IDS Based on Automated Fingerprinting

Awais Aslam Attique Dawood

March 2, 2012

1 Network Intrusion Detection Systems

Intrusion detection systems monitor network traffic to detect malicious activities. Malicious activities can be an outside attempt to gain control of a host, a worm spreading across the internet or suspicious traffic from a local host etc.

2 Types of IDS

IDS are basically either signature–based or anomaly–based. Signature–based IDS need to know specific signatures of malicious content (specific strings or code) beforehand. Anomaly–based IDS identify abnormal patterns in network traffic for detecting suspicious activities.

3 Automated Signature Generation

Sumeet et. al. [1] have presented a method to quickly generate signatures based on anomalous behaviour of worms spreading across the network in order contain them. The method is based on an observation that the probability of unique strings occuring in normal traffic directed to diverse destination is very low.

Intrusion detection techniques used by Snort and Bro rely on vulnerabilities that are well–known by comparing with a database. Automated worm detection assumes that some part of malicious program or code is invariant, i.e. it does not change in order to hide itself. The invariant portion of worm can be used to create signatures since it will occur frequently in network traffic.

The goal of this project is to come up with an implementation of the signature generation algorithm in [1].

References

[1] S. Singh, C. Estan, G. Varghese, and S. Savage, "Automated worm fingerprinting," in *OSDI*, pp. 45–60, 2004.

[2] `http://en.wikipedia.org/wiki/Intrusion_detection_system`.