

THE ELUSIVE EVOLUTIONARY IDS

Applying Genetic Algorithm to Intrusion Detection and
Prevention

Kyle Loomis Doug White
Roger Williams University

Alan Rea
Western Michigan University

Louis Glorfeld
University of Arkansas

The Standard IDS /IPS Philosophy

- Human Input is the Standard
 - Identify Threats via Observation and Experience
 - CERT.ORG
 - SANS.ORG
 - Etc.
 - Develop Mitigating Controls
 - Signature Detection
 - Firewall ACLS

Evolutionary Computing and IDS

- AI has long been sought as an automated technique for analysis of networking activity
 - Neural Nets
 - Expert Systems
 - Etc.

Genetic Algorithms

- Genetic Algorithms attempt to “evolve” solutions to complex problems
- The best traits of a generation of solutions are retained and the algorithm hill climbs towards an optimal solution
- Random mutations are introduced to avoid dead end solutions and to ensure a global solution is obtained.

Genetic Algorithm in IDS/IPS

- The current firewall configuration is a massive search space of potential states.
- In the space of all possible states, an optimal configuration exists.
 - Maximizes legitimate activity while minimizing illicit activity.

Using Genetic Algorithms for Network Intrusion Detection (Li):

- Encode the state of a single network connection or firewall rule (source IP, destination IP, protocol, connection time, source and destination ports, etc.) as a bit string representing a possible solution.
- Use the DARPA dataset (which contains both legitimate and malicious packets) as a training solution.
- Evolve firewall rules using a fitness determinant.

Our Approach

- Use Java and Shorewall to attempt to evolve rules based on traffic.
- Ideally, rules should be evolved to assess a given packet for legitimacy.
- This might lead to an approach to adaptive stateful firewalling.

Findings

- A given optimal set of rules was only valid in a static situation.
- As the environment evolved rapidly (new attacks and changes), the evolution of new rules could not keep pace.
- The time required to analyze state space of all packets exceeded the necessary response time.
- It may be useful for “pruning” existing rule bases.

Possibilities/Future Research

- The exploration of hybrid firewalling using both GA and static (expert) systems to assess and evaluate packets.
- Adaptation of signatures found in SNORT and other IDS to GA evolutions.

Questions?

- All slides found at www.whitehatresearch.com after the conference.
- Doug.white@whitehatresearch.com