

**Tutor: Timo Kiravuo**

### **Topic 1: How Protocols Behave When Idle?**

The classic end-to-end argument for the Internet assumes that the state of a (TCP) connection is only maintained in the endpoints and not in the network infrastructure. Current vision has added to this that the infrastructure may maintain soft state. Firewalls maintain access for opened connections, but for how long? To get some insight to this, I would like a student to find out how protocols behave when idle. The task would be to read the specifications for some common protocols, like TCP, HTTP, IMAP, POP(3), SSH, TLS, NNTP and IRC. Also a brief literature search should be made to figure out how current firewalls and NAT translators decide how long to maintain the state, to give the paper some depth.

This topic is fairly straight forward and demands work, but the structure is obvious.

Sources: relevant RFCs

### **Topic 2: Firewall Rule Aggregation and Optimization**

Firewall rule sets tend to grow complex and hard to analyze. They consume a lot of CPU power, too. Some rules may conflict or be redundant. The student's task is to find out what methods are available for making adding a new rule to an existing firewall rule set.

This topic demands some thinking and analyzing, the formal rules are not the easiest to get started with, however the power of formalism is strong and the student is likely to benefit from the extra effort.

Sources:

author = {Hazem Hamed and Ehab Al-Shaer},  
title = {Dynamic rule-ordering optimization for high-speed firewall filtering},  
booktitle = {ASIACCS '06: Proceedings of the 2006 ACM Symposium on Information, computer and communications security},  
doi = {<http://doi.acm.org/10.1145/1128817.1128867>}

### **Topic 3: Finding Home**

In the current IPv4 world we can not guarantee to have a fixed IP address. Thus when the residents of a home network travel, with their laptops and mobiles, they want to contact the services at home, but don't know where the home is. The goal of this paper is to review several methods for finding the home network. Dynamic DNS is the obvious solution. Rendezvous servers should also be discussed. P2P networks might also provide a solution. Other solutions exist for sure. Criteria needs to be decided on, also.

This topic is not too difficult on the content side, but has the problem of being open-ended and it can easily grow to an un-manageable mess. Thus the student should keep a tight control in their work and communicate with the tutor if the

problem starts to get out of hand.

#### **Topic 4: Methods for firewall control**

Instead of a static firewall the home firewall can be made dynamic. This means allowing the users or their applications to create and modify firewall rules. Some methods for this exist already, like UPnP and the NAT/FW NSIS protocol. The student's task is to write a review of existing methods for controlling the firewall. The student should think about the controller being inside or outside the firewall and analyze the different solutions in this regard.

This topic is fairly straight forward and will produce a simple report with reasonable work. However the basic topic might be too simple for a good grade, additional analysis work is needed for a better grade.