ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Vol. 4, Issue 1, January 2016

Key Base Intrusion Detection System: An Overview

Reshama Kshirsagar, Smita Mane, Purva Sahane, Prof. Ashwini Dhoke

Dept. of Computer Engineering, Dr. D. Y. Patil College of Engineering, Pune, MH, India

ABSTRACT: Most anomaly detection systems depend on machine learning algorithms to derive a model of regularity that is later used to identify suspicious events. Some works accompanied over the last years have pointed out that such algorithms are generally vulnerable to deception, especially in the form of attacks carefully constructed to avoid detection. Various learning schemes have been suggested to overcome this weakness. One such system is KIDS (Keyed IDS). KIDS' core idea is similar to the functioning of some cryptographic primitives, explicitly to introduce a secret element (the key) into the scheme so that some tasks are infeasible without knowing it. In KIDS the learned model and the calculation of the anomaly score are both key-dependent, a fact which likely avoids an attacker from creating evasion attacks. In this paper they show that improving the key is extremely simple delivered that the attacker can interact with KIDS and get feedback about searching requests. They present accurate attacks for two different adversarial settings and show that improving the key requires only a small amount of queries, which indicates that KIDS does not meet the requested safety properties. They finally reconsider KIDS' central idea and provide experimental arguments about its suitability and limitations. This paper summarizes recent works on KIDS, machine learning, anomaly detection etc. It shows that KIDS is a promising field with productive results and many challenging issues.

KEYWORDS: Key, Anomaly Detection, KIDS, Gray-Box, White-Box, Security, Machine Learning

I. INTRODUCTION

With the rapid expansion of Internet during recent years, security has become an essential for computer networks and computer systems. The main aim of security system is to protect the most valuable assets i.e data or information of an organization like banks ,companies ,universities and many other because these organizations have data or secret information in some form. Detecting different attacks like denial of service attack, IP spoofing, ping of death, network scanning etc against computer networks is becoming a crucial problem to solve in the field of cryptography and network security. Information security is way of hiding information from unauthorized access, use, modification, inspection, recording or destruction. computer security is protection of information system from theft or damage of hardware, the software and the information on them as well as from disruption or misdirection of the service they provide. To secure a computer system it is important to know the attacks that can be made against it, and these threats can classified into one of following categories:

Backdoor: A backdoor in a computer system, a cryptosystem or an algorithm, is any secret method of avoiding normal authentication or security controls. They may exist for a number of reasons as well as by original design or from poor configuration.

Denial-Of-Service Attack: Denial of service attacks are designed to make a machine or network resource unavailable to its intended users. Attackers can deny service to individual victims, such as by knowingly entering a wrong password sufficient following times to cause the victim account to be locked, or they may overwork the abilities of a machine or network and block all users at once. Many computer security problems can be fundamentally reduced to splitting malicious from non malicious activities. For example, in the case of spam filtering, intrusion detection, or the identification of false behavior. But, in general, defining in a exact and computationally useful way what is meaningless or what is aggressive is often too complex. To overcome these difficulties, solutions to such problems have usually accepted a machine-learning approach, especially through the use of classifiers to automatically develop models of (good and/or bad) behavior that are later used to identify the occurrence of possibly risky events.

DOI: 10.15680/IJIRCCE.2016. 0401143

Basic System:
Our attacks are very efficient, presenting that it is practically simple for an attacker to recover the key in any of the two settings. They believe that such a lack of security exposes that schemes like kids were simply not designed to prevent key-recovery attacks. however, They have discussed that conflict against such attacks is essential to any classifier that attempts to delay evasion by depend on a secret piece of information. They have provided conversation on this and other open questions in the hope of inspiring further research in this area. The attacks here accessible could be prevented by leading a number of ad hoc counter measures the system, such as limiting the maximum length of words and payloads, or including such quantities as classification features. We suspect, however, that these variants may still be vulnerable to other attacks. Thus, our recommendation for future designs is to base decisions on robust principles rather than particular fixes.

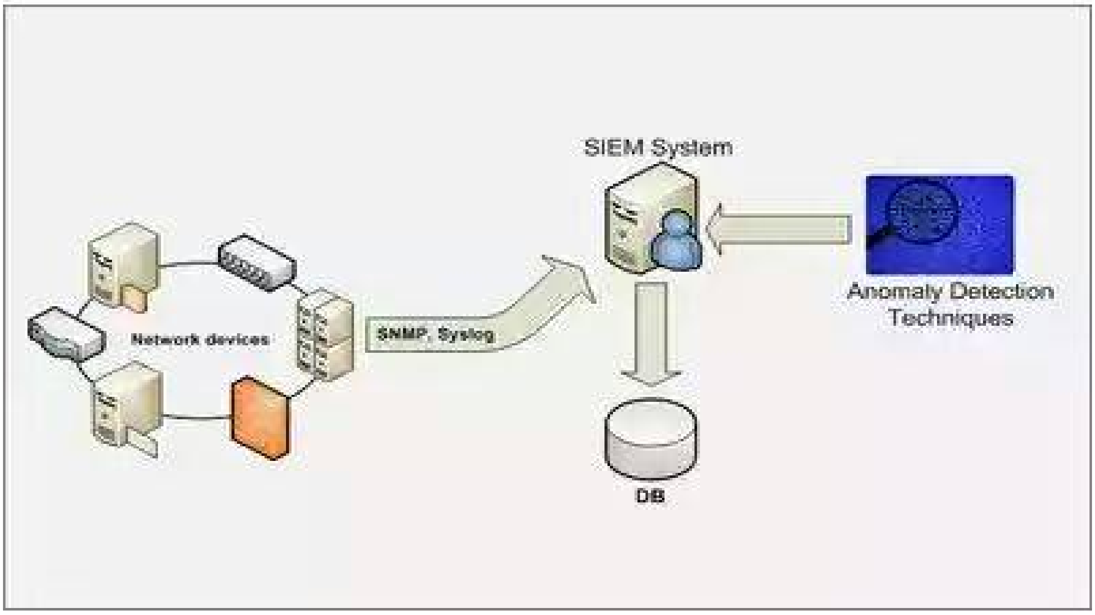

Figure 1: Proposed System Architecture

II. LITERATURE SURVEY

A.”Can Machine Learning be Secure” ,Barreno, B. Nelson, R. Sears, A.D. Joseph, and J.D. Tygar, 2006 : Machine learning techniques are used in a growing number of systems and networking issues, particularly those issues where the purpose is to detect irregular system activities. For example, network Intrusion Detection Systems (IDS) examine network traffic to detect irregular activities, such as attacks against hosts or servers. In this paper they found, a framework for replying the question, “Can machine learning be protected?” is provided. Novel offerings of this approach include classification of dissimilar types of attacks on machine learning methods and systems, a variety of defense against those attacks, a conversation of ideas that are main to security for machine learning, an analytical model giving a minor certain on attacker’s work function, and a list of undeveloped problems.
B. “The security of machine learning”, M. Barreno, B. Nelson, A.D. Joseph, and J.D. Tygar, 2010: Machine learning advocates have projected learning-based systems for variability of security applications, containing spam detection and network intrusion detection. Their idea is that machine learning will allow a system to respond to evolving real-world inputs, both unreceptive and benign, and learn to reject unwanted behavior. In this paper , they are going to present a classification recognizing and examining attacks against machine learning systems. They show how these classes control the costs for the attacker and protector, and they give a formal structure defining their interaction. They used a framework to survey and study the works of attacks against machine learning systems. They also

demonstrate taxonomy by showing how it can guide attacks against Spam Bayes, a popular statistical spam filter. Finally, they discuss how our taxonomy suggests new lines of defenses.

C. " Adversarial Pattern Classification Using Multiple Classifiers and Randomization",B. Biggio, G. Fumera, and F. Roli, 2008: In this paper, they consider a strategy containing hiding information near the classifier to the challenger concluded the introduction of some uncertainty in the decision function. They focus on an implementation of this approach in a multiple classifier system, which is a grouping architecture commonly used in security applications. The main aim is that, in these presentations, a pattern organization system looks a quick, adaptive adversary who causes patterns to loss the system itself.

D. "Adversarial Feature Selection Against Evasion Attacks", B. Nelson, B.I.P. Rubinstein, L. Huang, A.D. Joseph, and J.D. Tygar, 2011:

In this paper, they provide a more exhaustive investigation of this phase, shedding some light on the security properties of characteristic selection in opposition to evasion attacks. Inspired by earlier work on adversary-aware classifiers, they suggest a new adversary-aware feature collection model that can get better classifier security against evasion attacks, by combining specific expectations on the adversary's data handling strategy. They focus on an efficient, wrapper-based implementation of their approach, and experimentally authenticate its reliability on different application samples, including spam and malware discovery.

E." Outside the Closed World: On Using Machine Learning for Network Intrusion Detection", R. Sommer and V. Paxson, 2010::

They found that, the attack's using network's activity for anomalies. They can observe the differences between the intrusion detection field and other areas somewhere machine learning is used with more success. Their main aim is that the task of finding attacks is which are different from other applications, by making it harder for the intrusion detection association to employ machine learning effectively.

F. "Computer Security and Machine Learning:Worst Enemies or Best Friends?",K. Rieck, 2011

In this paper, they think again the problems, challenges and reward of combining machine learning and computer protection. They recognize factors that are decisive for the worth and acceptance of learning methods in protection. They present guidelines and perspectives for effectively linking both fields and aim at fostering study on intelligent security methods.

Proactive risk detection: A first step towards improving the possibility is thus the growth of transparent abnormality detection methods which allow understanding and adapting their detection models during process. One way for addressing this problem is linking learned models back to their original features, for example, without human intervention transforming statistical models into corresponding string patterns and rules.

Putomatic risk analysis: grouping malware into classes is simply a one step in protecting against malicious code.

Literature Review:

Author Name	**Year**	**Advantages**	**Disadvantages**	**Review**
M. Barreno, B. Nelson, R. Sears, A.D. Joseph, and J.D. Tygar[1]	2006	• Robustness • Detecting Attacks	• Lack of Quantitative measurement. • Unusual patterns	This paper proposes a framework for understanding security related issues.
M. Barreno, B. Nelson, A.D. Joseph, and J.D. Tygar[2]	2010	• Measuring the amount of information leaked from a learning system to an attacker • Try to gain information about the internal state of a machine learning system to: -Extract personal	• Corrupt the attempt to find susceptibility in the learned assumption	They have presented a framework for articulating a comprehensive view of different classes of attacks on machine learning systems in

		information encoded in the internal state		terms of three independent dimensions and an adversarial learning game.
B. Biggio, G. Fumera, and F. Roli[3]	2008	• Identify weakness of pattern recognition system • Design Robust pattern	• Attack data must be available for training	They observe the work in adversarial classification.
K. Rieck[4]	2011	• effectiveness • Controllability • Robustness	• excess of security threats, ranging from typical computer worms to involved drive-by downloads and boot system.	From this paper, they found that computer security and machine learning are distant from being “worst enemies”. as an alternative, there is good optimism to make them “best friends” in the near future.
R. Sommer and V. Paxson[5]	2010	• Reduce the cost using an anomaly detection system. • Limit the Detector’s scope • Examine false & true positives/negatives.	• High cost of errors • Lack of training data • Large variability in input data	They observes the unexpected imbalance between the general amount of research on machine learning-based anomaly detection followed in the academic intrusion detection Community, versus the lack of operational deployments of such systems.
B. Nelson, B.I.P. Rubinstein, L. Huang, A.D. Joseph, and J.D. Tygar. [6]	2011	• security in conflict to well-crafted attacks. • a novel adversary-aware characteristic selection model that canimprove classifier security against evasion attacks.	• attackers seek to evade a deployed system at test time by manipulating the attack samples. For occasion, spam, malware, and network interruption detection can be evaded by obfuscating, in that order, the content of spam emails .	From this they found that ,attribute selection may be measured a critical step in security-related applications, such as spam and malware finding, when small subsets of features have to be selected to decrease computational difficulty.

III. CONCLUSION

In this paper we have studied the strength of KIDS against key-recovery attacks. We have presented key-recovery attacks according to two adversarial settings, depending on the feedback given by KIDS to probing queries. We first demonstrate key-recovery attacks on a keyed classifier. Unexpectedly, our attacks are extremely efficient, showing that it is practically easy for an attacker to recover the key in any of the two settings discussed. Such a absence of security may tell that schemes like KIDS were only not designed to prevent key-recovery attacks. In this paper, recovering the key through efficient procedures, indicating that the classification process leaks information about it, which can be leveraged by an attacker, is achieved by using different kind of algorithms: Semantic security ElGamal algorithm &ElGamal decryption. However, the ultimate goal is to avoid the system, and we have just expected that knowing the key is essential to craft an attack that evades detection. We surveyed existing methods for KIDS and mentioned their strengths and weaknesses.

REFERENCES

[1] M. Barreno, B. Nelson, R. Sears, A.D. Joseph, and J.D. Tygar, "Can Machine Learning be Secure?" Proc. ACM Symp. Information, Computer and Comm. Security (ASIACCS '06), pp. 16-25, 2006.

[2] M. Barreno, B. Nelson, A.D. Joseph, and J.D. Tygar, "The Security of Machine Learning," Machine Learning, vol. 81, no. 2, pp. 121- 148, 2010.

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

[4] B. Nelson, B.I.P. Rubinstein, L. Huang, A.D. Joseph, and J.D. Tygar, "Classifier Evasion: Models and Open Problems," Proc. Int'l ECML/PKDD Conf. Privacy and Security Issues in Data Mining and Machine Learning (PSDML '10), pp. 92-98, 2011.

[5] K. Rieck, "Computer Security and Machine Learning: Worst Enemies or Best Friends?" Proc. DIMVA Workshop Systems Security (SYSSEC), 2011.

[6] R. Sommer and V. Paxson, "Outside the Closed World: On Using Machine Learning for Network Intrusion Detection," Proc. IEEE Symp.Security and Privacy, pp. 305-316, 2010.