Adaptive NIDS in Hardware

Farnaz Gharibian, Junaid A. Khan, and Ali Ghorbani
(w99bg,Junaidk,Ghorbani@unb.ca)

Introduction

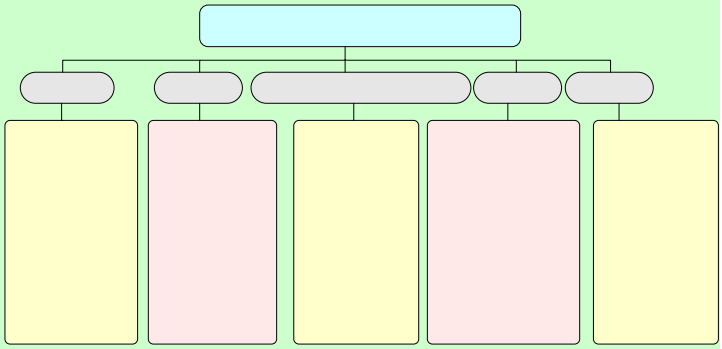
Network Intrusion Detection Systems (NIDS) identify attempts that compromise confidentiality, integrity, and availability of computer systems or computer networks. This research will target the efficient hardware implementation of NIDS with adaptive reconfiguration.

Motivation

- Software based NIDS have limited throughput for supporting high speed network with Gigabit rate.
- With continuous addition to network attack types, it is necessary to adaptively update detection rules.
- Adaptive detection rule update needs fast changes in hardware based NIDS.

Current Approaches

Almost all current hardware based NIDS solutions mainly focussed on efficient pattern matching in hardware



What is Missing?

- Very few solutions support complete NIDS in hardware.
- The high throughput approaches normally use reconfigurable discrete logic (RDL). With RDL it is not feasible to adaptively change rules.
- Most of the solutions either support fixed patterns or regular expressions, whereas we need to check both. Regular expression based solution can be used to detect fixed length pattern but normally needs larger logic.
- Most of the approaches are optimized for pattern matching but not for overall NIDS.
- Fast rule updates with high throughput is hard to achieve simultaneously.
- Support of large number of rules is not possible with many proposed approaches.
- None of the proposed architecture, in our knowledge, supports “offset” and “depth” options in SNORT, for content pattern matching.

Research Goals

Short Term

- A complete optimized System on Chip (SoC) NIDS sensor architecture.
- A hardware/software interface for the NIDS architecture.
- Support for adaptive changes in detection rules.
- Increased throughput by filtering data that does not need content pattern matching.

Long Term

- A pattern matcher that provide high throughput without needing any hardware reconfiguration.
- Support for multiple pattern matching, and offset & depth options.

Achievements

- Completed initial but ongoing literature survey on hardware based NIDS.

Suggestions! Comments! Questions?

network security laboratory

UNIVERSITY OF NEW BRUNSWICK UNB