

PREVENTION OF INSIDER ATTACKS USING HYBRID APPROACH

¹Sakshi Bhargava, ²Sahil Sharma
^{1,2}Computer Science and Engineering
 SRM Institute of Science and Technology, Chennai, India
¹bsakshi2003@gmail.com, ²sahilu01@gmail.com

Abstract: The main objective of this paper is to tell about the impact of internal attacks or breaches within an organization. One of the major reasons of data breaches is malicious insiders who have the access rights knowledge of data values and technical know-how of escalating their privileges in launching such insider attacks. There are many privileges given to the employees by the organization but liberty comes with a responsibility and that responsibility seems to be missing in many case studies found for larger organizations. The employees of the organization have been leaking sensitive information which have brought huge amount of loss for the company. Several measures to detect such insider attacks have been discussed and various models for the same have been taken into account in order to bring out the gravity of the topic. This paper discusses several measures which can be used to prevent and safeguard sensitive data and resources applicable to both enterprises as well as government agencies.

Keywords: Insider attacks, data exfiltration, data breach, classified data.

1. Introduction

In early days all devices and data were under the control of organization the attacks were either from inside or purely outside because of the network constraints. With the popularity of new technologies such as cloud computing and mobility of the devices the data is now distributed across various networks and service providers. Thus, a single breach can exploit huge amount of data. Data exfiltration can be done by insiders like employees contractors who use their access inappropriately. Insider attack refers to the threat that is caused by the individual who is integral part of the organization. This activity includes unauthorized access to sensitive information, copyright violations and communicating to outer world regarding the happenings inside an organization.

This threat has become a huge problem to our government agencies as well as large private firms. The most important challenges in detecting the insider attacks are

- (1) Defining the events that take place prior to such attacks.
- (2) Deriving a methodology that could predict the insider attacks effectively.

2. Definitions

A. Insider Attack

An insider attack is a form of attack which is performed by an integral member of the organization, with authorized access to the sensitive information leading to huge financial loss to an enterprise.

B. Data Exfiltration

Data exfiltration is the transfer of data either manually or by other means from network access by an authorized person.

C. Classified Data

Classified data is the data restricted by law and which can be accessed by limit class of people.

3. Related Works

Insider attacks and its gravity has been discussed by Dipankar Dasgupta, Arunava Roy, Debasis Ghosh [1] wherein they have devised a multi-user permission strategy to access sensitive information. This paper describes a model in order to prevent the internal breach in an organization. The organization has been seen as a hierarchy in the proposed model where the top level in the hierarchy having the highest privilege of giving access rights to the information seeker. According to the proposed model if a person wants to access a sensitive piece of information, he has to be granted permission by the top levels of the hierarchy which is decided by a complex random function. The complex random function makes sure that every time different permission granters are selected so that there is no chance of tracking the pattern.

The paper describes a complex algorithmic approach using connected graph which computes the randomness of the authority being assigned to grant the

permission. The figure [1, 1] below describes the working of the proposed model.

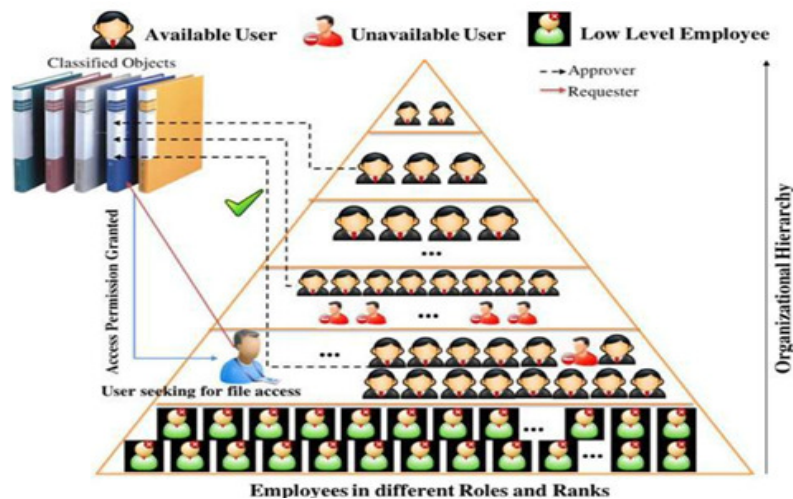


Figure 1. Overview of the model[1]

A study by F.L. Greitzer , L.J. Kangas , C.F. Noonan , A.C. Dalton , R.E. Hohimer [2] has found potential correlations between the behavior of the inside breachers at different breach points. They have proposed a predictive model which is based on Artificial Neural Networks (ANN) model and Bayesian model. The accuracy of these models are based on the feedback provided by various company heads and HRs. This model focuses on identifying the potential breachers and threats that an organization can face, preventing it from catastrophic losses. The major focus here is to analyze the employee behavior which would benefit the employee and employer alike.

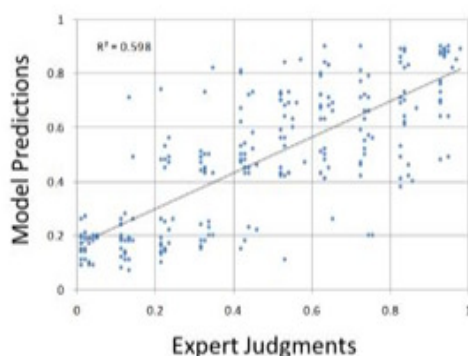


Figure 2. Model prediction vs Expert judgments graph [2]

Colin Armstrong [3] suggests the various insider threats are due to the increase in non-traditional sources

like social media. He has mapped the insider attacks to the social media via TPP triangle: technology, process and people. Because of vulnerability of such resources the insider attacks are expected to increase.

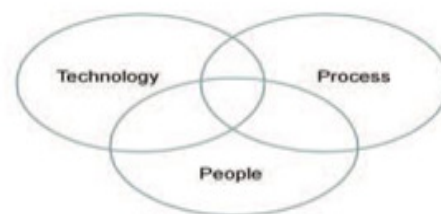


Figure 3. The TPP triangle [3]

The TPP triangle in the above figure [2, 2] covers the areas which are more prone to insider attacks and the attack vectors are to be determined with the emerging technologies. The attack vectors are determined based on survey conducted at various social media platforms like Facebook, Google, Twitter and many more. The user experience was recorded and how safe these platforms are is calculated on the basis of the response recorded by the users.

William T. Young, Alex Memory, Henry G. Goldberg, Ted E. Senator [4] have concluded in their research that the focus should be on building such a system that should point out the possible threats the even the builders of the existing system had never thought about. Their model is based on anomaly detection and is proved to be working well on different data set which here is called as ensemble. The ensemble has proved to be outstanding the existing

anomaly detection methods which are majorly based on known results.

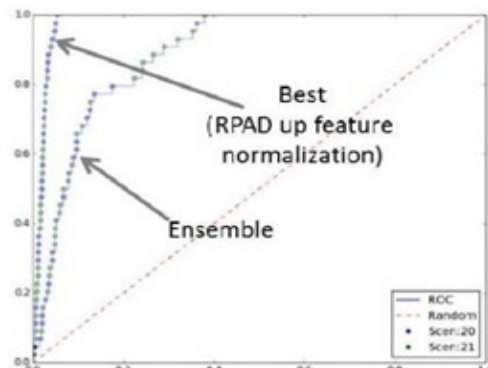


Figure 4. Performance graph of the model [4]

The above figure [4,3] gives us a clear understanding about the accuracy of the ensemble in detecting the anomaly, the methods used can be very useful in detecting the suspicious behavior among the employees of an organization.

4. Conclusion

Insider attacks have become a key issue in the field of security, thus our proposed system intends to make the decision making for granting access to the insider random and more complex so that the control is distributed over the organizational hierarchy.

5. Acknowledgment

It is a great honor to express our profound gratitude to our Computer Science & Engineering department, SRM Institute of Science and Technology, Kattankulathur, for encouraging and giving us support and good environment to gain valuable experiences.

References

- [1] Dipankar Dasgupta, Arunava Roy, Debasis Ghosh, Multi-user permission strategy to access sensitive information
- [2] F.L. Greitzer, L.J. Kangas, C.F. Noonan, A.C. Dalton, R.E. Hohimer, Identifying at-risk employees: modeling psychosocial precursors of potential insider threats, in: System Science (HICSS), 45th Hawaii International Conference on, 2012, pp. 2392–2401.
- [3] C. Armstrong, Mapping social media insider threat attack vectors. system sciences (HICSS), in: 46th Hawaii International Conference on, 2013, pp. 1840–1848.
- [4] W.T. Young, A. Memory, H.G. Goldberg, T.E. Senator, Detecting unknown insider threat scenarios, in: Security and Privacy Workshops (SPW), IEEE, 2014, pp. 277–288.
- [5] E.T. Axelrad, P.J. Sticha, O. Brdiczka, J. Shen, A Bayesian network model for predicting insider threats. Security and Privacy Workshops (SPW), IEEE, 82–89. 48 D. Dasgupta et al. / Information Sciences 423 (2018) 24–49.
- [6] CERT Insider Threat Team, Unintentional Insider Threats: A Foundational Study, Software Engineering Institute, 2013 May.
- [7] M.D. Guido, M.W. Brooks, Insider threat program best practices, in: System Sciences (HICSS), 46th Hawaii International Conference on, 2013, pp. 1831–1839.
- [8] M. Kandias, A. Mylonas, N. Virvilis, M. Theoharidou, D. Gritzalis, An insider threat prediction model, in: Trust, Privacy and Security in Digital Business, 2010, p. 6264.
- [9] Mishra, Mayank, et al. "Dynamic resource management using virtual machine migrations." IEEE Communications Magazine 50.9 (2012).
- [10] M. A. Tawfeek, A. El-Sisi, A. E. Keshk and F. A. Torkey, "Cloud task scheduling based on ant colony optimization," 2013 8th International Conference on Computer Engineering & Systems (ICCES), Cairo, 2013, pp. 64–69.
- [11] J. Oueis, E. C. Strinati and S. Barbarossa, "The Fog Balancing: Load Distribution for Small Cell Cloud Computing," 2015 IEEE 81st Vehicular Technology Conference (VTC Spring), Glasgow, 2015, pp. 1–6.
- [12] Huang, Dijiang, and Huijun Wu. Mobile Cloud Computing: Foundations and Service Models. Morgan Kaufmann, 2017.
- [13] Li, Kun, et al. "Cloud task scheduling based on load balancing ant colony optimization." Chinagrid Conference (ChinaGrid), 2011 Sixth Annual. IEEE, 2011.
- [14] T. Padmapriya and V. Saminadan, "Inter-cell Load Balancing technique for multi-class traffic in MIMO-LTE-A Networks", International Journal of Electrical, Electronics and Data Communication (IJEEDC), ISSN: 2320- 2084, vol.3, no.8, pp. 22–26, Aug 2015.
- [15] S.V.Manikanthan & K.srividhya "An Android based secure access control using ARM and cloud computing", Published in: Electronics and Communication Systems (ICECS), 2015 2nd International Conference on 26–27 Feb. 2015, Publisher:IEEE,DOI:10.1109/ECS.2015.7124833.

