Review “Fireman”

Name: Wenhui Zhang
Email: wuz49@ist.psu.edu

Paper Name：

Yuan, L., Chen, H., Mai, J., Chuah, C. N., Su, Z., & Mohapatra, P. (2006, May). Fireman: A toolkit for firewall modeling and analysis. In *Security and Privacy, 2006 IEEE Symposium on* (pp. 15-pp). IEEE.

Contribution:

In this paper describes a toolkit named as FIREMAN, which uses static analytics techniques to check misconfiguration of policy violations, inconsistencies, inefficiencies etc.. In this paper: (1) a comprehensive study of misconfiguration for distributed and single firewalls is described; (2) a static analysis on firewall rules are done at intra-firewall, inter-firewall and cross-path levels; (3) using binary decision diagram based FIREMAN implementation, previously unknown misconfigurations are found.

Motivation:

While firewall is an important and widely used solution for network security, misconfiguration of firewall is common and this weakens the desired security level for network. There are several challenges on correct configuration of firewalls: (1) it is hard to analysis firewall rule policies in high level as the rules are written in platform specific, low level languages; (2) it is hard to analysis firewall actions among large amount of rules; (3) firewall components are deployed on multiple network components, with dynamic routing of packets, it is hard to figure out which set of firewall rules are applied during this process.

Related works:

Works has been done using FDD for reducing configuration size; works are also done using BDD for faster lookups; works has been done for policy conformance etc.

Methodology:

There are some errors defined by FIREMAN: (1) policy violation, which means configuration violates the high-level semantics of the rules; (2) Inconsistency, which includes shadowing, which is an earlier rule makes a later rule impossible; (3) Inefficiency, which includes generalization and correlation.

Using the previously defined variables and errors, FIREMAN makes formal logic statements about firewall rules: (1) Pj belongs to Rj, this is a good rule; (2) Pj belongs to Dj, this is a shadowing rule; (3) Pj and Dj overlaps, this is correlation.

Where, Aj stands for All packets accepted before the jth rule; Dj stands for all packets denied before the jth rule; Fj stands for all packets sent to a different rule path before the jth rule; Rj stands for all packets not covered by the above by the jth rule; I stands for input.

Results:

FIREMAN uses static analysis of rule bases techniques and detects violations, inconsistencies, and inefficiencies of firewall rule policies. It proves that BDD approach is good.

Take away:

Define a firewall policy generation mechanism using static analysis is hard, as both violations, inconsistencies, and inefficiencies should be analyzed on rule bases.