ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering, Vol.3 , No.5, Pages : 411- 413 (2014)
Special Issue of ICACSSE 2014 - Held on October 10, 2014 in St.Ann's College of Engineering & Technology, Chirala, Andhra Pradesh

A Novel Intrusion Detection System with Classification and Signature approach

[1]Y. Keerthi, [2]CH . SwapnaPriya
[1]Final M.Tech Student, [2]Assistant Professor
[1,2]Dept of Computer Science and Eng
[1,2]Pydah College of Engineering, Visakhapatnam, AP, India

Abstract:- Identifying and preventing unauthorized access (Intrusion Detection) is still an important research issue in the field of information security. In mobile adhoc networks every node independently communicate with other node through the intermediate peers without intermediate servers, But security is the primary issue while transmission of data over the peers, We are proposing a hybrid approach with identification of unauthorized access by NAIVE BAYESIAN and authentication by the digital signature.

Index Terms: NAIVE BAYESIAN Classification, Digital Signature, Intrusion Detection System.

INTRODUCTION

Cloud computing is a process that provides the easy usage on request network browsing to a distributed pool of dynamic settings of computing resources . This cloud scheme increases the availability and it consists of five particular features, three delivery methods and four hosting models.

Cloud computing has created main interest [4] in both organizational and industry, built is an evolving scheme. Its goal is to tighten the economic model with traditional methods, computing methods, spreading services, and information topologies. Confusion exists in IT communities and it is about how a cloud differentiates from traditional models of computing and how these differences affect. Some consider cloud as a new technical awareness while others consider as it evolution of technology, economy. The cloud computing significantly enhances collaboration and scale thus enabling a really central computing model over the Internet topology. Whatever without certain security and privacy solutions implemented for clouds result in large failure. There are several case studies of possible cloud connectors to indicate that security and privacy is the main concern hindering.

Various anomaly detection and prevention mechanisms available in traditional approaches like signature based approaches, trust based approaches, statistical based approaches and probability based approaches. Traditional approaches not optimal while comparing with static attributes and retrieval of trust computational values from third parties or data rating calculated by intermediate nodes. Even though classification based techniques analyzes the behavior of incoming node, they are suffering from mismatched feature set selection and major issue is, semantic comparison is not possible. Various approaches available for identifying the unauthorized behavior of the incoming nodes like with their trust measures like direct trust, indirect trust and reputation metric, these metrics always maintained globally, so network cannot directly depend on third party. Main drawback with the Signature based IDS mechanisms are pattern based and these must be continuously updated and difficult to identify the new pattern. Direct classification techniques make more time complexity while classifying the network traffic of in and out data flows.

RELATED WORK

Various identities (malicious detection systems) methods implemented by the various research works such as Static measures, double ask and other works but these methods have their own advantages and disadvantages. It finds the number of losses by the neighbor peers and it can be referred as mismatched node. Constant measurement to verify source node features while data exchanging with destination node. Double ack checks the resultant of peers from two end points, for successful communication or failure communication of the peers.

- There is an instance of misbehavior node identification method during the network failures between peers.
- Constant measures may not results optimal results and cannot expect the node with distinct parameters
- Two ack works very effectively but overhead, when more number of packets transmitted.

There is previous method used for verifying schemes, to calculate attack graphs. We verify significant scalability disturbances using this tool. There is a reason for finding many attack paths in the graph that differentiate only in the order in which self-attack statements are attempted. Incomplete decreasing order can drop such paths but it has not been view that the

ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering, Vol.3 , No.5, Pages : 411- 413 (2014)
Special Issue of ICACSSE 2014 - Held on October 10, 2014 in St.Ann's College of Engineering & Technology, Chirala, Andhra Pradesh

method can improve the increasing number of attack graphs. After deleting such path results graphs could be exponential. We can identify that it is very difficult to decode the synonym of the Boolean values in node and logical association among peers is not always same.

There is another previous approach implemented by a tool for creating attack graphs [7][8]. Likewise the model verifying the approach that the peers in their attack graphs describe the activity of the network in the form of a group of variables and the edges notated an attacker's work and approaches that modify the state. Instead of using a model verifier, search engine used to conduct the analysis. This state based attack graph presentation has leads to exponential problems and such situations were indeed reported by the authors. Then used technique same as incomplete order of reduction to eliminate the duplicate attack paths to the explosion but it is not agreed from the paper how efficient this method has been and no executed data was given.

We noticed that most of the attacks are mono-tonic or non-monotonic and it have created causes in general configured data. Therefore at a correct level, all of these attacks' conditions can be explained using propositional methods on configuration information. In some other cases non-monotonic attacks can be referred as monotonic if one ignores the low-level stage details on how the attack can happen in that situation. For this there is a simple group of rules can implemented in almost all types of attack situations in a network [12].

PROPOSED WORK

In this paper we are proposing an integrated model of Intrusion detection system. Node behavior can be identified by classification algorithm and Digital signature for the authentication purpose and to identify the data packet which is received from the authorized user or not. NAIVE BAYESIAN algorithm classifies the source node information with training data which has the previous visited information and analyzes node after the posterior probability computation, our Experimental result gives optimal results than the previous approach because our approach developed an Intrusion detection system with combined IDS (here with NAIVE BAYESIAN) and digital signature . An Efficient IDS with NAIVE BAYESIAN classifier to identify the malicious peers and authentication can be provided by the hash codes of the data packets. Integrated approach gives optimal performance in dynamic nature.

Intrusion detection system can be developed with the efficient NAIVE BAYESIAN classification algorithm by classifying the testing sample of source node and with training samples, by calculating the initial and conditional probability with respect to individual attributes and decision classes and finally classifies the node as anonymous or un-anonymous node.

Sample space: set of agent

H= Hypothesis that X is a node

P (H/X_i) is our confidence that X_i is an incoming node

P(H) is Prior Probability of H and it is probability that any given training sample is an agent regardless of its anomaly or not anomaly behavior

P(H/X) is a conditional probability and P(H) is independent of X

Estimating probabilities

P(H), $P(X_i)$ and $P(X_i/H)$ may be estimated from given training and testing data samples

$P(H|X_i)=P(X_i|H)*P(H)/P(X_i)$

Steps Involved:

1. Each training data sample is of attribute type

$X= (x_j)$ j =1(1….n), where x_j is the values of X for attribute A_j

2. Suppose there are m decision classes C_j, j=1(1…m).

$P(C_i|X) > P(C_j|X)$ for 1<= j <= m, j>i

i.e classifier assigns X to decision class C_j having highest posterior probability conditioned on testing sample X

The decision class for which $P(C_j|X)$ is maximum is known as maximum posterior hypothesis of the sample.

From Bayes Theorem

3. $P(X_i)$ is constant and Only need be maximized.

- if class initial probabilities not known prior then we can assume all decision classes to be more equally likely decision classes
- Otherwise maximize the samples

$P(C_i) = Si/S$

4. Naïve assumption for attribute independence

$P(X|C_j) = P(x_1,…..,x_m|C) = PP(x_k|C)$

5. To classify an unknown testing sample X_i, compute each decision class C_i and Sample X is assigned to the class

iff ($Prob(X_i|C_i)P(C_i) > P(X_i|C_j) P(C_j)$).

Authentication of the data packets can be verified by the efficient signature algorithm, in this module sender applies digital signature algorithm on data packets which are transmitting and at the receiver end receiver verifies the data packet authentication by the

ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering, Vol.3 , No.5, Pages : 411- 413 (2014)
Special Issue of ICACSSE 2014 - Held on October 10, 2014 in St.Ann's College of Engineering & Technology, Chirala, Andhra Pradesh

same signature algorithm by comparing the signatures generated over the data packets.

Empirical Signature algorithm

Algorithm: Generate file with Signatures

Input: User File in ASCII (Fo)

Output: User File with Signature appended at end of (Fn)

Method: In order to apply hash function on each n byte block of file which is corrupted? If we consider it with the file we perform the following steps to make (m mod n)= 0 of Fo

M← Calculate Length of (F0)
n← Length of Block (any one of128/ 256 /512/ 1024 /204/4096/ 8192) bytes

res← reserved 16 bytes
P ←m mod n
Q ← n- (P + res)

if(Q > 0)
F←Append Q zeros at the end of F_0
Else if(Q < 0)
R ←n+ Q
F1 ←Append R zeros at the end of F_0
F1← Append res at the end of F_0
In order to generate Signatures of Fl, perform the following steps
I← Calculate_ Length of (F_l)
count←l/n
For j←1 to count
S ← 0
S ←reverse[$\sum^{n}_{A=1}$((A XOR B) v (A ∩ B))]

Where B <- to_Integer (to_Char (A))

Sig ←Sig+ to-Binary (S)

Fn←F1 + Sig

For Implementation purpose we have used a synthetic data set which includes the previous peers details which are anonymous or un anonymous and fields includes in training dataset are node name or ip address, type of protocol and number of packets transmitted and input sample can be retrieved from the node which connected.

Every node in the network acts as independent node, it means, can receive, transmit and classifies the peers .Every individual node itself maintains the training dataset to classify the anonymous behavior of the node which is connected

CONCLUSION

Current research efficiently works with classification mechanism by computing the conditional probabilities of the testing sample with respect to training samples and authentication of data packets can be verified by the intermediate peers while transmitting the data from source to destination node. Our experimental results shows efficient results than the traditional approaches.

REFERENCES

1. Cloud Security Alliance, "Security Guidance for Critical Areas of Focus in Cloud Computing V2.1," http:// www.cloudsecurityalliance.org/csaguide.pdf.
2. D. Catteddu and G. Hogben, "Cloud Computing: Benefits, Risks and Recommendations for Information Security," ENISA, 2009; www.enisa.europa.eu/act/rm/ files/deliverables/cloud-computing-risk-assessment/ at_download/fullReport.
3. P.J. Bruening and B.C. Treacy, "Cloud Computing: Pri vacy, Security Challenges," Bureau of Nat'l Affairs, 2009; www.hunton.com/files/tbl_s47Details/FileUpload 265/2488/CloudComputing_Bruening-Treacy.pdf.
4. H. Takabi, J.B.D. Joshi, and G.-J. Ahn, "SecureCloud: Towards a Comprehensive Security Framework for Cloud Computing Environments," Proc. 1st IEEE Int'l Workshop Emerging Applications for Cloud Computing (CloudApp 2010), IEEE CS Press, 2010, pp. 393–398.
5. Y. Chen, V. Paxson, and R.H. Katz, "What's New About Cloud Computing Security?" tech. report UCB/EECS-2010-5, EECS Dept., Univ. of California, Berkeley, 2010; www.eecs.berkeley.edu/Pubs/ TechRpts/2010/EECS-2010-5.html.
6. E. Bertino, F. Paci, and R. Ferrini, "Privacy-Preserving Digital Identity Management for Cloud Computing," EEE Computer Society Data Engineering Bulletin, Mar. 2009, pp. 1–4.
7. M. Ko, G.-J. Ahn, and M. Shehab "Privacy-Enhanced User-Centric Identity Management," Proc. IEEE Int'l Conf. Communications, IEEE Press, 2009, pp. 998–1002.
8. J. Joshi et al., "Access Control Language for Multidomain Environments," IEEE Internet Computing, vol. 8, no. 6, 2004, pp. 40–50.
9. M. Blaze et al., "Dynamic Trust Management," Computer, vol. 42, no. 2, 2009, pp. 44–52.
10. Y. Zhang and J. Joshi, "Access Control and Trust Management for Emerging Multidomain Environments," nnals of Emerging Research in Information Assurance, Security and Privacy Services, S. Upadhyaya and R.O. Rao, eds., Emerald Group Publishing, 2009, pp. 421–452.