**Security Technology Tools II**

**ITM437 Information Security and Technology**

**Professor: Dr. Abbas Yousefi**

**By Odiscious Dozier**

**Trident University**

**SLP 03**

INTRODUCTION

With the profound increase of data in the world, the threats of cyber-crime are imminent and growing. The need for information security is not only clear, but an entire architecture of defense is required to fight against various threats. IDSs have proven to be effective, but flawed in many ways. This discussion addresses the, motivations for evaluating IDPSs, measureable IDPS characteristics, examples of some current IDPS evaluation efforts, and challenges in evaluating IDPSs.

MOTIVATIONS FOR EVALUATING IDPS

Quantitative evaluations is conducted through the systematic empirical investigation of observable phenomena. With regard to IDPS, a finite amount of data is collected and statistical analysis is conducted to help give useful results for a large array of potential customers (Given, 2008).

Acquisition managers benefit from such information and, in practice, are able to improve the process of system selection. Traditional methods which have proven to be less than optimal are all too often based on the claims of subject matter experts (SMEs) employed by various vendors. Other sources like limited-scope reviews in trade magazines have also proved to be an unreliable source of information (Mell, 2003).

Security analysts, who review the output of IDSs, benefit from such information when seeking to understand and report on various topics related to information security within their organization’s realm of networking concerns – internal or external or both. The likelihood that alerts will be generated when a particular kind of attack is initiated, is an example of such a concern (Goodall et al., 2004).

“R&D program managers need to understand the strengths and weaknesses of currently available systems so that they can effectively focus research efforts on improving systems, and measure their progress” (Mell, 2003).

MEASURABLE IDPS CHARACTERISTICS

This section is a list of a partial set of measurements that can be made on IDSs. Focus is given to those measurements that are not only quantitative, but also relate to accuracy of detection.

COVERAGE

“This measurement determines which attacks an IDS can detect under ideal conditions. For signature-based systems, this would simply consist of counting the number of signatures and mapping them to a standard naming scheme. For non-signature based systems, one would need to determine which attacks out of the set of all known attacks could be detected by a particular methodology” (Mell, 2003).

As the White House shared, in 2009, “cybersecurity risks pose some of the most serious economic and national security challenges of the 21st Century" (“Cyberspace Policy Review”, 2009). The large number of cyber-attacks, the number of dimensions that form each attack, their individual goals, the effects of the attacks, and the residual evidence of the attack make measuring the coverages of an IDS difficult, but necessary (Han et al., 2014).

The various cyber-attacks have a culmination of threat areas, located within an organization or external to it. Investigating cybercrimes has revealed that each attack has its own goal; for example, denial of service, penetration, or scanning attacks. The cyber-attacks work against the, software, operating system, or protocol, and they are designed with malicious specificity. They are precise and particular to their intended victim (Han et al., 2014).

Attacks may also be defined by researchers as having the finest level of granularity. This is where each target has a target configuration, like a certain version of a protocol, and a mode of operation that are very specific (Mell, 2003).

Additional struggles with obtaining accurate coverage measurements include obstacles like site-precedence. This is where one site might give a higher level of importance to a particular cyber-attack and another site will not share the same level of concern for such an attack. An E-commerce site, for example, might be very interested in detecting distributed denial of service attacks, whereas a military site might be more interested in surveillance attacks (Stavroulakis et al., 2010).

PROBABILITY OF FALSE ALARMS

“This measurement determines the rate of false positives produced by an IDS in a given environment during a particular time frame. A false positive or false alarm is an alert caused by normal non-malicious background traffic” (Mell, 2003). To determine the rate of false alarms produced by an IDS, in a given environment within a particular timeframe, is resolved by finding the probability of false alarms. Different false alarm rates, however, in different network environments make measuring false alarms difficult. Also, configurable IDSs can be tuned to reduce the false alarm rate and with the diversities involved in host activities and network traffic, it could be difficult to determine the aspects that cause false alarms (Stavroulakis et al., 2010).

PROBABILITY OF DETECTION

This measurement, “also known as the hit rate”, gives the correctly detected rate of attacks that have been detected, correctly, by an IDS within a given environment and within a set interval of time (Stavroulakis et al., 2010). The challenge with this measurement is that it is difficult to gain complete confidence from the results.

The success of an IDS is largely dependent upon the set of attacks used during the testing process. Also, with a false positive rate the probability of detection will vary. Further confidence is lost when considering an IDS can be tuned/configured to either favor the ability to detect attacks or minimize false positives. Techniques such as fragmenting packets are attacks that can evade a NIDS, all together, further reducing the accuracy of this measurement (Mell, 2003).

RESISTANCE TO ATTACKS DIRECTED AT THE IDS

This measurement demonstrates the resistance levels of an IDS when attacker’s attempt to disturb its standard operation. Some of these attacks may be in any of the following forms:

1. A Distributed Denial of Service attack. This type of attack can send large amounts of non-attack traffic that exceeds the IDS’s processing capability. If the IDS drops packets, it may be unable to detect attacks. It can also act as a “smokescreen” that distracts the operator and allows the attacker an opportunity to breach the IDS with a different attack (Markoff, 2013).

2. Sending to the IDS non-attack packets triggering many signatures within the IDS; which, provide an overwhelming number of false positives or crash alert processing or crash display tools or any combination of these (Mell, 2003).

ABILITY TO HANDLE HIGH BANDWIDTH TRAFFIC

This measurement demonstrates how well an IDS will function under stressful network conditions. Measurements are taken when the IDS is presented with a large volume of traffic (Stavroulakis et al., 2010).

ABILITY TO CORRELATE EVENTS

This measurement demonstrates the ability of an IDS to correlate attack events and its ability to identify staged penetration attacks. These events may be gathered from any number of devices and, currently, IDSs have limited capabilities in this area (Mell, 2003).

ABILITY TO DETECT NEVER BEFORE SEEN ATTACKS

This measurement demonstrates, as its name implies, the ability of an IDS to detect novel attacks or attacks that have not occurred before (Stavroulakis, 2010).

ABILITY TO IDENTIFY AN ATTACK

“This measurement demonstrates how well an IDS can identify the attack that it has detected by labeling each attack with a common name or vulnerability name or by assigning the attack to a category” (Mell, 2003).

ABILITY TO DETERMINE ATTACK SUCCESS

“This measurement demonstrates if the IDS can determine the success of attacks from remote sites that give the attacker higher-level privileges on the attacked system” (Mell, 2003).

CAPACITY VERIFICATION FOR NIDS

This measurement quantifies the ability of a NIDS to, capture, process, and perform, at the same level of accuracy regardless of its operational activity (Mell, 2003).

OTHER MEASUREMENTS

“There are other measurements, such as ease of use, ease of maintenance, deployments issues, resource requirements, availability and quality of support etc. These measurements are not directly related to the IDS performance but may be more significant in many commercial situations” (Mell, 2003).

CURRENT EVALUATION EFFORTS

Over time, there has been an increase in evaluation complexity. Evaluations have grown to include more IDSs and more attack types; such as, stealthy and DDoS attacks. Research evaluations have been limited to novel attacks that were designed specifically for the evaluation. They have typically evaluated performance of anomaly detection systems and generated receiver operating characteristic (ROC) curves. Commercial system evaluations include performance measurements under high loads (Mell, 2003).­

In the document, entitled, “A Methodology for Testing Intrusion Detection Systems”, the researchers define performance objectives for an IDS. Their step by step methodology includes, broad detection range, economy in resource usage, and resilience to stress (Chung et al, 1996).

* Broad detection range states, for each intrusion, within a broad range of known intrusions, the IDS should be able to identify the threat vs. normal behavior.
* Economy resource usage states, the IDS should run efficiently. System resources like, main memory, central processing unit (CPU), and disk space, should not be significantly impacted.
* Resilience to stress states, the IDS should operate without err under very high levels of computing activities.

CHALLENGES IN EVALUATING IDPS

The most common challenge in evaluating IDSs is the inability to generate realism with the synthetically generated background traffic. The DARPA dataset, which can be found at this link, <http://www.ll.mit.edu/ideval/data/>, is a prime example of such traffic. In addition, collecting attack scripts and victim software, testing signature based vs. anomaly based IDSs and their differing requirements for doing so, and network-based vs. host-based IDSs (Ghorbani et al., 2010).

CONCLUSION

This discussion addressed the, motivations for evaluating IDPSs, measureable IDPS characteristics, examples of some current IDPS evaluation efforts, and challenges in evaluating IDPSs. Because so many areas of the personal and business world are data driven, level of confidence requirements, with regard to security, are very high. To increase confidence in an IDS, it is important to thoroughly test the system and keep current with all the latest information in regards to such systems. As improvements are released, systems should be updated to reduce the risk of a security breach.

REFERENCES

Chung, M., Mukherjee, B., & Olsson, R., Puketza, N., Zhang, K. (1996). *A Methodology for Testing Intrusion Detection Systems* (1st ed., pp. 1 - 22). Baltimore: IEEE. Retrieved December 15, 2015, from http://seclab.cs.ucdavis.edu/papers/tse96.pdf

Cyberspace Policy Review. (2009). Retrieved December 12, 2015, from https://www.whitehouse.gov/assets/documents/Cyberspace\_Policy\_Review\_final.pdf

Given, L. (2008). The Sage encyclopedia of qualitative research methods. Los Angeles, Calif.: Sage Publications. Web. 12 Dec. 2015.

Goodall, John, Wayne Lutters, and Anita Komlodi. (2004). *The Work Of Intrusion Detection: Rethinking The Role Of Security Analysts*. 1st edition. New York: Proceedings of the Tenth Americas Conference on Information Systems, 2015. Web. 12 Dec. 2015.

Ghorbani, A., Lu, W., & Tavallaee, M. (2010). Test, Evaluation, and Data Sts. In Network Intrusion Detection and Prevention: Concepts and Techniques (p. 182). Web. 15 Dec. 2015.

Han, C., & Dongre, R. (2014, October 1). Q&A. What Motivates Cyber-Attackers? Retrieved December 12, 2015, from <http://timreview.ca/article/838>

Markoff, J. (2013, April 1). Distributed Denial of Service. Retrieved December 15, 2015, from <http://www.nytimes.com/2013/04/02/science/distributed-denial-of-service.html?_r=0>

Mell, P. (2003). *An Overview of Issues In Testing Intrusion Detection Systems*. 1st edition. Gaithersburg: U.S. Department of Commerce, 2015. Web. 12 Dec. 2015.

Select and Implement an Intrusion Detection and Prevention System. (2015). Retrieved December 12, 2015, from [http://www.infotech.com/workshops/select-and-implement- intrusion-detection-and-prevention-systems](http://www.infotech.com/workshops/select-and-implement-%09intrusion-detection-and-prevention-systems)

Stavroulakis, P., & Stamp, M. (2010). Intrusion Detection Systems. In Handbook of information and communication security (pp. 202-203). Heidelberg: Springer. Web. 12 Dec. 2015.