TID – Modern Theoretical Computer Science Firewall Rules Discovery and Generation

Matej Kollár

October 8, 2012

I will give presentation based on [1], mainly the part about firewall policy discovery and generation.

Blind policy discovery is an important problem, as firewalls are cornerstones of network defense mechanisms. Attackers may already use described theory and techniques and therefore network administrators should study and understand them as well.

Exhaustive search can give us exact answer, but it is infeasible as complexity grows exponentially with number of bits describing our search space. It is also bad for attackers, as it is easily detectable. Intelligent techniques can help, but we will have to sacrifice exactness.

Boolean function learning from examples is of our interest, as it provides us with basic tools. And as we are dealing only with a subproblem, additional techniques and heuristics can be used. Intelligent samples generation, either initial or based on firewall response to refine already discovered policies, is also important.

Need to evaluate effectiveness of developed system leads to question of preparing real-world-like policies (real policies are hard to get hands on in quantity required for proper benchmarking and are often considered confidential). Author of [1] uses probabilistic context-free grammars and generation based on given traffic trace. I will present first approach.

Connection to TID

Use of formalisms:

- Formal description of model used to describe network flow processing.
- Probabilistic context-free grammars.

Connection to my Doctoral Thesis

- Networking.
- Device configuration.
- Formalisms.

References

[1] Taghrid Samak. *Discovery, Generation and Analysis of Network Policy Configurations.* PhD thesis, DePaul University, Chicago, IL USA, October 2010.