

Data Fusion Support for Intrusion Detection and Prevention

Mohsen Beheshti, Richard A. Wasniowski

*Computer Science Department, California State University Dominguez Hills
{mbeheshti, rwasniowski}@csudh.edu*

The main problem with current intrusion detection and prevention systems is high rate of false alarms triggered off by attackers. Effective protecting the network against attacks remains problem in both research and the computer network managing professionals. Improved monitoring of malicious attacks will require integration of multiple monitoring systems. In our project we are analyzing potential benefits of distributed multi sensor systems for intrusion detection.

Our main purpose for this work is to examine how to integrate multiple intrusion detection sensors in the order to minimize the number of incorrect-alarms. The first problem is how to integrate data from multiple sensors, and the second how to identify most important data provided by multiple sensors. We are currently developing series of analytical models to use potential benefits of multiple sensors for reducing false alarms.

The purpose of this presentation is to discuss implementation of prototype multisensor based intrusion detection system. We are especially interested in analyzing traffic that has an abnormal or malicious character and should prompt a closer look. A specific feature of the model is that the systems use multiple sensors to process log files. This reduces the overhead in a distributed intrusion detection system.

The Snort [1] based multiple sensors system monitors two networks. Our configuration allows generating Snort events with identical timestamps to ensure that we can successfully merge data from multiple snort sensors with identical timestamps. On both networks one web server is an Intel-based PC running Microsoft Windows 2003, the second web server is Centos based Linux system. Each Snort sensor is an Intel-based PC running CENTOS4.3/4.4 with Snort 2.3/2.6 and MySQL 4.3.10. Snort sensors are configured with identical rule sets to run in Intrusion Detection System mode, and to log to the MySQL database and alerts log files. In addition to monitoring online traffic we simulate attacks and the attacker system is an Intel-based PC running Fedora Core (FC4) laptop computer.

The system is implemented using Open Software whenever possible such as Snort, HoneyPot, MySQL etc. We have collected a large amount of data such as alert logs and multiple MySQL databases and improved snort rules design and we are currently finalizing processing those sets of data. This project is described in details on web site [4].

On the whole, our information fusion based intrusion detection and prevention model is in fact a prototype and needs to evolve into more mature and efficient model. Future work emphasizes a revisit of database design to allow more efficient data fusion from multiple sensors.

Research is partially supported by NGA and DoD.

References

- [1] Beale, Jay, 2004. Snort 2.1 Intrusion Detection, Second Edition, Syngress.
- [2] Richard Bejtlich, "The Tao of Network Security Monitoring: Beyond Intrusion Detection", 2004 by Addison-Wesley.
- [3] Cox, Kerry and Gerg, Christopher, 2004. Snort and IDS Tools, O'Reilly Media, Inc.
- [4] csc09.csudh.edu/csl