International Journal of Research in Advent Technology (IJRAT) Special Issue
E-ISSN: 2321-9637
Sharadchandra Pawar college of Engineering, Dumbarwadi, Pune 410504,
Organizes
National Conference on "Advancement in Engineering & Science" -MOMENTUM-18,
26th & 27st February 2018
Available online at www.ijrat.org

Preventing Key Attacks on Data Sharing System

Suraj B. Gawali[1], Bhagwan Kurhe[2]
Department of Computer Engineering Sharadchandra pawar COE, Otur
Department of Computer Engineering Sharadchandra pawar COE, Otur
surajgawalipatil@gmail.com[1], b.kurhe@gmail.com[2]

Abstract—Today security plays an very important role in the Networking system. Key recovery is the difficult task in dataaring system. When authorized user access the file then the creater will get the file as well as the key to decrypt that file. Butter some time interval if user found less trustworthy then data owner may block that user. The main problem is that user isill having the key so there may be possibility that user can are that key with others so to recover that issue data owner sign the particular file so even though the user try to leak theey then there is no issue of accessing the file. In this paper we proposed two type of key recovery Black box and Gray box keycovery. Many anomaly detection systems depend on machine learning algorithms to derive a model of normality that is latered to detect suspicious events.

Index Terms—Intrusion Detection System; Anomaly Detection

1. INTRODUCTION

Most of the computer security problems can be essentially reduced to separating malicious from non-malicious activities. This is, one such a example, in the case of spam filtering, intrusion detection, or the identification of fraudulent behavior. In general defining in a precise and computationally useful way what is harmless or what is offensive is often much complex. To overcome these difficulties, many solutions to such problems have traditionally adopted a machine-learning approach, 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 event. KIDS idea of learning with secret is not entirely a new. Anagram , another payload-based anomaly detection system was which addresses the evasion problem in same manner was introduced by Wang et al. Here we compare between two broad classes of classifier that make use of key. In thefirst group, that we term randomized classifiers, the classifier which is entirely public (i.e equivalently, is trained with public information only). However, in detection mode some parameters 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 we choose key is randomly. We emphasize that randomization can also be applied at training time, although it is sufficiently effective when used during testing only, at least as far as evasion attacks are concerned. KIDS belong to a second group, that we call keyed classifiers.There are practically various types of cryptanalytic attacks that depends on many factors: Attacks based on few ciphertext are better than attacks that require many ciphertext, 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.

2. LITERATURE SURVEY

[1] Juan E. Tapiador, Agustin Orfila, Arturo Ribagorda, and Benjamin Ramos,Key Recovery Attacks on KIDS, a Keyed: The difficult problem of computing optimal strategies is to modify an attack so that it evades detection by a Bayes classifier. The problem can be described in game theoretic terms, where each modification made to an instance comes at price and successful detection and evasion have measurable utilities to the classifier and the adversary, respectively. The author study how to detect such optimally modified instances by adapting the decision surface of the classifier and also formulates how the adversary may react to this. The setting requierd in assumes an adversary with full knowledge of the classifier to be evaded after how evasion can be done when such information is unavailable.

[2]M. Barreno, B. Nelson, A.D. Joseph, and J.D. Tygar,The Security of Machine Learning: It has proposed on the risks of applying machine learning algorithms to security domains. In it they introduce a

taxonomy which groups attacks on machine learning systems into different categories, depending on whether the adversary influences training or only analyzes an already trained system; whether the goal is to force just one mis-classification, or else

to generate too many so that the system becomes unusable; etc. The author described useful discussion on potential counter measures and enumerate various open problems.

[3]B. Biggio, G. Fumera, and F. Roli. ”Adversarial Pattern Classification Using Multiple Classifiers and Randomisation:

In this paper, they formulate the adversarial classifier reverse engineering problem (ACRE) as the task of learning

sufficient information about a classifier to construct attack instead of looking for optimal strategies. The author use a membership oracle as implicit adversarial model the attacker is given a chance to query the classifier with any chosen instance to determine whether it is malicious or not. A

reasonable objective is to find instances that evade detection with an affordable number of queries. The ACRE is learnable if there exist an algorithm that finds a minimal-cost in-stance evading detection using only polynomial many queries.A classifier is only 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 feature are ACRE klearnable

under linear cost functions. These classifiers should not be used in adversarial environment. More work by generalizes these results to convex-inducing classifiers, shows that it is generally not required to reverse engineer the decision boundary to construct undetected instances of near minimalcost. For the few open problems and challenges related to the classifier evasion problem. Additional works has revisited the role of machine learning in security application with particular emphasis on anomaly detection.

3. PROPOSED SYSTEM

In this paper, we proposed KIDS for recovering of key .Our work shows that recovering the key is extremely simple provided that the attacker can interact with KIDS. Keyed Intrusion Detection System, is a key dependent network anomaly detector that inspects packet payloads. We have provided discussion on this and other open questions in the hope of stimulating further research in this area. The attack 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. To provide user security for file transfer we requires pro-posed system. As in many roll based access system if the user have the access of the file then user can access the file any time but if the user found unauthorized then there is main challenge is revoking the access of that user .KIDS provide that facility of revoking the access of the user also resignature concept for the particular file

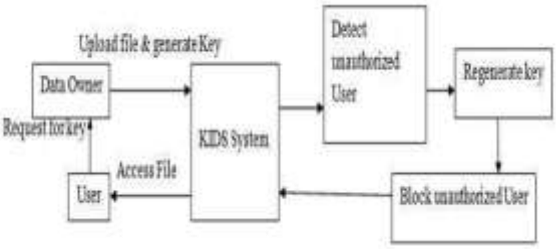


Fig. 1. Proposed System Architecture

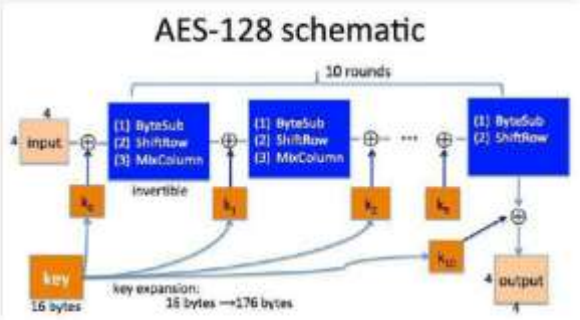
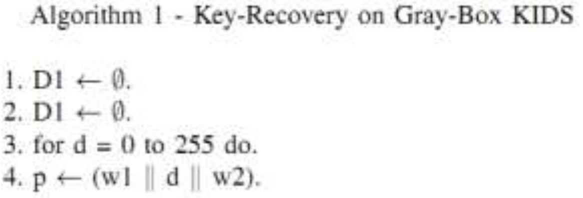


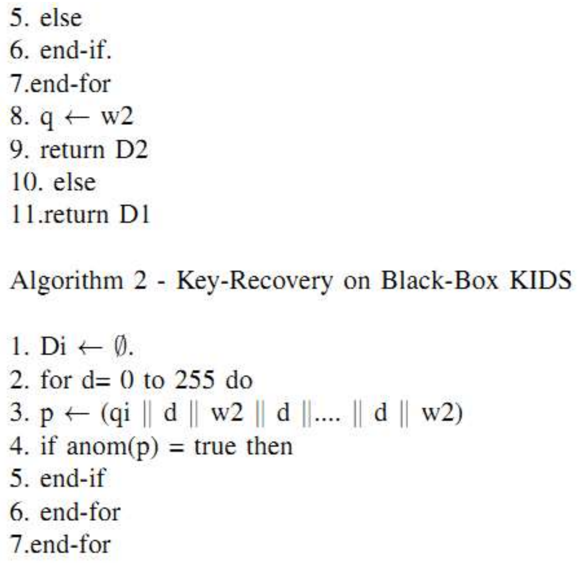
Fig. 2. AES 128 Schematic

4. ALGORITHM



Algorithm 1 - Key-Recovery on Gray-Box KIDS

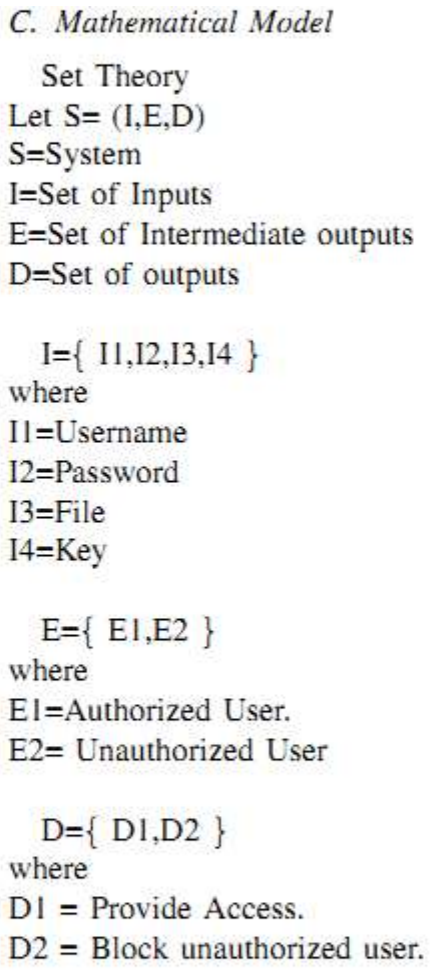
```
1. D1 ← ∅.
2. D1 ← ∅.
3. for d = 0 to 255 do.
4. p ← (w1 || d || w2).
```



```
else
end-if.
end-for
q ← w2
return D2
else
return D1
```

Algorithm 2 - Key-Recovery on Black-Box KIDS

```
Di ← ∅.
for d= 0 to 255 do
p ← (qi || d || w2 || d ||.... || d || w2)
if anom(p) = true then
end-if
end-for
end-for
```



C. Mathematical Model

Set Theory

Let S= (I,E,D)
S=System
I=Set of Inputs
E=Set of Intermediate outputs
D=Set of outputs

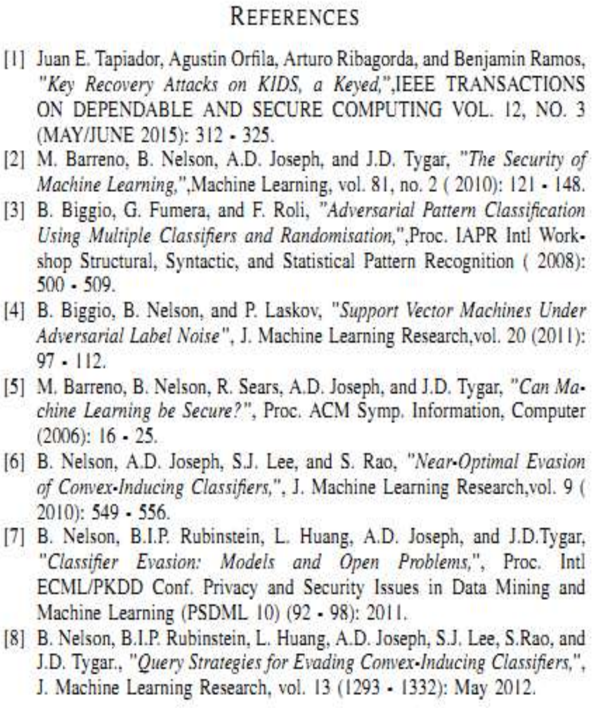
I={ I1,I2,I3,I4 }
where
I1=Username
I2=Password
I3=File
I4=Key

E={ E1,E2 }
where
E1=Authorized User.
E2= Unauthorized User

D={ D1,D2 }
where
D1 = Provide Access.
D2 = Block unauthorized user.

5. CONCLUSION

This system is based on Key-Recovery on Black-Box KIDS Key-Recovery on Gray-Box KIDS. KIDS system will offer a good platform to prevent information from leakage by regenerating key. This system will detect unauthorized user, and recover or regenerate key Block respective unauthorized user. The focus in this work has been on recovering the key through efficient process.



REFERENCES

[1] Juan E. Tapiador, Agustin Orfila, Arturo Ribagorda, and Benjamin Ramos, *"Key Recovery Attacks on KIDS, a Keyed,"*,IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING VOL. 12, NO. 3 (MAY/JUNE 2015): 312 - 325.

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

[3] B. Biggio, G. Fumera, and F. Roli, *"Adversarial Pattern Classification Using Multiple Classifiers and Randomisation,"*,Proc. IAPR Intl Workshop Structural, Syntactic, and Statistical Pattern Recognition (2008): 500 - 509.

[4] B. Biggio, B. Nelson, and P. Laskov, *"Support Vector Machines Under Adversarial Label Noise"*, J. Machine Learning Research,vol. 20 (2011): 97 - 112.

[5] M. Barreno, B. Nelson, R. Sears, A.D. Joseph, and J.D. Tygar, *"Can Machine Learning be Secure?"*, Proc. ACM Symp. Information, Computer (2006): 16 - 25.

[6] B. Nelson, A.D. Joseph, S.J. Lee, and S. Rao, *"Near-Optimal Evasion of Convex-Inducing Classifiers,"*, J. Machine Learning Research,vol. 9 (2010): 549 - 556.

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

[8] 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 (1293 - 1332): May 2012.