Faculty of Computer Science 2007-2008 Seminar Series

Protecting Network QoS against DDoS Attacks

By

Dr. Wei Lu

Researcher at the Information Security Centre of eXcellence for the Faculty of Computer Science, University of New Brunswick and an Adjunct Assistant Professor at the University of Victoria for the Department of Electrical and Computer Engineering

Wednesday, October 10th, 2007
3:30pm
ITC317

With more than a million hosts already controlled by hackers, Distributed Denial of Services (DDoS) attacks by Botnets are becoming a severe threat on current Internet infrastructure. Traditional approaches against DDoS attacks on the victim end tend to generate high false alarm rate and thus lead to more collateral damage on network quality of service (QoS). In this talk, NetShield, an adaptive DDoS detection and mitigation system, is presented in order to address limitations of current DDoS defense approaches. NetShield system is composed of two components: detection module and mitigation module. In detection module, CUSUM algorithm and EM based clustering algorithm are applied to identify DDoS intrusions in realtime; In mitigation module, filtering rules are set based on historical web access and are activated once the front detection module triggers DDoS alarms. On a lab evaluation with German Telecom, a Botnet with 100 attackers was simulated to generate the highly structured DDoS traffic and the stand-alone NetShield system successfully detected and blocked all malicious traffic to the target video server in a short time, and thereby guaranteeing the reliable network services by ISP.

****
STUDENTS ARE ENCOURAGED TO ATTEND
****