**King Fahd University of Petroleum & Minerals**
**College of Computer Sciences and Engineering**

# CSE 550 – Computer Network Design (3-0-3)
## Spring 2007 (Term 062)

## Projects Descriptions

**Project 1 Title: DoS Attacks on Firewalls (DAF)**

**Project 1 Description:** The project involves developing techniques to probe firewalls for the purpose of discovering their configuration, and then launching intelligent DoS (Denial of Service) attacks on them. This project should also demonstrate how this can work on an existing network's firewall. These attacks will target the default rule or the last-matching rules. The default rule is typically the last rule in the rule set, i.e. ACL (Access Control List) of the firewall. The last-matching rules are those that exist at the bottom of the firewall rule set. The last matching rules, including the default rule, require the most CPU processing power. In order to discover remotely these rules, the attacker probes intelligently the firewall. This project will demonstrate how these rules can be discovered and how such attacks can be devised. The students will learn the basics of firewalls and ACLs. They will also study and survey existing firewall attacks. They will then identify, in details, the technique for the proposed probing, discovery, and intelligent DoS attack. The technique would include the algorithm and code for determining the default rule or the last-matching rules in a firewall rule set. Then, they will build an experimental setup of a typical and realistic network with Linux Netfilter firewall. They will then run a test of the attack to discover the firewall default rule or the last-matching rules. Then, they will devise the second component of the code to launch a set of DoS attacks aimed at triggering the last-matching rules of the firewall. Finally, they will measure the effectiveness of the attack by examining the performance of the firewall during the actual attack. The performance will be measured in terms of attack rate and firewall's throughput and CPU utilization.

**Project 2 Title: Countermeasures for DoS Attacks on Firewalls (CDAF)**

**Project 2 Description:** The project involves developing effective remedies and countermeasures against DoS (Denial of Service) attacks on firewalls, and demonstrating how this can work on an existing network's firewall. These attacks target the default rule or the last-matching rules. The default rule is typically the last rule in the rule set, i.e. ACL (Access Control List) of the firewall. The last-matching rules are those that exist at the bottom of the firewall rule set. The last matching rules, including the default rule, require the most CPU processing power. In order to discover remotely these rules, the attacker probes intelligently the firewall. This allows the attacker to devise intelligent DoS attacks. This project will demonstrate how such attacks can be counter-measured. The students will learn the basics of firewalls and ACLs. They will study and survey existing firewall attacks and countermeasures to DoS attacks. They will also investigate the effectiveness of the existing countermeasures for firewalls to deter related DoS attacks. Then, they will investigate possible remedies and countermeasures against DoS attacks and the schemes to discover last-matching rules. They will then identify, in details, the technique for the proposed countermeasure for such DoS attacks. They can do this using one or both of the following:

- Identify different possible solutions and countermeasures to obscure and hide the firewall's last-matching rules, and thereby disallowing their discovery by attackers (avoidance and prevention).
- Devise countermeasures that can adapt dynamically to changes in the network's behavior due to being attacked (i.e., after DoS attacks have been launched) (detection and recovery).

Finally, they will study the effectiveness and performance of the countermeasures quantitatively. This will be carried out using an experimental setup of a typical and realistic network with a Linux Netfilter firewall.