# An order-independent approach for the design and management of firewall ACLs

Artem Voronkov
Karlstad University

Firewalls are an essential component of network security, helping to provide protection against external threats.

The objective of this work is to simplify the design and management of firewall Access Control Lists (ACLs). To configure a firewall properly is a very challenging task. These configuration files could be unreadable even for system administrators. A part of this complexity comes from the structure of these files because it is such that the higher the position of a rule in this rule set, the higher priority it has. Challenging problems arise when you add a new rule to the policy, because of a need to find a proper position where to place it. Misconfigurations will sooner or later likely lead to an inappropriate system security. To cope with this we need to find a way to reduce resources spent on support and improve the scalability of rule sets.

We propose for this problem an order-independent rule sets solution. It consists of two parts: a visualisation tool that explicitly represents security policy without specifying the order of rules and a special language that will transform the list of rules from an order-independent state to an order-dependent. Firewalls operate in the usual way, because they work with the same type of files they worked before. As for users, it could be easier to cope with the rules, since they are represented in a more readable form.