Key Recovery Attacks on KIDS

Gayatri R.Nirgude, Manisha D. Pawar,Nishigandha P. Nirmal,Harshada S. Patil.

Gayatri R.Nirgude ,BE Student, Dept. of Information Technology,Sanjivani C .O.E. Kopergaon, Savitribai Phule Pune University, Pune,Maharashtra, India

Manisha D. Pawar, BE Student, Dept. of Information Technology,Sanjivani C .O.E. Kopergaon, Savitribai Phule Pune University, Pune,Maharashtra, India

Nishigandha P. Nirmal, BE Student, Dept. of Information Technology,Sanjivani C.O.E. Kopergaon, Savitribai Phule Pune University, Pune,Maharashtra, India

.Harshada S. Patil, BE Student, Dept. of Information Technology,Sanjivani C .O.E. Kopergaon, Savitribai Phule Pune University, Pune,Maharashtra, India

ABSTRACT

KIDS is Keyed Intrusion Detection System that detects whether the user is authorized or unauthorized and based on it the system will block the unauthorized user and provide access to the normal user. Key recovery system is the difficult tasks in data sharing system. In group of employees or organization when any employee want to share important data or file then he can share it using this proposed system. This proposed system send the key to the user that user will get the file as well as the key to decrypt that file which is send by system. Key for decryption will get to the user through his or her registered e-mail id. That Key will be unique and each user will receive separate key for access that file. Every user have to enter that key to accessing the shared file. There are two possibilities of key recovery attack i.e. grey box attack and black box attack. System will detect both type of attacks and block that user for accessing that particular file only when he or she entered five times wrong key. The main problem is that user is still having the key so there may be possibility that blocked user can share that key with other person so we have to solve that problem. So this system provide security against anti-collision attack. System will generate new key and send it to users except blocked user.

Keyword: *Anomaly detection system, Black-box attack, Grey-box attack*

1. INTRODUCTION:

Use of internet is increasing day by day..Most of people uses internet for transmitting data over internet or store data on internet. There is possibility that data can may get hacked or misused. For better protection from such unauthorized access various anomaly detection methods are proposed. Anomaly detection system classifies activity in good or bad behavior. Anomaly detection system has two types Network Intrusion Detection System (NIDS) and Host Intrusion Detection System. A KID is NIDS based system which is used to provide better security from attacks on data. Security of KIDS system depends on secrecy of key and method used to generate key. Important in KIDS system is to provide better security from Black box attack and Gray box attacks. KIDS system provides security to data and protects stored data in encrypted format and keys are only known to authorize persons to make sure confidentiality of data.

Most anomaly detection system depends on machine learning algorithms to derive model of normality. That model later used to detect suspicious events. Such algorithms are generally susceptible to fraud, notably in the form of attacks carefully constructed to evade detection. So there is need to establish clearly defined and motivated adversarial models for secure machine learning algorithms. Various learning schemes have been proposed to

overcome this weakness. One such system is proposed in 2010 by Mrdovic and Drazenovic i.e.Keyed IDS (KIDS).It is key dependent network anomaly detector. KIDS or keyed classifier must preserve one fundamental property. The impossibility for an attacker to recover the key under any adversarial model. Key-recovery problem as one of adversarial learning. To overcome this problem gray-box and black-box key-recovery attacks were introduce. It is same t othe functioning of some cryptographic primitives, namely to introduce a secret element i.e. key into the scheme so that some operations are infeasible without knowing it.

1.1 Key Intrusion Detection System (KIDS):

KIDS is an anomaly detection system which detects the anomalous user from the anomaly score assigned to a chosen payload, and gives detail of that anomalous user and recover the key. In KIDS the core idea is of learning with a secret". In this system we present two instantiation of such attack for KIDS, one for each model. We pose key-recovery problem as one of adversarial learning. By adapting the adversarial setting proposed in the related problem we the notion of gray and black -box key-recovering attacks.

This system is going to detect the anomalous user from the anomaly score. This anomaly score is assigned to a chosen payload. In this system we are going introduced two methods for generating the attack on the system i.e. Gray-Box Key -Recovery on KIDS and Black-Box Key -Recovery on KIDS. This attacks which are 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 encompass such quantities as classification features. I suspect, however, that these variants may still be vulnerable to other attacks. After, the detection of anomalous user, the detail of that user such as which file it tried to access, how many times that user tried , how much was the effect of that attack on system performance information is given. After that if we have assign any key to that user than we revoke that key back and block that user and if have not assign any key to that user than we directly block that particular user.

2. RELATED WORK:

Many people have done work in this area. Some of work is given below:

2.1 Most anomaly detection systems rely on machine learning algorithms. KIDS the learned model and the computation of the anomaly score are both key-dependent, a fact which prevents an attacker from creating evasion attacks. It is cryptographic primitives, namely to introduce a secret element (the key) into the scheme so that some operations are infeasible without knowing it [1].

2.2 Passwords are used for user authentication by almost every Internet service today. Numerous attempts to replace passwords have failed in part because changing user's behavior has proven to be difficult. One approach is to classify login attempts into number of parameters such as source IP, geo-location, browser configuration, time of day, and so on. This service can then require additional verification. e.g. phone-based authentication [2].

2.3 M. Barreno, B. Nelson, A.D. Joseph, and J.D. Tygar present a taxonomy identifying and analyzing attacks against machine learning systems. It show how these classes influence the costs for the attacker and defender. It analyze the literature of attacks against machine learning systems [3].

2.4 Keyed IDS (KIDS) is namely 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. It prevents an attacker from creating evasion attacks. It shows recovering the key is extremely simple provided that the attacker can interact with KIDS and get feedback about probing requests[4].

3. PROBLEM DEFINATION

KIDS model does not meets the claimed security properties. Attacker easily recovers key by interacting system and its output. For ensuring data confidentiality, integrity and access control improvement in KIDS system is required.

4. PROPOSED SYSTEM

4.1 SYSTEM ARCHITECTURE

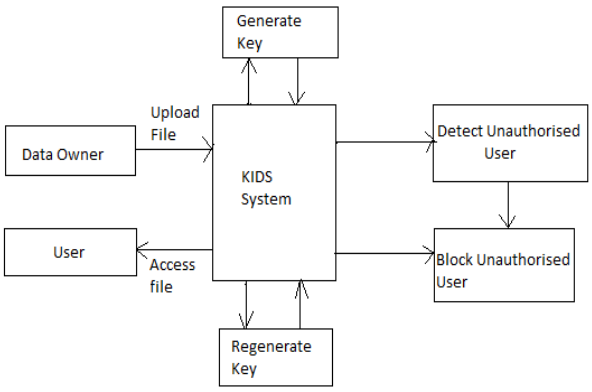

Fig1: System Architecture

In KIDS system data owner will upload file to KIDS system. KIDS system will generate key for particular uploaded file and share that file to valid and authorized users. When user want to access that file he or she must enter key which they get from KIDS system. On that key there are two possible attacks can be performed by unauthorized user to access file. These can be Black Box attack and Gray Box attack. In these attacks unauthorized user will try to revoke that key for file. In Black Box attack unauthorized person will pass string of characters which will be separated by delimiters or not, if match is found with actual key user can access file .In Black Box attack user is knowing only some part of key he or she will try different possible combination to access file means if unauthorized user is knowing w1 of key then he will try w2 and get key. Hens in KIDS system only three chances are provided to enter key if it becomes greater than three user will get block for particular file. KIDS system will generate new key for that file and send it to only valid user other than blocked user. Here collusion attack is prevented means if user is trying to access file by old key he will not able to access file. KIDS system provides better security to data from unauthorized access. Success of KIDS depends on secrecy of key.

4.2 PROPOSED ALGORITHMS

1. Key generation: Key is generated using Randomized algorithm. Eight bit alphanumeric key is generated.

2. Store file in encrypted format: File is Store in Encrypted format by using Elgamal algorithm. It is asymmetric algorithm, two public and private Keyes are used. And at receiver site file is decrypted.

3. Share secrete key with valid users: system will share generated key with valid users through their Email to access that particular file.

4. Find hidden internal collusion: Here blocked user should not access file using old key.

5. Detect unauthorized user: If user enters key more than three times then that user is get blocked for that particular file.

6. Regenerate key and send to valid users: After attack happen on file new key is generated by system and send to valid user except blocked user.

5. RESULT AND DISCUSSION

KIDS system do authentication work. Each user can able to upload file and system creates secret key for each individual files. Without secret key user not able to access uploaded data. Also after grey box and black box attacks KIDS system alert about attack.

6. CONCLUSION

The Propose system improves the security and confidentiality of stored data of system. KIDS System which works against the grey/black box attacks. System saves user data in encrypted format and takes the prevention steps against unauthorized use. System will detect both type of attacks and block that user for accessing that particular file only when he or she entered five times wrong key. So this system provide security against anti-collision attack. System will generate new key and send it to users except blocked user. Therefor blocked user will not be able to access that file. If blocked user try to leak the information about the key then there is no issue about security of file. Data owner of that file is also able to revoke access of any user for that particular file.

7. ACKNOWLEDGMENT

I take this opportunity to express my sincere gratitude to my guide Prof. C.D.Bawankar and head of department, and Prof. A. A. Barbind Prof. and project coordinator Dr. M. A. Jawale Department of information technology, Sanjivani COE, Kopargaon, for kind cooperation and capable guidance during the entire work. I would also like to thank our, Principal and Management for providing lab and other facilities.

8. REFERENCES

[1] Juan E. Tapiador, Agustin Orfila, Arturo Ribagorda,and Benjamin Ramos,"Key-Recovery Attacks on KIDS, a Keyed Anomaly Detection System",pp.312-325,2015

[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] K. Wang, G. Cretu, and S. Stolfo, "Anomalous payload-Based Worm Detection and Signature Generation," Proc. Eighth Int'l Conf. Recent Advances in Intrusion Detection (RAID '05), pp. 227-246, 2005.

[4] Markus Durmuth,David Mandell Freeman and Battista Biggio,"A statistical approach to measuring user authenticity", NDSS 1-15, 2015.

[5] B. Biggio, B. Nelson, and P. Laskov, "Support Vector Machines Under Adversarial Label Noise,"J. Machine learning Research, vol. 20, pp. 97-112, 2011.

[6] N. Dalvi, P. Domingos, Mausam, S. Sanghai, and D. Verma, "Adversarial Classification," Proc. 10th ACM SIGKDD Int'l Conf. Knowledge Discovery and Data Mining (KDD '04), pp. 99-108, 2004.