International Journal of Innovative Research in Science and Engineering
Vol. No.3, Issue 07, July 2017
www.ijirse.com
ISSN (O) 2454-9665
ISSN (P) 2454-0663

Key Recovery Attacks on KIDS, A Keyed Anomaly Detection System.

Kiran M. Thorat[1], Mohnish S. Waghulde[2]

Chinmay R. Kamble[3], Rudrani S. Biradar[4]

[1,2,3,4]B.E. Student, Dept. of Computer Engineering, JSPM's RSCOE

Savitribai Phule Pune University, Pune, Maharashtra, (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 — Upload file & generate Key, Request for key, Access File.

I. 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

ISSN (O) 2454-9665
ISSN (P) 2454-0663

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. So attacker always tries 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.

II. EXISTING SYSTEM

A. Existing System The problem of computing optimal strategies to modify an attack so that it evades detection by a Bayes classifier they formulate the problem in game-theoretic terms, where each modification made to an instance comes at a price, and successful detection and evasion have measurable utilities to the classifier and the adversary, respectively. The authors study how to detect such optimally modified instances by adapting the decision surface of the classifier, and also discuss how the adversary might react to this. The setting used in assumes an adversary with full knowledge of the classifier to be evaded. Shortly after, how evasion can be done when such information is unavailable. They formulate the adversarial classifier reverse engineering problem (ACRE) as the task of learning sufficient information about a classifier to construct attacks, instead of looking for optimal strategies. The authors use a membership oracle as implicit adversarial model: the attacker is given the opportunity to query the classifier with any chosen instance to determine whether it is labeled as malicious or not. Consequently, a reasonable objective is to find in-stances that evade detection with an affordable number of queries. A classifier is said to be ACRE learnable if there exists an algorithm that finds a minimal-cost in-stance evading detection using only polynomials 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 under linear cost functions.

Therefore, these classifiers should not be used in adversarial environments. 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 ma-chine learning in security applications, with particular emphasis on anomaly detection.

International Journal of Innovative Research in Science and Engineering
Vol. No.3, Issue 07, July 2017
www.ijirse.com
ISSN (O) 2454-9665
ISSN (P) 2454-0663

III. PROPOSED SYSTEM

Our attacks are extremely efficient, showing that it is reasonably easy for an attacker to recover the key in any of the two settings discussed. We believe that such a lack of security reveals that schemes like kids were simply not designed to prevent key-recovery attacks. However, in this paper we have argued that resistance against such attacks is essential to any classifier that attempts to impede evasion by relying on a secret piece of information. We have provided discussion on this and other open questions in the hope of stimulating further research in this area as shown in Fig1. The attacks here presented could be prevented by introducing 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.

Advantage: Provides data integrity and confidentiality.

IV. CONCLUSION

A Proposed our attacks are extremely efficient, showing that it is reasonably easy for an attacker to recover the key in any of the two settings discussed. We believe that such a lack of security reveals that schemes like kids were simply not designed to prevent key-recovery attacks. However, in this paper we have argued that resistance against such attacks is essential to any classifier that attempts to impede evasion by relying on a secret piece of information. We have provided discussion on this and other open questions in the hope of stimulating further research in this area. The attacks here presented could be prevented by introducing 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 fixe.

ISSN (O) 2454-9665
ISSN (P) 2454-0663

V. ACKNOWLEDGEMENT

We take this opportunity to express our sincere gratitude to our guide,Prof. S.B.Javheri and head of department, Prof. Seemah kedar, Department of Computer Engineering, RSCOE, Pune University, for her kind cooperation and capable guidance during the entire work. we would also like to thank our, Principal and Management for providing lab and other facilities.

REFRENCES

[1] M. Barreno, B. Nelson, R. Sears, A.D. Joseph, and J.D. Tygar. "Can Machine Learning Be Secure?" In ASIACCS 2006, pp. 16–25, 2006.

[2] M. Barreno, B. Nelson, A.D. Joseph, and J.D. Tygar. "The security of machine learning." In Machine Learning, 81(2):121–148, 2010.

[3] B. Biggio, G. Fumera, and F. Roli. "Adversarial Pattern Classifica- tion Using Multiple Classifiers and Randomisation." In Proc. 2008 IAPR Intl. Workshop on Structural, Syntactic, and Statistical Pattern Recognition, pp. 500–509. Springer-Verlag, 2008.

[4] B. Biggio, B. Nelson, P. Laskov. "Support Vector Machines Under Adversarial Label Noise." In Journal of Machine Learning Research - Proceedings Track, Vol. 20, pp. 97–112, 2011.

[5] N. Dalvi, P. Domingos, Mausam, S. Sanghai, and D. Verma. "Adversarial classification." In KDD 2004, pp. 99–108, 2004.

[6] P. Fogla, M. Sharif, R. Perdisci, O. Kolesnikov, and W. Lee. "Polymorphic blending attacks." In USENIX Security Symp., 2006.

[7] C. Gates and C. Taylo. "Challenging the anomaly detection paradigm: A provocative discussion." In New Security Paradigms Workshop (NSPW), pp. 21–29, 2006 [8] A. Kolcz and C.H. Teo. "Feature weighting for improved classifier robustness." In CEAS 2009 - 6th Conf. on Email and Anti-spam, 2009.

[9] O. Kolesnikov, D. Dagon, and W. Lee. "Advanced polymorphic worms: Evading IDS by blending in with normal traffic." In USENIX Security Symposium, 2005. [10] D. Lowd and C. Meek. "Adversarial learning." In KDD 2005, pp. 641–647, 2005