# Survey on Prevention of Key based Attack on Data Sharing System

**Mr. Khaire S. H.[1] Prof. Hemant Gupta[2] Prof. Mayank Bhatt[3]**
[1]PG Student [2]Assistant Professor [3]HOD
[1,2,3]Department of Computer Science and Engineering
[1,2,3]LNCTS, Indore, M.P, India

*Abstract*— Today security is very important in the networking system. There are multiple anomaly detection systems rely on machine learning algorithms to derive a model of normality that is later used to detect suspicious events. Such algorithms are generally susceptible to deception, notably in the form of attacks carefully constructed to evade detection. Various learning schemes have been proposed to overcome this weakness. One such system is Keyed IDS (KIDS), introduced at DIMVA "10. KIDS" core idea is akin to the functioning of some cryptographic primitives, namely to introduce a secret element (the key) into the scheme so that some operations are infeasible without knowing it. In KIDS the learned model and the computation of the anomaly score are both key-dependent, a fact which presumably prevents an attacker from creating evasion attacks but in that some limitations. To avoid that limitations and provide high level of security additional modules we are adding in the KIDS system that is re-signature. In this work we show that recovering the key is extremely simple provided that the attacker can interact with KIDS and get feedback about probing requests. We are studying on the Re-Signature technique for key recovery in IDS system. This system is very efficient and secure as compare to existing system.

***Key words:*** Data Sharing System, Key based Attack

## I. Introduction

Many computer security problems can be essentially reduced to separating malicious from non-malicious activities. This is, for example, the case of spam filtering, intrusion detection, or the identification of fraudulent behavior. But, in general, defining in a precise and computationally useful way what is harmless or what is offensive is often too complex. To overcome these difficulties, most solutions to such problems have traditionally adopted a machine-learning approach, notably through the use of classifiers to automatically derive models of (good and/or bad) behavior that are later used to recognize the occurrence of potentially dangerous events. Strictly speaking, KIDS' idea of "learning with a secret" is not entirely new: Wang et al. introduced in Anagram, another payload-based anomaly detection system that addresses the evasion problem in quite a similar manner. We distinguish here between two broad classes of classifiers that use a key. In the first group, that we term randomized classifiers, the classifier is entirely public (or, equivalently, is trained with public information only). However, in detection mode some parameters (the key) are randomly chosen every time an instance has to be classified, thus making uncertain for the attacker how the instance will be processed. Note that, in this case, the same instance will be processed differently every time if the key is randomly chosen. We emphasize that randomization can also be applied at training time, although it may only be sufficiently effective when used during testing, at least as far as evasion attacks are concerned. KIDS belong to a second group, that we call keyed classifiers. The practicality of various types of cryptanalytic attacks depends on many factors: Attacks based on few cipher text are better than attacks that require many cipher text, known plaintext attacks are better than chosen plaintext attacks, no adaptive attacks are better than adaptive attacks, single key attacks are better than related key attacks, etc. Since it is difficult to quantify the relative importance of all these factors in different scenarios, we usually concentrate on the total running time of the attack, which is a single well defined number.

## II. Existing System

The major problem of computing optimal strategies to modify an attack so that it evades detection by a Bayes classifier. The problem can be formulated 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. ACRE learnable if there exists an algorithm that finds a minimal-cost in-stance evading detection using only polynomial 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. Additional works have revisited the role of ma-chine learning in security applications, with particular emphasis on anomaly detection.

## III. Survey Review

1) Pedro Domingo's develop a formal framework and algorithms for the view classification as a game between the classifier and the adversary, and produce a classifier

that is optimal given the adversary's optimal strategy. Experiments in a spam detection domain show that this approach can greatly outperform a classifier learned in the standard way, and (within the parameters of the problem) automatically adapt the classifier to the adversary's evolving manipulations.

2) Zach Jorgensen show that a classifier using their multiple instance counter attack strategy is more robust to good word attacks than its single instance Counterpart and other single instance learners commonly used in the spam filtering domain.
3) M.P. Revathi shows novel public auditing mechanisms for the integration of shared data with able user cancellation in mind. A public checker is always able to audit the integrity of shared data without accessing the either or data from the cloud, even if some part of shared data has been re-signed by the cloud.
4) Marco Barreno shows how these classes influence the costs for the attacker and defender, and give a formal structure defining their interaction. Framework used to survey and analyze the literature of attacks against machine learning systems. Also illustrate the taxonomy by showing how it can guide attacks against Spam Bayes, a popular statistical spam filter.

## IV. PROVABLY-SECURE CERTIFICATE LESS PROXY RE SIGNATURE SCHEME.

The paper proposes a provably-secure certificate less proxy re-signature scheme. Based certificate less public cryptosystem, it solves the using of certificate in certificate based scheme and removes key escrow in ID-based scheme. Analysis shows that the proposed scheme can satisfy the required properties of a proxy re-signature, and it avoids public key replacement attack and malicious KGC attack. The scheme provides stronger security. Proxy re-signature is a very useful tool for the interoperable DRM architecture and the proof of passed path in cloud computing. However, cloud users usually are mobile devices which are constrained with processing and power limitations. When a mobile user obtain the converted signature from the proxy (cloud server), it still cannot verify it due to the heavy computation cost. We propose a new definition of server-aided verification proxy re-signature which consists of a proxy re-signature scheme and a server-aided verification protocol. With the server aided verification protocol, some computational tasks for proxy re-signature verification are carried out by the proxy (cloud server), which is generally untrusted, therefore, it is very useful for mobile devices. We present, on the basis of unidirectional proxy re-signature scheme, two novel existential enforceability server-aided verification proxy re-signature schemes.

## V. KEY-RECOVERY ON KIDS

In this section we present a key-recovery attack when the only information about a payload an adversary gets from KIDS is its classification label, i.e., whether it is normal or anomalous. In some respects, this information is less fine grained than the anomaly score, so it is reasonable to expect that attacks working under this assumption will be slightly more complex .The central idea behind our attack is actually quite simple. We will provide KIDS with a normal payload concatenated with a carefully constructed tail. Such a tail contains a large number of unseen words separated by the candidate delimiter. If the delimiter does not belong to the key, the entire tail will be processed as just one word and the anomaly score will be roughly similar to that of the original payload. If this is the case, then the payload will be marked as normal with high probability. Conversely, if the delimiter does belong to the key, the tail will be fragmented into a large number of previously unseen words and transitions. This will negatively impact the anomaly score, invariably resulting in an anomalous payload. We next provide a more formal description and analysis of the attack. We is also studying on the key Keyed Intrusion Detection System. System tries to adapt to intrusion detection systems Kerckhoffs' principle stating that a cryptosystem should be secure even if everything about the system, except the key, is public knowledge.

## VI. CONCLUSION

This In this paper we have analyzed the strength of KIDS against key-recovery attacks. In doing so, we have adapted to the anomaly detection context an adversarial model borrowed from the related field of adversarial learning. We have presented key-recovery attacks according to two adversarial settings, depending on the feedback given by KIDS to probing queries. We are also providing high level security to it by providing the re-signature technology.

## 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] C. Gates and C. Taylo, "Challenging the Anomaly Detection Paradigm: A Provocative Discussion," Proc. New Security Paradigms Workshop (NSPW), pp. 21-29, 2006.
[3] Kolcz and C.H. Teo, "Feature Weighting for Improved Classifier Robustness," Proc. Sixth Conf. Email and Anti-Spam (CEAS '09), 2009.
[4] O. Kolesnikov, D. Dagon, and W. Lee, "Advanced Polymorphic Worms: Evading IDS by Blending in with Normal Traffic," Proc. USENIX Security Symp., 2005.
[5] 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.
[6] Metasploit Framework, www.metasploit.com, 2013.
[7] 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.
[8] 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.
[9] B. Nelson, A.D. Joseph, S.J. Lee, and S. Rao, "Near-Optimal Evasion of Convex-Inducing Classifiers," J. Machine Learning Research, vol. 9, pp. 549-556, 2010.

[10] B. Nelson, B.I.P. Rubinstein, L. Huang, A.D. Joseph, S.J. Lee, S. Rao, and J.D. Tygar, "Query Strategies for Evading Convex-Inducing Classifiers," J. Machine Learning Research, vol. 13, pp. 1293- 1332, May 2012.

[11] R. Perdisci, D. Ariu, P. Fogla, G. Giacinto, and W. Lee, "McPAD: A Multiple Classifier System for Accurate Payload-Based Anomaly Detection," Computer Networks, vol. 5, no. 6, pp. 864-881, 2009.

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