International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 10
June 2016

Secure Adverbial Anomaly Detection Schema for Web-Based Recovery Attacks

B. Divya Rani[1]; K. Katyayani[2] & M.Eranna[3]

[1]M.Tech Dept of CSE, PVKK College, Affiliated to JNTUA, AP, India .
[2]Associate Professor, Dept of CSE, PVKK College, Affiliated to JNTUA, AP, India
[3]Associate Professor, Dept of CSE, PVKK College, Affiliated to JNTUA, AP, India

Abstract: *With the anomaly detection systems, many approaches and techniques have been developed to track novel attacks on the systems. Anomaly detection systems based on predefine rules and algorithms; it's difficult to define all rules. To overcome this problem various machine learning schemes have been introduced. One such scheme is KIDS (Keyed Intrusion Detection System) which is completely depend on secrecy of key and method used to generate the key. In this scheme, attacker easily able to recover key by interacting with the KIDS and observing the outcome from it. Using this scheme one cannot able to meet security standards. So based on survey we need the scheme which will help us to provide more security on cloud storage and for personal computer. We are going to proposed scheme for more security which will be used to secure sensitive data of various domains like in healthcare domain patient related data like contact details and history.*

Keywords: Anomaly detection systems; Keyed Intrusion Detection System; Adversarial Learning; Feature Selection; Classifier Security; Evasion Attacks; machine learning.

1. Introduction

In recent years use of internet has been increased tremendously. Most of people used internet to transmit their data and used cloud to save it. There is possibility that the data may get hacked and get misused. For better protection from such unauthorized users various Anomaly intrusion detection schemes are introduced in recent year. Security problem mainly divided into two groups one is malicious and other is non malicious activity.

A malicious attack is an attempt to forcefully abuse or take advantage of someone's computer, whether through computer viruses, social engineering, phishing, or other types of social engineering. This can be done with the intent of stealing personal information (such as in social engineering) or to reduce the functionality of a target computer. Malicious Code mostly Hide in Email, Web Content, Legitimate Sites, File Downloads. For example Trojan, Horse, Viruses, Worms, Phishing, Baiting, Spam. Non-malicious attacks occur due to poor security policies and controls that allow vulnerabilities and errors to take place.

An intrusion detection system (IDS) is a device or software application that monitors network or system activities for malicious activities or policy violations and produces reports to a management station. IDS come in a variety of "flavors" and approach the goal of detecting suspicious traffic in different ways. There are network based (NIDS) and host based (HIDS) intrusion detection systems. NIDS is a network security system focusing on the attacks that come from the inside of the network (authorized users). Some systems may attempt to stop an intrusion attempt but this is neither required nor expected of a monitoring system.[1] .So attacker always try to avoid detection. In terms of network security the evasion attack means bypass a flaw in a security system that allows an attacker to circumvent security mechanisms to get system or network access in order to deliver an exploit, attack, or other form of malware without detection. Evasions are typically used to counter network-based intrusion detection and prevention systems but can also be used to by-pass firewalls. A further target of evasions can be to crash a network security device, rendering it in-effective to subsequent targeted attacks.

Few detection schemes are introduced in last decade to protect from such evasion attacks. KIDS (Keyed Intrusion Detection System) one of the scheme to avoid evasion attacks. KIDS first time introduced by Mrdovic and Drazenovic at DIMVA'10.Most current network attacks happen at the application layer, analysis of packet payload is necessary for their detection. Unfortunately malicious packets may be crafted to normal payload, and so avoid detection if the anomaly detection method is known. Model of normal payload is key dependent. Key is different for each implementation of the method and is kept secret. Therefore model of normal payload is secret although detection method is public. This prevents attacks. Payload is partitioned into words. Words are defined by delimiters. Set of delimiters plays a role of a key [2].

This paper is organized as follows. General background of adversarial machine learning in Section 2. Section 3 illustrates the KIDS scheme. Section 4 explains the existing method and Section 5 includes the proposed method . The final section provides a conclusion for our proposed approach.

2. Literature survey

2.1 Adversarial Learning and Evasion

The Machine learning has been widely used in security related tasks such as malware and network intrusion detection, and spam filtering, to recognize between malicious and legitimate samples is major problem, Dalvi et al. explorer the same problem in [5] so evasion can be classified. However, these problems are particularly challenging for machine learning algorithms due to the presence of intelligent and adaptive adversaries who can

carefully manipulate the input data to downgrade the performance of the detection system, violating the underlying assumption of data stationary, i.e., that training and test data follow the same (although typically unknown) distribution Research in adversarial learning has not only been addressing the problem of evaluating security of current learning Algorithms to carefully-targeted attacks, but also that of devising learning algorithms with improved security. To counter evasion attacks, explicit knowledge of different kinds of adversarial data manipulation has been incorporated into Learning algorithms, e.g., using game-theoretical. An implicit assumption behind traditional machine learning and pattern recognition algorithms is that training and test data are drawn from the same, possibly unknown, distribution. This assumption is however likely to be violated in adversarial settings, since attackers may carefully manipulate the input data to downgrade the system's performance.

Lowd and Meek[4] observe that the attacker need not model the classifier explicitly ,but only find lowest attacker cost instance as in the Dalvi et al. setting . They formalize a notion of reverse engineering as the adversarial classifier reverse engineering (ACER) problem. Given an attacker cost function ,they analyze the complexity of finding a lowest attacker cost instance that the classifier labels as negative. They assume no general knowledge of training data, though the attacker does know the feature space and also must have one positive example and one negative example. A classifier is ACRE-learnable of there exists a polynomial query algorithm that finds a lowest attacker cost negative instance. They show that linear classifier is ACRE learnable with linear attacker cost functions and some other minor restrictions. The ACER-learning problem provides a means of qualifying how difficult it is to use queries to reverse engineer a classifier from particular hypothesis class using a particular feature space.

2.2 Evasion preventing methods

Kolesnikov et al. [5] introduce a new class of polymorphic attacks, called polymorphic blending attacks, that can effectively evade byte frequency-based network anomaly IDS by carefully matching the statistics of the mutated attack instances to the normal profiles. The proposed polymorphic blending attacks can be viewed as a subclass of the mimicry attacks. Author take a systematic approach to the problem and formally describe the algorithms and steps required to carry out such attacks. They not only show that such attacks are feasible but also analyze the hardness of evasion under different circumstances. They present detailed techniques using PAYL, a byte frequency-based anomaly IDS.

Several application payload-based anomaly IDS have been proposed which monitor the payload of a packet for anomalies. In [6], Kruegel et al. proposed four different models, namely, length, character distribution, probabilistic grammar, and token finder, for the detection of HTTP attacks. PAYL, proposed by Wang and Stolfo [7], records the average frequency of occurrences of each byte in the payload of a normal packet. A separate profile is created for each port and packet length. In their recent work, the authors suggested an improved version of PAYL that computes several profiles for each port. At the end of the training, clustering is performed to reduce the number of profiles. They proposed that instead of byte frequency, one can also use an n-gram model in a similar fashion. One main drawback of the system is that they do not consider an advanced attacker, who may know the IDS running at the target and actively try to evade it.

B. Biggio, G. Fumera, and F. Roli[8] experiments support the analytical results derived based on the analytical framework , which showing that hiding information to the adversary through the randomization of the decision function can improve the hardness of evasion of a classifier. Author consider a strategy consisting in hiding information about the classifier to the adversary through the introduction of some randomness in the decision function and focus on an implementation of this strategy in a multiple classifier system.

3. KIDS-A Keyed Intrusion Detection System

Mrdovic and Drazenovic [2] proposed Keyed Intrusion Detection System in which secret key plays important role. Network anomaly detector inspects packet payloads. The proposed method has 3 important steps for implementation of the key.

1) Training Mode

   In training mode payload divided into words. Words are nothing but the sequence of byte located between delimiters.

   From this any special two byte assign to secret set S. This set S again classified into normal words, frequency count.

2) Detection Mode

   In detection mode anomaly score get counted according to word frequency count.

3) Key Selection

   The Key got selected after its score and checking its detection quality. Repeating all three steps generates new key each time.

3.1 KEY Recovery attacks

Author Juan E. Tapiador, Agustin Orfila, Arturo Ribagorda, and Benjamin Ramos[9] experiment analysis shows that in KIDS scheme attacker easily able to interact with it and using the feedback of the interaction attacker attacks on the secure data. Attacker takes help of various queries to get more information related to secret key. The attack makes exactly 257 queries to KIDS: 256 with each tentative key element d, plus one final query to determine which subset corresponds to the key [9].

International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 10
June 2016

4. Existing System

The major issue of computing better strategies to change an attack so that it evades detection by a Bayes classifier. In existing system the formulation of the problem mostly in game theoretic terms, where each change in instance is costlier, and successful detection and evasion have countable utilities to the classifier and the adversary, respectively. The setting used in consideration an adversary with full of information of the classifier to be evaded. Shortly after, how evasion can be done when such information is unavailable.

Author formulated the adversarial classifier reverse engineering problem (ACRE) as the exercise of learning enough information about a classifier to construct attacks, instead of looking for better strategies. The authors use a membership oracle as absolute adversarial model: the attacker is given the opportunity to query the classifier with any selected instance to firmly decide whether it is labeled as malicious or not. As a result, appropriate objective is to find instances with an affordable number of queries for evade detection. A classifier is said to be ACRE learnable if there exists an algorithm that finds a minimal-cost instance evading detection using only poly-nominally many queries. Similarly, a classifier is ACRE k-learnable if the cost is not minimal but Bounded by k. Among the results given, it is proved that linear classifiers with continuous features are ACRE k-learnable for linear cost functions Therefore, these classifiers not suitable for adversarial environments and should not be used. Subsequent work by generalizes these results to convex-inducing classifiers, showing that it is generally not necessary to reverse engineer the decision boundary to construct undetected instances of near-minimal cost. For the some open problems and challenges related to the classifier evasion problem. More generally, some additional works have revisited the role of machine learning in security applications, with particular emphasis on anomaly detection.

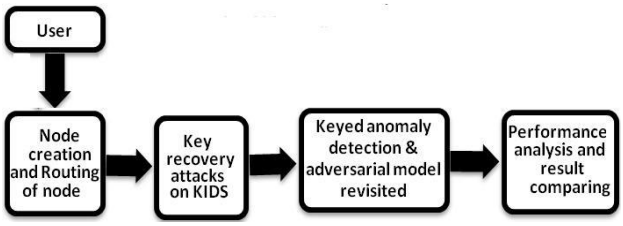
Disadvantages of current system:

- Malicious Node consumes More energy
- Not meet security standards.

5. Proposed System

Our assaults are to a great degree proficient, demonstrating that it is sensibly simple for an assailant to recoup the key in any of the settings examined. We trust that such an absence of security uncovers that plans like children were just not intended to anticipate key-recovery assaults. Here we have contended that resistance against such assaults is key to any classifier that endeavors to hinder avoidance by depending on a mystery bit of data. We have given exchange on this and other open inquiries in the trust of empowering further research around there. The assaults here exhibited could be forestalled by presenting various impromptu counter measures the framework, for example, constraining the most extreme length of words and payloads, or including such amounts as order components. We think, then again, that these variations may in any case be powerless against different assaults. In this manner, our suggestion for future plans is to construct choices in light of hearty standards as opposed to specific fixes. Our aim is enhance KIDS and meet all security properties so that it can able to secure store data in clouds. Like data in healthcare domain.

5.1 Proposed System architecture



System Architecture

Proposed system module Details:

- Node Creation & Routing

In this module, a remote system is made. Every one of the hubs are haphazardly sent in the system region. Our system is a portable system, hubs are doled out with versatility (movement).Source and destination hubs are characterized. Information exchanged from source hub to destination hub. Since we are working in versatile system, hubs portability is set i.e. hub move starting with one position then onto the next.

- Key- Recovery Attacks On Kids

At the point when surveying the security of frameworks, for example, KIDS, one note worthy issue originates from the non appearance of broadly acknowledged antagonistic models giving an exact portrayal of the aggressor's objectives and his abilities one such model for secure machine learning and talked about different general assault classes. Our work does not fit well inside in light of the fact that our principle objective is not to assault the learning calculation itself, but rather to recoup one bit of mystery data that, in this way, may be vital to successfully dispatch an avoidance assault

- Keyed Anomaly Detection and Adversarial Models Revisited

Firmly identified with the focuses talked about above is the need to set up plainly characterized and persuaded ill-disposed models for secure machine learning calculations. The suspicions made about the assailant's abilities are basic to legitimately break down the security of any plan, yet some of them may well be unlikely for some applications. One disputable issue is whether the assailant can truly get criticism from the framework for examples he picks. This bears a few analogies with Chosen-Plaintext Attacks (CPA) in cryptography. This supposition has been made by numerous works in secure mama chine learning, including our own.

- Performance Analysis

For performance evaluation we will use the following graph

– Packet delivery ratio

– Throughput
– Delay

Advantages of current system:

- Energy Efficient System.
- More secure KIDS

6. Conclusion

We have analyzed the strength of KIDS against key-recovery attacks. We have presented key-recovery attacks according to adversarial settings, depending on the feedback given by KIDS to probing queries. Analysis showing that it is reasonably easy for an attacker to recover the key. Our focus in this work has been on recovering the key through efficient procedures, demonstrating that the classification process leaks information about it that can be leveraged by an attacker. However, the ultimate goal is to evade the system, and we have just assumed that knowing the key is essential to craft an attack that evades detection or, at least, that significantly facilitates the process. It remains to be seen whether a keyed classifier such as KIDS can be just evaded without explicitly recovering the key.

References

[1] A Scarfone, Karen; Mell, Peter (February 2007). "Guide to Intrusion Detection and Prevention Systems (IDPS)" (PDF). Computer Security Resource Center (National Institute of Standards and Technology) (800–94). Retrieved 1 January 2010.

[2] R. S. Mrdovic and B. Drazenovic, "KIDS-Keyed Intrusion Detection System," Proc. Seventh Int'l Conf. Detection of Intrusions and Malware,and Vulnerability Assessment (DIMVA '10), pp. 173-182, 2010.

[3] N. Dalvi, P. Domingos, Mausam, S. Sanghai, and D. Verma, "Adversarial classification," in 10th ACM SIGKDD Int'l Conf. on Knowl. Discovery and Data Mining, 2004, pp. 99–108.

[4] D. Lowd and C. Meek, "Adversarial Learning," Proc. 11th ACM SIGKDD Int'l Conf. Knowledge Discovery in Data Mining (KDD '05), pp. 641-647, 2005.

[5] O. Kolesnikov, D. Dagon, and W. Lee, "Advanced Polymorphic Worms: Evading IDS by Blending in with Normal Traffic," Proc.USENIX Security Symp., 2005.

[6] C. Kruegel and G. Vigna. Anomaly detection of web-based attacks. In Proceedings of ACM CCS, pages 251-261, 2003.J. G

[7] K. Wang and S. Stolfo. Anomalous payload-based network intrusion detection. In Recent Advances in Intrusion Detection, 2004.

[8] B. Biggio, G. Fumera, and F. Roli, "Adversarial Pattern Classification Using Multiple Classifiers and Randomisation," Proc. IAPR Int'l Workshop Structural, Syntactic, and Statistical Pattern Recognition,pp. 500-509, 2008.

[9] Juan E. Tapiador, Agustin Orfila, Arturo Ribagorda, and Benjamin Ramos "Key-Recovery Attacks on KIDS, a Keyed Anomaly Detection System" IEEE transaction on DEPENDABLE AND SECURE COMPUTING, VOL. 12, NO. 3, MAY/JUNE 2015