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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

Keyed Intrusion Detection System for Key-Recovery Attacks

Dipali R. Patil, Prof. Vina M. Lomte

M. E Student, Dept. of Computer Engineering, RMD Sinhgad S.O.E. Warje, Savitribai Phule Pune University, Pune, Maharashtra, India

H.O.D, Dept. of Computer Engineering, RMD Sinhgad S.O.E Warje, Savitribai Phule Pune University, Pune, Maharashtra, India

ABSTRACT:. With the anomaly detection systems, many techniques and approaches have been developed to track novel attacks on the systems. Anomaly detection systems used many algorithms and predefine rules; it's impossible to define all rules and algorithm and also once algorithm is known to attacker then new attack is created for same. To overcome this issue various machine learning schemes have been developed. One of such scheme is KIDS (Keyed Intrusion Detection System) which is depends on method used to generate KEY and secrecy of the KEY. Problem with KIDS is that attacker easily able to get key after grey box attack or black box attack. Hence improvement in KIDS system is required to provide more security with this attacks .Proposed system provides more security under both this attacks and also protect stored data. Proposed scheme can used to save data of various domains in cloud storage like for healthcare domain user can save the patient data. With the anomaly detection systems, many techniques and approaches have been developed to track novel attacks on the systems. Anomaly detection systems used many algorithms and predefine rules; it's impossible to define all rules and algorithm and also once algorithm is known to attacker then new attack is created for same. To overcome this issue various machine learning schemes have been developed. One of the such scheme is KIDS (Keyed Intrusion Detection System) which is depends on method used to generate KEY and secrecy of the KEY. Problem with KIDS is that attacker easily able to get key after grey box attack or black box attack. Hence improvement in KIDS system is required to provide more security with this attacks .Proposed system provides more security under both this attacks and also protect stored data. Proposed scheme can used to save data of various domains in cloud storage like for healthcare domain user can save the patient data.

KEYWORDS: Intrusion Detection System, Anomaly detection system, Network Intrusion Detection system.

I. INTRODUCTION

Use of internet increased tremendously. Most of the people used internet to transmit their data and used cloud to save it. There is possibility that data may get hacked and get misused. For better protection from such unauthorized users various Anomaly intrusion detection methods are proposed. Intrusion Detection System used to monitor network activity and inform to the main station about the details. Anomaly detection system classifies the activity and inform about unusual activity. Anomaly detection system includes predefine rules and extract features of behavior of system, uses the same data and compare it with the live data. Provide that result to the main station.

Anomaly detection system are having two types Network Intrusion Detection System (NIDS) and Host based Intrusion Detection System .NIDS mainly related to network and it monitor the network activity for multiple machines or servers .HIDS monitor single host or server [1].Keyed Intrusion Detection System(KIDS) is NIDS type system which is used to provide better security from various attacks. KIDS depends on method used to generate KEY and secrecy of the KEY[2]. With KIDS attacker easily able to get the KEY with interacting with the KIDS system and observing the outcome. Hence improvement in KIDS system is required to provide more security from grey or black box attacks [9] .In this paper proposed system provide more security under this attacks and also protect stored data. Proposed scheme can used to save data of various domains in cloud storage like for healthcare domain user can save the patient data.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

Motivation: Now a day's more and more people are getting connected to the Internet to take advantage of internet facility like data storage in cloud and data transfer over to other internet user. Network connectivity has become critical aspect. On one side, the Internet provides potential of reaching easily to end users, at the same time risk, because of the both (harmless, harmful) users of the internet. Attackers or hackers can get access to organizations information for various reasons. Since provide more security for data is one of the important factor in the networking.

For better network security Anomaly detection system is used which monitor the network activity and inform to the main station about unusual activity to take action. In case of anomaly detection system once attacker knows the rules or its set of algorithm they create new algorithm to attack on the system so for better improvement KIDS system is required. In KIDS to know behavior of model secret key is needed. Issue with KIDS is that attacker gets to know the key after interaction with the system so improvement is needed. With Improvement KIDS system provides better security from attacks. KIDS system stored data in encrypted format and keys are known only to authorize user to make sure confidentiality of the data. If any attacks happen it prevent attacker and provide information to main station about the incident

II. RELATED WORK

The Machine learning has been used in large area of security related tasks like network intrusion detection and spam filtering ,malware and , to identify between malicious and justify samples is serious problem, N. Dalvi, P. Domingos, Mausam, S. Sanghai, and D.Verma. explorer the same problem in [3] so bypassing can be classified. However, these problems are specifically challenging for machine learning rules and algorithms because of the existence of intelligent and adaptive adversaries who can carefully handle the input data to demote the performance of the detection system, breaching the underlying consideration of data stationary, so that meaning is that training data or test data follow the same distribution (although typically unknown).

Adversarial learning reasearch not only been direct the problem of analyse security of commom learning Algorithms to intentionally-targeted attacks, but also that of formulate learning algorithms with upgrade security. To deal with evasion attacks, clear knowledge of different types of adversarial data handling has been included into learning algorithms, e.g., using game-theoretical. An implicit assumption at the back of traditional machine learning and pattern recognition algorithms is that training data or test data are produce from the same, possibly not known, distribution. This assumption is however similar to the violated in adversarial settings, since malicious user may intentionally manipulate the input set data to downgrade the systems performance.

D. Lowd and C. Meek[4] notice that the attacker not required model the classifier explicitly ,but only observe lowest attacker instance as in the N. Dalvi, P. Domingos, Mausam, S. Sanghai, and D.Verma setting . They develop a concept of reverse engineering the adversarial classifier reverse engineering (ACER) problem .Given an malicious user cost function ,they observe the complexity of finding a lowest attacker cost that the classifier the labels as negative. They consider no general information of the training data, though the attacker may know the property space and also must include one positive and one negative example each. A classifier is ACRE-learnable of their presence a polynomial query algorithm that detect a lowest attacker cost for negative instance. They conclude that linear classifier is learnable ACRE with linear attacker cost functions and some other
Minor limitation. The ACER-learning problem gives a means of teach how challenging it is to use queries in to the reverse engineer classifier from specially hypothesis class using
a special feature space.

Evasion preventing methods:

O. Kolesnikov, D. Dagon, and W. Lee [5] introduce the new class of polymorphic type attacks, called polymorphic blending attacks, in that can effectually evade byte frequency-based network anomaly IDS by attentive matching the enumeration of the mutated attack single occurrence to the normal profiles. The develop the polymorphic blending attacks can showed as the subclass of the mimicry attacks. Author used a systematic way to the issue and formally explains the algorithms and steps needed to carry out such type of attacks. They not only explain that such attacks are attainable but also define the hardness of evasion under various circumstances. They present many detailed techniques using PAYL, a byte frequency-based the anomaly IDS. Many application payload-based anomaly IDS have been created which supervise the payload of a packet for the anomalies. In C. Kruegel and G. Vigna [6], develop four individual models, namely, character distribution, length, token finder, and probabilistic grammar, for the detection of the HTTP attacks. PAYL, developed by K.Wang and S. Stolfo [7], records the overall average frequency of

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

occurrences of each individual byte in the payload of the normal packet. A separate profile proposed for each packet length and port. In their recent task, the author's advice an improved version of PAYL to computes several profiles for each individual port. At the last of the training, clustering is used to decrease the number of profiles. They develop that instead of the byte frequency, one can also use the an n-gram model in a similar manner. One main disadvantage of the system is they not consider an recent advanced attacker, who may have knowledge of the IDS running at the end target and the actively try to evade it.

B. Biggio, G. Fumera, and F. Roli[8] experiments provide basis to analytical results derived from analytical framework , which convey that hiding the information of the adversary through randomization of decision function can be progress the hardness of evasion of the classifier. Author examine strategy consisting in the hiding information all about the classifiers to the adversaries through introduction of some randomness in the decision function and main focus on implementation of this method in a different multiple classifier system. Mrdovic and Drazenovic [2] develop Keyed Intrusion Detection System in which secret key is most important factor. Network anomaly detectors monitor packet payloads. The proposed strategy has three most important steps for implementation of the key. 1. Training Mode In the training mode payload distributed into words. Words are nothing but the byte sequence located between the delimiters. From this any unusual two byte assign to secret set S. This set S then again classified into the normal words, frequency count. 2. Detection Mode In the detection mode anomaly score to get counted according to the word frequency count. 3. Key Selection Here the Key then got selected after checking its detection quality.

Problem definition: 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.

III. PROPOSED SYSTEM

Our aim is to provide great degree expert, that it is the sensibly easy for an attacker to recoup the key in any of the settings. It is consider that the such an absence of security not protect from anticipate like children from key-recovery assaults. Here claimed the resistance against such assaults is key to any classifier that attempt to hinder avoidance by depending on a mystery bit of data. We have given exchange on this and other open enquiries in the trust of empowering further research around there.

The assaults here exhibited could be the forestalled by presenting various impromptu the counter measures of the frameworks, for example, constraining the most large length of words , or including such amounts as order components. Then again, that these variations may in any case be the powerless against some individual assaults. In this manner, our suggestion for future plans is to construct choices in light of hearty standards as opposed to specific fixes. Our aim is enhance the KIDS and try to meet maximum security properties so that it can able to secure stored data in clouds for various healthcare domain.

Architecture of proposed system and Proposed system module Details:
Node Creation & Routing: In this module, authenticated node is created for each user. KIDS system gets all details about user and stored the same for creating the rules. After node creation when user saved files, each files get saved in encrypted format. For each file user get secret Key.
Key- Recovery Attacks On Kids: At this point assault can able to attack and get the knowledge about the secret key. Assault able to get user data files and used same information for various reasons . Assault changes the Key and modified the same so it will not available further more to any authenticated user. Implicitly here grey box or black box attacks happened in which secret Key partially or fully modified and then make available to end nodes.
Keyed Anomaly Detection and Adversarial Models: Revisited After secret key modification KIDS system alerts to the main station and check the authentication list. If Unauthenticated node found then it get blocked by KIDS system. Modified key then recoup and provided to the intended node.
Performance Analysis: For performance evaluation following graph can be used Delay, Packet delivery ratio

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

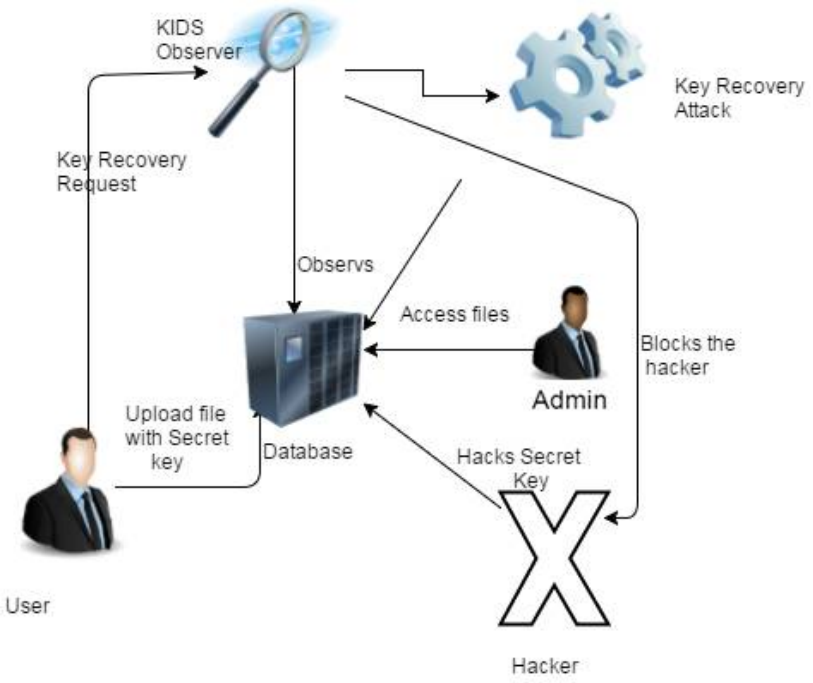

Fig.1. System Architecture

IV. PROPOSED ALGORITHM

Proposed System has below implementation techniques and algorithm. Key Generate using: AES algorithm, Data Stored using: Blowfish algorithm, Find Hidden Internal collision Recover the Key. Proposed system algorithm details steps are mention below

A. *AES Algorithm*

Secret Key are created using AES algorithm.

- Given a plaintext X, initialize state to be X and perform an operation Add round key, which x-ors the round key with state.
- For each of the first r − 1 rounds, perform a substitution operation called SubBytes on state using an S-box; perform a permutation ShiftRows on state; perform an operation MixColumns on state; and perform AddRoundKey.
- Define the ciphertext Y to be state

B. *Blowfish Algorithm:*

Save uploaded file data using blowfish algorithm.

Divide x into two 32-bit halves: xL, xR

- For i = 1to 16:
  xL = XL XOR Pi
  xR = F(XL) XOR xR
  Swap XL and xR
  Swap XL and xR (Undo the last swap.)
  xR = xR XOR P17
  xL = xL XOR P18
  Recombine xL and xR

C. *Share the secret Key*

Share the secret key with authenticated node.

D. *Find Hidden Internal collision*

Compare the K=K'

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

E. *Recover the Key*

V. MATHEMATICAL MODEL

Solution perspective for scheme studied
S= {s, e, X, Y, fm}
Initial state (s): User.
Exit/End state (e): Success or failure
Input (X):
X1 = User credentials X2 = User Data
Output (Y):
Y1 = Secret Key for each User
Algorithm (fm):
1) Secret Key created using AES algorithm.
2) Data save in encrypted format using blowfish algorithm.
3) Share the secret Key
4) Find internal collision

2^n Verification

$$H_1^{'} = e_{k"}(e_k(D_1^{'})); and$$

$$H_2^{'} = e_k(W \oplus H_1^{'}) \quad \text{.....[11]}$$

5) Recover the Key

$$d_{k'}(M^k) \oplus E_{q+1} = d_k(d_{k'}(M)) = d_{k'}(M^{"}) \oplus E_{q+1}^{'} \quad \text{..[11]}$$

VI. RESULT AND DISCUSSION

KIDS system do authenticated node for each node. Each user can able to upload file data and secret key created 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 and proceed with prevention steps using training data will implemented. Plotted graph for SMT time calculation shows that for hacking more required time as KIDS system having more complexity due to use of multiple graph then also time required for key recovery is less than the time of hacking.

	upload time(smt)	hack time(smt)	recovery time(smt)
file1	196	486	176
file2	168	352	171
file3	155	581	156
file4	142	454	120
file5	528	470	124
file6	373	522	138
file7	176	414	135
file8	229	380	123
file9	325	472	216
file10	237	478	209

Fig.2. Performance of the system

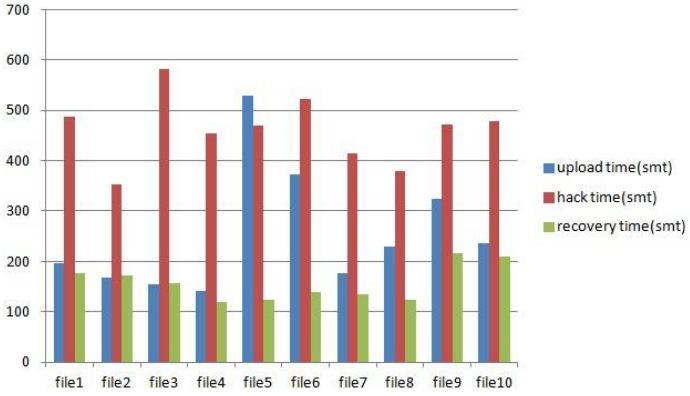

Fig.3. Graph for Performance of the system

VII. CONCLUSION

The Propose system improves the security and confidentiality of stored data over cloud and Intranet. The new implemented technique offers a better KIDS System which works against the grey/black box attacks. Also to increase

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

Security complexity system saves user data in encrypted format and takes the prevention steps against unauthorized use.

VIII. ACKNOWLEDGMENT

I take this opportunity to express my sincere gratitude to my guide and head of department, Prof. Vina M. Lomte, Department of Computer Engineering, RMDSSOE, Pune University, for her 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.

REFERENCES

1. A Scarfone, Karen; Mell, Peter (February 2007). "Guide to Intrusion Detection and Prevention Systems (IDPS)" . Computer Security Resource Center (National Institute of Standards and Technology) (80094). Retrieved 1 January 2010.
2. R. S. Mrdovic and B. Drazenovic, "KIDS-Keyed Intrusion Detection System" Proc. Seventh Intl Conf. Detection of Intrusions and Malware,and Vulnerability Assessment (DIMVA 10), pp. 173-182, 2010.
3. N. Dalvi, P. Domingos, Mausam, S. Sanghai, and D. Verma, "Adversarial classification,"in 10th ACM SIGKDD Intl Conf. on Knowl. Discovery and Data Mining, 2004, pp. 99108.
4. D. Lowd and C. Meek, "Adversarial Learning", Proc. 11th ACM SIGKDD Intl Conf. Knowledge Discovery in Data Mining (KDD 05), pp. 641-647, 2005.
5. O. Kolesnikov, D. Dagon, and W. Lee, "Advanced Polymorphic Worms: Evading IDS by Blending in with Normal Traffic", Proc.USENIX Security Symp.2005.
6. C. Kruegel and G. Vigna. "Anomaly detection of web-based attacks" In Proceedings of ACM CCS, pages 251-261, 2003.J. G
7. K.Wang and S. Stolfo. "Anomalous payload-based network intrusion detection". In Recent Advances in Intrusion Detection, 2004.
8. 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,pp. 500-509, 2008.
9. Aarti Devi, Ankush Sharma, Anamika Rangra "A Review on DES, AES and Blowfish for Encryption & Decryption" International Journal of Computer Science and Information Technologies, Vol. 6 (3) , 2015, 3034-3036.
10. Yufen Shen "The Implementation of Anti-attack AES Mathematical Model in Library Network Encryption" 2nd International Conference on Computer and Information Application (ICCIA 2012)
11. Don Coppersmith1 , Lars R. Knudsen2 , and Chris J. Mitchell3 "Key recovery and forgery attacks on the MacDES MAC algorithm" IBM Research, T.J. Watson Research Center, Yorktown Heights, NY 10598, USA
12. Juan E. Tapiador, Agustin Orfila, Arturo Ribagorda, and Benjamin Ramos Key- Recovery Attacks on KIDS, a Keyed Anomaly Detection System" IEEE transaction on DEPENDABLE AND SECURE COMPUTING, VOL. 12, NO. 3, MAY/JUNE 2015

BIOGRAPHY

Ms Dipali Patil is pursuing her Masters of Engineering in the Computer Science Department, Sinhgad School of Engineering, Savitribai Phule University. She received Bachelor of Engineering degree in Computer Science from University Of North Maharashtra,Jalgaon, India

Prof. Vina M. Lomte is the HOD of Computer Dept. at RMD SSOE College, Pune, having more than 10+ years of experience in the field of teaching and research. The domains of her research are Software Testing, Software Engineering and Web Security.