behind and significant damage to systems and infrastructure can occur before effective defenses can be implemented.

Researchers at University of Maryland have come up with an innovative technique for detecting "Distributed Denial of Service (DDoS)" attacks without changing the existing routing infrastructure. This new detection system (using TCP packets) has several advantages over currently existing technology in terms of:-
1. Flexibility: can be deployed in single and multi-homed stub networks.
2. Performance: high detecting capability even with the network having asymmetric traffic or very low flow rates.
3. Efficiency: very little processing and communication overhead.
4. Robustness: detects different types of attacks on traces with orders of magnitude difference in packet rates without parameter tweaking.

Inventors have performed extensive packet level simulations under different attack scenarios. Observations are listed below:
1. Detect attack flows that are one-third the intensity of an average flow of in the network.
2. Detect attack for asymmetric traffic in multi-gateway networks if the attack rate is at least five times the average flow rate in the network.

Researchers have even extended this detection technique to detect subnet attacks and were successful in detecting attacks that target hosts in large subnets and in the presence of non-attack traffic to other hosts in the subnet. The experiments conducted for single domain networks revealed that the scheme can detect attacks with aggregate flow intensity equal to the average flow in the network in less than a minute. The experiments for multi-domain stub networks demonstrated that the scheme detects attacks even when the network has four gateways and when up to 50% of flows are asymmetric.

For additional information please contact the Office of Technology Commercialization, University of Maryland. Phone: 301-405-2924

APPLICATIONS

DDos dectection, network security

ADVANTAGES

detects DDoS attacks in situations of traffic flow relative to normal traffic

CONTACT INFO

UM Ventures
0134 Lee Building
7809 Regents Drive
College Park, MD 20742
Email: umdtechtransfer@umd.edu
Phone: (301) 405-3947 | Fax: (301) 314-9502

Additional Information

INSTITUTION

University of Maryland, College Park

PATENT STATUS

Not Filed

LICENSE STATUS

Available for exclusive or non-exclusive license

CATEGORIES

- Information Technology

EXTERNAL RESOURCES

- US Patent 8,397,284

IS-2006-004