Developing an Intelligent Intrusion Detection and Prevention System against Web Application Malware

Ammar Alazab[1], Michael Hobbs[1], Jemal Abawajy[1], and Ansam Khraisat[2]

[1] School of Information Technology, Deakin University, Waurn Ponds, Australia
{aalazab,mick,jemal.abawajy}@deakin.edu.au
[2] University of Ballarat, Ballarat, Australia

Abstract. Malware authors are continuously developing crime toolkits. This has led to the situation of zero-day attacks, where malware harm computer systems despite the protection from existing Intrusion Detection Systems (IDSs). We propose an Intelligent Intrusion Detection and Prevention System (IIDPS) approach that combines the Signature based Intrusion Detection system (SIDS), Anomaly based Intrusion Detection System (AIDS) and Response Intrusion Detection System (RIDS). We used a risk assessment approach to determine an appropriate response action against each attack event. We also demonstrated the IIDPS make the detection and prevention of malware more effective.

Keywords: Intrusion Detection System, Response Action, Malware, Signature Base Detection, Anomaly Base Detection, Web application.

1 Introduction

Malicious software (Malware) in web applications may result in stealing of confidential data, breaking of data integrity, reduced availability, causing damage or risk of data loss. Thus malware prevention and detection is vital to secure the web applications[1]. Recent trends in web application malware have become a major threat and they are increasing in complexity and evolving rapidly as systems provide more opportunities for more automated activities[2]. Furthermore, the damage caused by web application malware to individuals and businesses have dramatically increased. Today, writers of malware develop sophisticated techniques for concealing or constantly changing their attacks to evade established detection software. Attackers, who achieve unauthorized access to financial web applications, are causing losses to the financial sectors and there is no one single technique that can stop them[3]. Generally, the attacker developed new sophisticated techniques to specifically target and compromises web applications. As a result, attackers have access to other user's data. Furthermore, every year the quantity and creativity of web application hacks growths and the threat impact from these attacks increases rapidly, costing organizations millions every year[4].Moreover, the new generation of cybercrime is high degree of stealthiest and the attacker developing tool kits attacks that pose severe challenges to protect internet users. These crime tool kits such as Zeus and SpyEye, which have powerful capability

A.I. Awad, A.E. Hassanien, and K. Baba (Eds.): SecNet 2013, CCIS 381, pp. 177–184, 2013.

of attacks and have led to the threat of zero-day attacks, have showed a necessity to identify an Intelligent Malware Detection and Prevention System.

However, most exiting intrusion detection systems suffer from critical problems, such as: low detection accuracy; high false alarm rate; and the difficulties in dealing with the new attack. In this paper, we propose IIDPS for the efficient prevention and detection of malware.

Protecting web application from malicious attacks is an essential issue. Within this, intrusion prevention and intrusion detection systems have been the topic of a lot of research and have been suggested in a number of papers[5][6][7]. Nevertheless, the action that should follow the functionality of prevention and detection, namely response action, has needed to be involved as a primary function against any potential attack.

This paper is organized as follows. In Section 2, we present the background and related work. In Section 3, we describe the design and structure of our IIDPS model. Section 4 provides the conclusion to this paper.

2 Background and Related Work

Initially intrusion detection techniques mostly relied on matching to signatures patterns of well-known malware for triggering a detection decision. This style of detection strategy is usually known as Signature Base Detection (SBD). Nevertheless, it is very hard for SBD to detect zero-day attack, since such a malware example would have previously unidentified signatures. Thus anomaly base detection has attracted many researchers to overcome for this problem. Unfortunately anomaly detection systems suffer from high false negative, that is, the incorrect classification of valid software as malware[1].

Based on the input data sources the IDSs are examine, there are two main types of IDSs: network-based IDSs and host-based IDSs. Host-based IDSs (HIDS) examine host-bound audit sources such as application system audit, operating system, system logs, or database logs. A HIDS detector play significant role for detection inside attacks that do not involve network traffic. While network-based IDSs (NIDS) examine network packets that are taken from a network. Network-based IDS can be implementing to protect several hosts that are connected to a network. NIDS can report an attack that could be launched from the external at an earlier stage, before the attacks actually reach the host. However, NIDSs have the capacity problem to examine all packets in a high speed network.

Based on examination techniques, there are two approaches to analysing events using IDSs intrusion detection techniques can be categorized into two classes: signature based detection and anomaly based detection.

Up until now, there have only been a few approaches that have implemented IDS to find anomalies in web applications using a (SIDS) and an (AIDS). However, very few have used a combination of the two approaches[6]. Unfortunately none of them can guarantee a high level of security on web applications due to the web application architecture. Regarding current research for intrusion detection on web applications, Table 1 provides a summary of the research in developing an Intrusion detection system.

Table 1. Current Research in the Area of Anomaly Based Detection on Web Application

Name	Comments	Detection	Prevention	Response
(Vigna et al., 2009) [7] Reducing errors in the anomaly-based detection of web-based attacks through the combined analysis of web requests and SQL queries.	Reduce FP and FN but doesn't validate with Data Mining Algorithms.	NO	YES	NO
(Maggi, Robertson, Kruegel, & Vigna, 2009) [8] Protecting a Moving Target: Addressing Web Application Concept Drift	Anomaly- based detection of changes in web application	YES	NO	NO
(Kruegel, 2008) [9] Anomaly Detection of Web-based Attacks.	Anomaly detection with parameter profiles associated web applications (length and structure of parameters) from the analyzed data.	YES	NO	NO
(W. K. Robertson, 2010) [10] Detecting and preventing attacks against web applications.	Detection system that accurately detects attacks against web applications.	YES	NO	NO
(Cova, Balzarotti, Felmetsger, & Vigna, 2007) [11] Swaddler: An Approach for the Anomaly-Based Detection of State Violations in Web Applications	Anomaly detection by Learning the relationships between the application's execution and the application's internal.	YES	NO	NO
(Dagorn, 2008)[12] WebIDS: A Cooperative Bayesian Anomaly-Based Intrusion Detection System for Web Applications.	Learning-based anomaly detection system for Web applications	YES	NO	NO

3 Intelligent Intrusion Detection and Prevention System (IIDPS)

As shown in Section 2, traditional IDS have restrictions, including low flexibility, inability to distinguish novel attacks, high cost, slow updates and lacks extensibility. It also shows that both SIDS and AIDS have drawbacks such as low detection zero-day attack. The aim of the new approach is design and develops an effective IIDPS that address the weakness of SIDS and AIDS. Our IIDPS combines SIDS, AIDS and RIDS to become an IIDPS. Figure 1 shows an overview of the proposed Intelligent Intrusion Detection and Prevention System. In our system, AIDS help to detect unknown attacks, while SIDS detects known attacks. The basic idea of the new system is to take benefits from both SIDS and AIDS to create effective IDS. The IIDPS has three stages; the SIDS stage, the AIDS stage and the response action stage as shown in Figure 1.

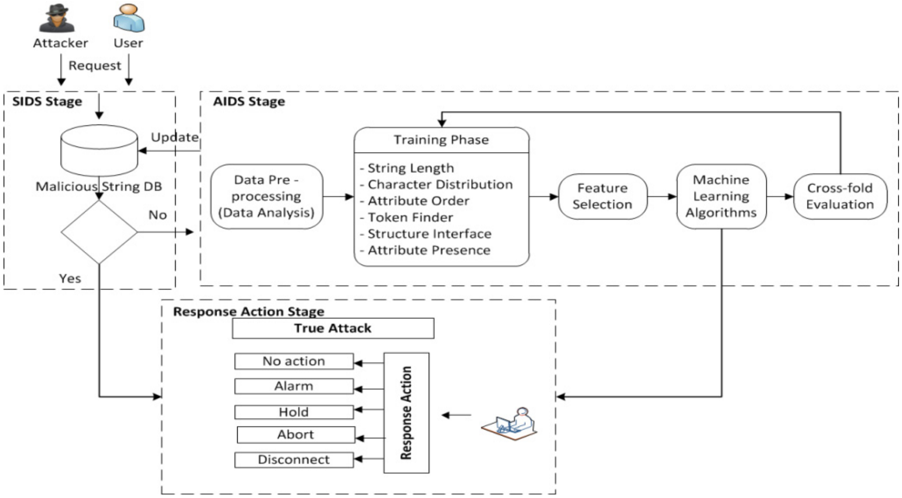

Fig. 1. Overview of IIDPS and Response Action Model

3.1 SIDS Stage

The SIDS stage simply uses pattern matching to handle the received request from clients. Whether or not this request is legitimate or illegitimate, SIDS will detect a known malicious string attack that has been previously stored in the SIDS signature database. If the request is passed to the final stage has the same pattern as found on the malicious string database, it means the request will be identified on the system as a true attack. As a consequence, response action is taking the appropriate response action. Otherwise, if the received request is not found in the malicious string, the AIDS stage handles the request.

3.2 AIDS Stage

The second stage is the AIDS stage. The main idea of this stage is to overcome the shortfalls of the SIDS stage. The main assumption is that any request received from users is an anomaly request, unless proven otherwise. In the AIDS stage, the system builds the profile of users by using data that is accepted as normal behaviour. Then it monitors the activities of new users and compares the new data with the obtained profile and tries to detect deviations.

In this stage, the system gathers information from the user request such as request length, character distribution and particular token, and if any suspicious event is detected, the system will store it in the signature database. The reason from the store signature in the database is taking precautions against the new attack in future requests.

Once the users profile has been built, the system can decide if the user activity is a normal or abnormal behaviour. The profile information collected from the users' activities by using the learning mode enables identification of the appropriate response to any attack, as shown at the bottom of Figure 1.

3.3 Response Action Stage

The final element of our approach is taking appropriate response actions against a request if it is found to be an anomaly. A response action is a set of instructions that is carried out for a given attack. Response actions are triggered by the response action policy in reply to an attack which is detected by SIDS or AIDS. Once SIDS and AIDS detect an attack then this stage comes to reacts with attacks. The Response Action has two stages, risk assessment stage and response reaction stage.

Risk Assessment

The main purpose for risk assessment is to estimate the risk level of an attack. We have adopted the DREAD model from Microsoft to help calculate risk and rate the threats[13]. By using the DREAD model, it is possible to arrive at the risk rating for a given threat by asking the following questions:

- **D**amage potential: How great is the damage if the vulnerability is exploited?
- **R**eproducibility: How easy is it to reproduce the attack?
- **E**xploitability: How easy is it to launch an attack?
- **A**ffected users: As a rough percentage, how many users are affected?
- **D**iscoverability: How easy is it to find the vulnerability?

We applied DREAD risk assessment to identify the risk level for an application attack. We use the risk matrix to determine the risk assessment process. These matrices provide a qualitative risk ranking that classifies the degree from very high to very low as shown in Table 2. The probability of risk ranges from zero to one. The threat impact can be classified in five states as shown in the following sets:

Probability of Risk= {Very Low, Low, Medium, High, Very High}

Impact of Risk= {Very Low, Low, Medium, High, Very High}

Table 2. Standard terms for severity quantification

Probability	Description
Very high	Expected to occur with almost certainty
High	Expected to occur
Medium	Likely occur
Low	Very unlikely to occur
Very low	Almost no possibility of occurring

We calculate each query risk and evaluate the probability of the risk occurring against the security impact using the following equations

Risk =Probability x Impact

Expected Value= [Risk Probability Value]* [Risk Impact Value]

On the vertical axis, there is probability of the risk occurring, thus a higher chance of that risk occurring and becoming an issue. The horizontal axis shows the level of impact in the assumption that the risk will occur. As shown in Figure 2, the value outputs near to zero point to normal features, while outputs near to one indicate anomalous ones.

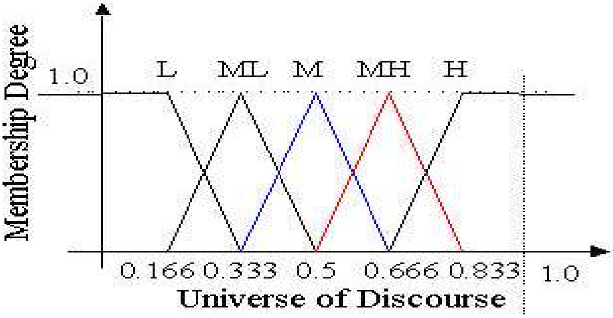

Fig. 2. Rule Action

One of the advantages of this approach is being able to show risks and identify how risky they are on the database. If all the risks are clustered in the top right of the diagram, then evidently the database is very risky. In other words, it may be exploited by a malicious writer.

Response Reaction

In this stage, we will identify the best response against a database threat according to the level of severity. Once the risk is estimated from the previous stage, our approach can and determines appropriate action response. The reaction of our approach is responsible for providing a corresponding response action when an anomaly activity is detected.

Once the users' try request a malicious string, the response action will be executed. This response action will handle this request according to severity methods as shown in Table 3. There are six principle methods to handle risk. Table 3 shows each response action according to severity request.

Table 3. Response Actions

Severity Level	Severity Level	Description
Low Severity	No action	The system will process as normal
	Alarm	Sent notification to DBA
Medium Severity	Audit	The request is audit
	Hold	The user requests is aborted
High Severity	Disconnect	The user session is disconnect
	Refuse	The user request is refused

Once the risk has been calculated, an appropriate action will be executed according to the severity level. For example if damage potential is very high; reproducibility is very high; exploitability is very high ; affected users is high, and discoverability is very high then risk level is consider very high.

4 Conclusion

A detection system with a response system would be highly reliable against suspicious behaviour, as it is able to detect and react to maliciously requests that could possibly be a zero day attack. In this paper, we developed IIDPS with a response action that provides an early stage detection system. Our IIDPS combines SIDS, AIDS and RIDS to become an IIDPS. Our approach of IIDPS is capable of preventing and distinguishing various types of abnormal activity. SIDS was used to recognize known attacks, while AIDS was used to recognize unidentified attacks. A risk assessment was also done in order to respond to the attack, with several response techniques used to minimize the damage caused by malicious activities.

References

1. Alazab, A., Abawajy, J., Hobbs, M.: Web Malware That Target Web Application. In: Caviglione, L., Coccoli, M., Merlo, A. (eds.) Social Network Engineering for Secure Web Data and Services. IGI Global, USA (2013)

2. Alazab, A., Alazab, M., Abawajy, J., Hobbs, M.: Web Application Protection against SQL injection Attack. In: Proceedings of the 7th International Conference on Information Technology and Applications, pp. 1–7. IEEE (2011)
3. Alazab, M., Ventatraman, S., Watters, P., Alazab, M., Alazab, A.: Cybercrime: The Case of Obuscated Malware. In: 7th International Conference on Global Security, Safety & Sustainability (2011)
4. Alazab, M., Venkatraman, S., Watters, P., Alazab, M.: Zero-day Malware Detection based on Supervised Learning Algorithms of API call Signatures. In: Australasian Data Mining Conference (AusDM 2011), pp. 171–182. ACS (2011)
5. Shameli-Sendi, A., Ezzati-Jivan, N., Jabbarifar, M., Dagenais, M.: Intrusion response systems: survey and taxonomy. Int. J. Comput. Sci. Network Secur (IJCSNS) 12(1), 1–14 (2012)
6. Alazab, A., Hobbs, M., Abawajy, J., Alazab, M.: Using feature selection for intrusion detection system. In: International Symposium on Communications and Information Technologies (ISCIT), pp. 296–301. IEEE (2012)
7. Vigna, G., Valeur, F., Balzarotti, D., Robertson, W., Kruegel, C., Kirda, E.: Reducing errors in the anomaly-based detection of web-based attacks through the combined analysis of web requests and SQL queries. Journal of Computer Security 17, 305–329 (2009)
8. Robertson, W., Maggi, F., Kruegel, C., Vigna, G.: Effective anomaly detection with scarce training data. In: Proceedings of the Network and Distributed System Security Symposium (NDSS), San Diego, CA (2010)
9. Kruegel, C., Vigna, G.: Anomaly detection of web-based attacks. In: Proceedings of the 10th ACM Conference on Computer and Communications Security, pp. 251–261. ACM (2003)
10. Robertson, W.K., Adviser-Kemmerer, R.A., Adviser-Vigna, G.: Detecting and preventing attacks against web applications. University of California at Santa Barbara (2009)
11. Cova, M., Balzarotti, D., Felmetsger, V., Vigna, G.: Swaddler: An approach for the anomaly-based detection of state violations in web applications. In: Kruegel, C., Lippmann, R., Clark, A. (eds.) RAID 2007. LNCS, vol. 4637, pp. 63–86. Springer, Heidelberg (2007)
12. Dagorn, N.: WebIDS: A Cooperative Bayesian Anomaly-Based Intrusion Detection System for Web Applications (Extended Abstract). In: Lippmann, R., Kirda, E., Trachtenberg, A. (eds.) RAID 2008. LNCS, vol. 5230, pp. 392–393. Springer, Heidelberg (2008)
13. `http://msdn.microsoft.com/en-us/library/ff648644.aspx`