International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2015): 78.96 | Impact Factor (2015): 6.391

Internal Intrusion Detection for Data Theft and Data Modification using Data Mining

Rahul Neware

P.G. Student, Department of Computer Science and Engineering, G.H.R.C.E. College, CRPF Gate Hingna Road Nagpur, Maharashtra, India

Abstract: ***Many times user shares username and password with their friends, colleagues or any other well known person to do their jobs or perform any task in their system. Many times this type of users which knows the password and username of user will logged into the system and perform various malicious behave inside system. In India about 40% attacks and data loss occurs due to the internal intruder. Internal Intruder are very difficult to detect because attacker logged into the system as a real system user. There is traditional Intrusion detection system (IDS) is available but it only finds intruder outside of the firewall and within the networks. For single standalone system Host based intrusion detection system (HBIDS) is invented but by using this antivirus program is stopped working and it will only filters the network traffic and finds the simple malicious program and block it but the internal data modification and data theft is not shown by HBIDS. Proposed system in this paper will find out the internal intruder and data theft, data modification and data copy attack perform by the internal intruder.***

Keywords: Internal Intruder, Intrusion detection System (IDS), Data Mining, Digital Signature, Data theft or Data Modification

1. Introduction

Internal Intruder is most dangerous aspect while considering the privacy of user various times potential user share his password and username to the known user e.g. friends or colleagues by doing his jobs instead. Attacker get the details of user by using phishing attack, Brute force attack or can also use Trojan horse program to get the login details of the user because most of the time user uses normal username and passwords for logged into the system and that is the main reason attacker easily get their login details.

Once the attacker gets into the system it will perform various unwanted tasks like Date stealing, Data modification of important data of any organization and other thing like spear phishing attack, Pharming attack and the most important it will used system in firing DDoS attack in network. When the attacker perform this type of attack when logged into the system as a potential user it is difficult to detect Traditional Intruder detection system and Host based intrusion detection system to detect this type of attack because they only deal with the active attacks which are performed outside of the firewall and within network so it is very difficult to detect such type of attack.

In this research we show when any data theft, data modification performed or copy of data is performed on the save data of the system. This paper totally focuses on the data theft, data modification. It shows in the phases as follows 1) Potential user logged into the system and create file of any type then store it with 1 backup file and signature of that file. 2) Intruder logged into the system with valid details of potential user and performs any modification or theft of data. 3) Matching of signature of modified data and created data takes place and showed the intruder.

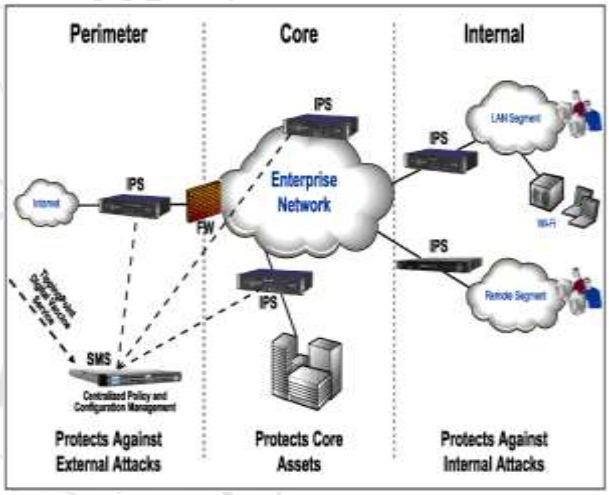

Figure 1.1: Various placement of Intrusion Protection System (IPS)

2. Related Work

Computer Forensics is a governing body which deals with investigation and analysis technology to gather and preserve evidences from computer and which type of attack is performed by attacker. Many researchers studied about Internal Intrusion but every time they find out that Intrusion detection is hard to detect while attacker is performing any malicious task. Intrusion Detection System only find out threats between network and relation of them with network layer like types of attacks, network behaviors and stores it as a attacker log.

Packet sniffer tool is used to collect and give information about network position and packet distribution [13]. After that attack log patterns are studied from log file of user habit by O' Shaughnessy and Gray [14]. Some Nature inspired optimization techniques are used by Wu and Banzhaf to give the patterns of operation by attacker [15]. F.Y.Leu used command level to collect attacker system call patterns [16].

Lightweight Intrusion Detection System is developed by Hu et al to find out which system of user have performed malicious behavior.

3. Architecture of System

System consists of Server side and Client side set of operations in first started with the client side. Potential user of system first Registered into the system which gives him a valid username and password and this pattern of Username and password is used for logged into the system successfully. This patterns are stored into the database and used for checking validity of user. Once the user logged into system it will perform various operations like Create new file, Edit File, Delete File, etc. While creating new File user enter some value or strings values into it, after entering all the data as soon as he saved the file signature of that file is formed by using Data Mining Algorithm (Map Reducing algorithm) and overall file is encrypted by using any encryption algorithm (AES).

As any attacker enter into the system as a potential user it will change data or perform any changes into data then the changes creates new signature of modified data and server side before changing habit file this signature is compared with signature of the potential user of system. If the signature is not matched then Intruder is detected by system otherwise changes are made by potential user.

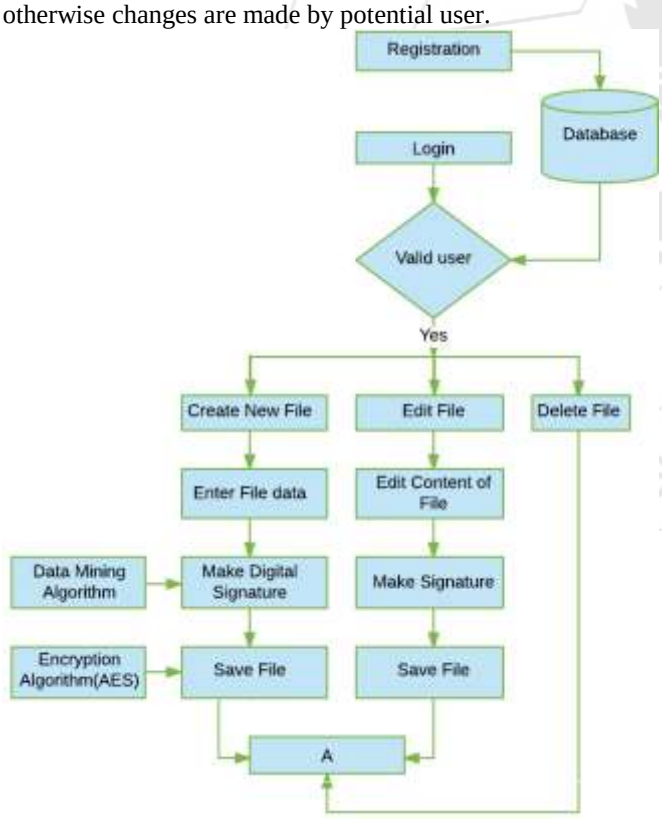

Figure 3.1: Client side operations

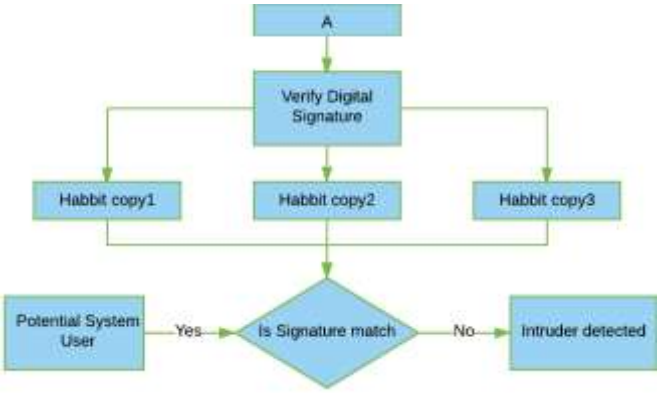

Figure 3.2: Server side intrusion detection

4. Conclusion and Future Scope

It is very difficult to detect internal intruder because attacker logged into the system with the potential user login patterns. In the proposed system data modification or any data related attack are detected. In future we can take the continuous data from the systems which are connected in the network to detect internal intruder and by using data mining and machine learning train the system. Using continuous user patterns detection of attack is possible by using Computer Forensics database which shows attack type and on that time prevention can be made from continuous use of system by intruder.

References

[1] S. Gajek, A. Sadeghi, C. Stuble, and M. Winandy, "Compartmented security for browsers—Or how to thwart a phisher with trusted computing,"in Proc. IEEE Int. Conf. Avail., Rel. Security, Vienna, Austria, Apr. 2007,pp. 120–127.
[2] C. Yue and H. Wang, "BogusBiter: A transparent protection against phishing attacks," ACM Trans. Int. Technol., vol. 10, no. 2, pp. 1–31, May 2010.
[3] Q. Chen, S. Abdelwahed, and A. Erradi, "A model-based approach to self-protection in computing system," in Proc. ACM Cloud Autonomic Comput. Conf., Miami, FL, USA, 2013, pp. 1–10.
[4] F. Y. Leu, M. C. Li, J. C. Lin, and C. T. Yang, "Detection workload in a dynamic grid-based intrusion detection environment," J. Parallel Distrib. Comput., vol. 68, no. 4, pp. 427–442, Apr. 2008.
[5] H. Lu, B. Zhao, X. Wang, and J. Su, "DiffSig: Resource differentiation based malware behavioral concise signature generation," Inf. Commun. Technol., vol. 7804, pp. 271–284, 2013.
[6] Z. Shan, X. Wang, T. Chiueh, and X. Meng, "Safe side effects commitment for OS-level virtualization," in Proc. ACM Int. Conf. Autonomic Comput., Karlsruhe, Germany, 2011, pp. 111–120.
[7] M. K. Rogers and K. Seigfried, "The future of computer forensics:A needs analysis survey," Comput. Security, vol. 23, no. 1, pp.12–16, Feb. 2004.
[8] J. Choi, C. Choi, B. Ko, D. Choi, and P. Kim, "Detecting web based DDoS attack using MapReduce operations in cloud computing environment," J. Internet Serv. Inf. Security, vol. 3, no. 3/4, pp. 28–37, Nov. 2013.

[9] Q. Wang, L. Vu, K. Nahrstedt, and H. Khurana, "MIS: Malicious nodes identification scheme in network-coding-based peer-to-peer streaming," in Proc. IEEE INFOCOM, San Diego, CA, USA, 2010, pp. 1–5.
[10] Z. A. Baig, "Pattern recognition for detecting distributed node exhaustion attacks in wireless sensor networks," Comput. Commun., vol. 34, no. 3, pp. 468–484, Mar. 2011.
[11] H. S. Kang and S. R. Kim, "A new logging-based IP traceback approach using data mining techniques," J. Internet Serv. Inf. Security, vol. 3, no. 3/4, pp. 72–80, Nov. 2013.
[12] K. A. Garcia, R. Monroy, L. A. Trejo, and C. Mex-Perera, "Analyzing log files for postmortem intrusion detection," IEEE Trans. Syst., Man, Cybern., Part C: Appl. Rev., vol. 42, no. 6, pp. 1690–1704, Nov. 2012.
[13] M. A. Qadeer, M. Zahid, A. Iqbal, and M. R. Siddiqui, "Network traffic analysis and intrusion detection using packet sniffer," in Proc. Int. Conf. Commun. Softw. Netw., Singapore, 2010, pp. 313–317.
[14] S. O'Shaughnessy and G. Gray, "Development and evaluation of a data set generator tool for generating synthetic log files containing computer attack signatures," Int. J. Ambient Comput. Intell., vol. 3, no. 2, pp. 64–76, Apr. 2011.
[15] S. X. Wu and W. Banzhaf, "The use of computational intelligence in intrusion detection systems: A review," Appl. Soft Comput., vol. 10, no. 1, pp. 1–35, Jan. 2010.

Author Profile

Rahul Neware is a PG Student in GHRCE College Nagpur, Maharashtra. He's 6 international publications and 2 conference publications with Young Scientist award.