AIWAS: The Automatic Identification of Web Attacks System

Toan Huynh, University of Alberta, Canada
James Miller, University of Alberta, Canada

ABSTRACT

A recent report states that 63 percent of documented vulnerabilities exist in Web applications. Hence, Web applications represent an ideal platform for malicious attackers to target. This paper presents an anomaly intrusion detection system (AIWAS) to help system administrators protect their Web applications from these attacks. AIWAS maps each user’s input into an Instance Model (IM). The IM, which contains attackable features of the input, allows machine learning algorithms to classify the input as either benign or malicious. AIWAS then prevents malicious inputs from reaching the protected Web applications. A case study demonstrates the effectiveness of AIWAS against actual attacks.

Keywords: Anomaly Detection, Attacks, Intrusion Detection System, Machine Learning, Web Application Security

INTRODUCTION

The Laws of Vulnerabilities 2.0 (Qualys, 2009) states that “80 percent of vulnerability exploits are now available within single digit days after the vulnerability’s public release”. The Internet Security Threat Report (Fossi et al., 2008) from Symantec notes that, in 2008, Web applications contain 63 percent of all documented vulnerabilities. Insecure applications can be extremely costly. For example, ChoicePoint, after exposing 145,000 customer accounts, reported $11.4 million in charges directly related to the incident (Rapid7, 2005). Immediately after the incident was disclosed, ChoicePoint’s total market capitalization also dropped by $720 million. Meanwhile, CardSystems is barred from accepting Visa and American Express cards after compromising 40 million accounts due to a SQL Injection vulnerability. Hence, security is a prominent non-functional requirement for modern Web applications.

Network Intrusion Detections Systems (NIDS) are security tools that allow system administrators to detect and protect their Web applications from attacks. NIDS are commonly described as either misuse or anomaly based systems (A-NIDS). Misuse based systems contain rules designed to filter out known attacks. Misuse systems cannot detect and prevent attacks that are not contained in their rule set because these attacks are too recent (zero day

DOI: 10.4018/jssoe.2012010105
attacks); hence, most new NIDS approaches are anomaly based (A-NIDS). These systems do not rely on any rule set; therefore they can potentially detect these new attacks (Forrest et al., 1996; Anderson, 1972; Heberlein et al., 1990). With A-NIDS, empirical information on system usage is first collected. Using collected information, the A-NIDS creates a model of normal behaviour. Observations that deviate from the model are classified as anomalous.

This paper presents an A-NIDS specifically for Web applications. The system creates a model of users’ behaviours through observations of their inputs. Essentially, the introduced A-NIDS studies the input specification associated with “normal” usage of the system and validates any given input against this specification. This technique allows the A-NIDS to filter out malicious inputs before they reach the Web application.

The remaining sections of the paper are organized as follows. The Related Works section provides information on existing A-NIDS. The AIWAS section introduces the Automatic Identification of Web Attacks System (AIWAS). The Case Study section contains a case study with three Web applications to validate the effectiveness of AIWAS. The last section presents the conclusion and future works.

RELATED WORKS

A-NIDS often utilize machine learning (ML) techniques. Lazarevic et al. (2005), Tavallae et al. (2010) and Tsai et al. (2009) provide a review of existing A-NIDS. Traditional A-NIDS (Lee & Heinbuch, 2001) concentrate on low-level packet information implying that application specific information is lost (Krugel, 2002). As a result, A-NIDS often have low detection rates for attacks targeting the Web application layer. A new generation of A-NIDS has been proposed to specifically target the Web application layer; a brief overview of these A-NIDS follows.

Kruegel et al. (2003, 2005) presented one of the first A-NIDS designed specifically for Web applications. The system contains six anomaly models and six techniques for estimating the probability of an attack based upon these models. Valeur et al. (2005) present an approach that profiles normal database access performed by Web applications to detect SQL injection attacks on a DBMS. Swaddler (Cova et al., 2007a) extends Kruegel et al. (2003, 2005) by also examining the state of the Web application. Liu et al. (Liu et al., 2009) introduces the SQLProb proxy to detect and remove SQL injection attacks. SQLProb is evaluated using the AMNESA (Halfond & Orso, 2005) attack data set with excellent results.

Ingham et al. (2006) introduces Deterministic Finite Automata induction as a method to detect malicious Web requests. However, their results show that the approach currently suffers from low detection and high false positive rates. Cheng et al. (2008) proposes an Embedded Markov Model to detect attacks and monitor users’ behaviour. Estevez-Tapiador et al. (2005) uses a hybrid approach that is both learning and specification-based. The approach builds a Markov model using the specification of the HTTP protocol and the actual payload from the training data. Sphinx (Bolzoni & Etalle, 2008) detects attacks on data flows within Web applications using “positive signatures” which are rules that match normal inputs rather than malicious inputs. Park and Park (2008) use an extended Needleman-Wunsch (1970) algorithm to build a profile of normal Web requests. Future Web requests that do not match this profile are classified as anomalous.

When used in A-NIDS, the ML algorithms classify data as either malicious or benign (Tsai et al., 2009). Current A-NIDS for Web applications attempt to create custom anomaly models for this classification step. However, no existing A-NIDS for Web applications leverage the available knowledge from various ML techniques; and traditional ML-enabled NIDS suffer from low detection rates because they have no domain knowledge of the application layer. This paper presents a novel A-NIDS for Web applications called AIWAS. This approach differs from the available techniques because it does not create an anomaly model. It creates
Towards a Stepwise Variability Management Process for Complex Systems: A Robotics Perspective
[www.igi-global.com/article/towards-a-stepwise-variability-management-process-for-complex-systems/119076?camid=4v1a](www.igi-global.com/article/towards-a-stepwise-variability-management-process-for-complex-systems/119076?camid=4v1a)

RESCUE: An Integrated Method for Specifying Requirements for Complex Sociotechnical Systems
[www.igi-global.com/chapter/rescue-integrated-method-specifying-requirements/28413?camid=4v1a](www.igi-global.com/chapter/rescue-integrated-method-specifying-requirements/28413?camid=4v1a)