Pattern Discovery for Insider Threat Detection

Ratnik Gandhi, Mehul S. Raval and Sanjay Chaudhary
{ratnik.gandhi, mehul.raval, sanjay.chaudhary}@ahduni.edu.in
School of Engineering and Applied Science, Ahmedabad University.

One of the central problems in cyber security is identification of an adversary. With the advent of internet technologies remote access of resources have skyrocketed. In this changing scenario it is difficult to identify and prevent access by unauthorized users. In fact, there are many examples of attacks on individuals and organizations planted from remote locations using the Internet [1]. These attacks are known to cause significant monetary losses and have caused harm to repute and privacy of organizations [1, 2].

Insider Threat

Attacks which remain hidden for a long time cause significant damage to institutions. Recent reports suggest some of these attacks can manipulate a country's general election or a referendum [3]. At the level of an organization such attacks can influence outcomes of tender processes.

Most organizations' security focus is on defense against outside attacks. On the other hand they have limited focus on people with rightful access to resources and systems but having malign intentions to harm other people, system, data, organization and business from within.

At times, it is possible that due to lack of information about organizational policies some activities of non-malicious users might be reported as activities of a malicious user [4]. This can happen with naïve or careless users. A different category of users are those who on purpose ignore security guidelines. This article focuses on the users of latter category i.e., malicious and willful insider. Further, the discussion is primarily focused on security related to IT resources in an organization. Formally, an insider and insider threat is defined as follows [4,5]:

- **An Insider:** A person with authorized accesses to resources and data of an organization.
- **Insider threat:** Actions by an insider that causes losses or harm to organizations or individual working in them.

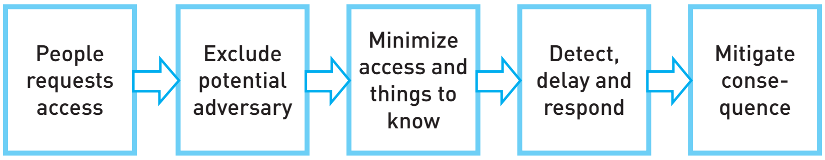
People requests access
Exclude potential adversary
Minimize access and things to know
Detect, delay and respond
Mitigate conse-quence

Fig. 1 : Sequential defense approach to insider threat [12].

Effects of Insider attacks

The Yahoo! reported breach of 1.5 billion user account in 2016. Of all the global data breaches a 25% of the data breach is due to inside actors [6]. These data breaches cost millions of dollars in revenue or monetary losses to organizations. A comprehensive list of 24 such attacks is reported in [7]. There are also reported instances of stealing millions of data records from credit card, insurance and health care companies by an insider [8]. It has been observed that 40% of these cyber-incidents are caused by insiders [9]. The CERT [10] maintains summary of various reports with more than 1000 cases of insider attacks. It also suggests practices to detect and prevent some of these insider threats. Insider threats have highest impact on public healthcare and finance organizations [6]. A malicious user can also sabotage IT system and can steal intellectual properties (IPs) for personal gains or to cause financial losses to organizations and individuals.

Mechanisms for Protection

For understanding nature of possible threats, system vulnerabilities and attacks, consequences must be well studied. Some of the research goals in this area must be directed towards effective detection, prevention, mitigation, punishment, and remediation methods. Some of the commonly employed protective mechanisms employed by organizations are [11]:

- Monitoring and auditing user activities.
- Screening of employee for security.
- Deployment and execution of relevant organizational policies.
- Security mechanisms for protecting material, device control and counter intelligence.
- User training for identifying risks and how to take counter measures.

Machine Learning Approaches

Identifying malicious user activities, due to absence of sufficient data, are a difficult problem to handle using machine learning [13]. One of the known public dataset in this area is by CERT [14]. The dataset has been created by synthetically generating malicious activities based on the knowledge of attacks in past.

Considering the analysis of user behavior, [13] develops a framework (BAIT-Behavior Analysis of Insider Threat) for identifying insider threat. They observe that a malicious user is likely to be more active and fetches more data. For classifying an honest or normal user from a malicious user they propose algorithms using Support Vector Machine (SVM) and Multinomial Naive Bayes classifiers.

In a different approach [15] presents a prediction tool for insider threat on file and directory resources. Results in [16] present security architecture for insider threat detection. It is worth noting that in contemporary scenario isolated strategies for mitigating insider threat are bound to fail and thus a more comprehensive approach is required [17]. Results in [18] combine some of the above methods and with the help of psychology and Bayesian nets identify insider threat. The article also discusses twelve behavioral signals for detecting insider threat. Further, the article uses

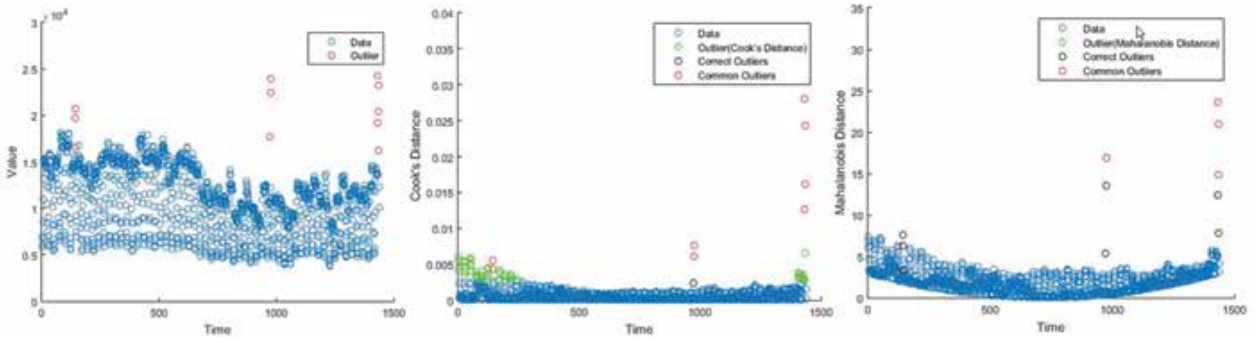

Fig. 2a : Yahoo Time series Benchmark Dataset with marked data and anomaly points; 2b. Cook's distance and Mahalanobis distance of Data in; 2c. Outliers -True and False positive (green), Benchmark positive(Black) and Both positive(Red)

Artificial Neural Network (ANN) along with these signals for identifying insider threat.

With the availability of user activity data at various levels of an operating systems (OS), [19] proposes an external threat model for detecting insider attack. Their method makes use of supervised anomaly identification with frequency parameters like *n*-grams and histograms of user activities. The results in [20, 21] considers insider threat detection in access control scenario. The method presented in [21] uses rules and density estimation for identifying anomalies. They use ranking for categorizing the threats.

For mitigating insider threat monitoring an organization's user activities such as network access, login-logoff and device inserted/removed (some other activities being super user account access; sensitive data accesses; excessive database access; repeated failed logins; user login through alternate accounts) is useful. But these activities produce significantly varied data in high volumes. Designing rule based analytics or human analytics of such actives is thus impractical. Machine learning based approaches can help and scale these analytical capabilities. Benefit of machine learning based approaches is that the deployed algorithms do not require modeling of insider threat behavior explicitly. The work in [22] detects intrusion with the help of a single layer neural network model. More advance results use recurrent neural networks (RNN) and train using Unix commands for predicting intrusion [23]. On the other hand results in [24] use autoencoders for learning in online scenario.

Simple Case Study

There have been studies characterizing user activity data as time series logs and algorithms for anomaly identification [25-29]. Let us consider an example in which network traffic of a server is used to identify Denial of Services (DoS) attack. These presented algorithms for anomaly detection will then model the traffic profile using parameters such as IP packages, new connections requests and can identify abnormal activities by considering data models. Figure 2 shows results of one such anomaly identification algorithm on Yahoo's time series benchmark data [30]. The model considered is linear regression (unsupervised machine learning) and then for identifying anomalies the algorithm uses Cook's and Mahalanobis distances [31].

The experiments clearly give comparative analysis of two statistical measures on benchmark time series data. The methods presented have some false positive and false negative rates. In this scenario we should consider Machine Learning algorithms as an important primary filter for rejecting obvious true positive and true negative cases. We must also deploy separate methods or human analytics on the false positive and false negative data to further classify them correctly and identify/prevent malicious user activities.

Conclusion and Research Avenues

In this article we discussed the threat caused by a malicious insider. We also discussed machine learning approaches to identify some of the malicious activities. It must be noted that the volume of data for malicious users activities is insignificant. It is known that the machine learning algorithms are sensitive to volume of data and hidden trends inside them. In this scenario the choice of a machine learning model must be done with care. The machine learning algorithms automate the process of insider threat detection and scales well with volume of data. These algorithms are independent of data and consider only the choice of feature within data.

As potential research avenues, methods based on analysis of psychological parameters of individuals in conjugation with machine learning algorithms to assess threat are promising. It would also be relevant to provide rigorous test results of such combined methods in practice. Another interesting research avenue is to consider the applications of deep learning methods to natural language processing, behavioral analysis and sentiment analysis [32]. Further, as the activities of malicious users have temporal correlations it would be interesting to study the problem of insider threat detection using a deep learning architecture called Long Short Term Memory (LSTM) which can help find this temporal correlations [33].

References

[1] https://en.wikipedia.org/wiki/List_of_cyberattacks

[2] https://www.gemalto.com/press/Pages/Gemalto-releases-findings-of-2016-Breach-Level-Index.aspx

[3] https://www.dni.gov/files/documents/ICA_2017_01.pdf

[4] Predd, Joel, Shari Lawrence Pfleeger, Jeffrey Hunker, and Carla Bulford. "Insiders behaving badly." *IEEE Security & Privacy* 6, no. 4, pp.66-70, 2008.

[5] Collins. Matthew, Theis. Michael, Trzeciak. Randall, Strozer. Jeremy, Clark. Jason, Costa. Daniel, Cassidy.

Tracy, Albrethsen. Michael, and Moore. Andrew, "Common Sense Guide to Mitigating Insider Threats, 5th Edition," Software Engineering Institute, Carnegie Mellon University, Pittsburgh, Pennsylvania, Technical Report CMU/SEI-2016-TR-015, 2016.

[6] 2017 data breach investigations report executive summary, http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/

[7] Chris King, "Spotlight On: Malicious Insiders and Organized Crime Activity", Technical note, CMU/SEI-2012-TN-001, Jan. 2012.

[8] G. Fyffe, "Addressing insider threat," Network Security, vol. 2008, no.3, pp. 11-14, 2008.

[9] S. L. Pfleeger and S. J. Stolfo, "Addressing the insider threat," IEEE Security & Privacy, vol. 7, no. 6, pp. 10–13, 2009.

[10] E. Cole and S. Ring, Insider Threat: Protecting the Enterprise from Sabotage, Spying, and Theft: Protecting the Enterprise from Sabotage, Spying, and Theft. Syngress, 2005.

[11] Duran, Felicia, Stephen H. Conrad, Gregory N. Conrad, David P. Duggan, and Edward Bruce Held. "Building a system for insider security." IEEE Security & Privacy 7, no. 6, pp. 30-38, 2009.

[12] "Insider Analysis", Module 23, The 19th International training course, SAND2006-1987C, Sandia National laboratories, 2006, pp. 214-287.

[13] A. Azaria, A. Richardson, S. Kraus and V. S. Subrahmanian, "Behavioral Analysis of Insider Threat: A Survey and Bootstrapped Prediction in Imbalanced Data," in *IEEE Transactions on Computational Social Systems*, vol. 1, no. 2, pp. 135-155, June 2014.

[14] https://www.cert.org/insider-threat/tools/

[15] G. Magklaras and S. Furnell, "Insider threat prediction tool: Evaluating the probability of it misuse," Computers & Security, vol. 21, no. 1, pp. 62–73, 2001.

[16] G. Jabbour and D. A. Menasce, "The insider threat security architecture: a framework for an integrated, inseparable, and uninterrupted self-protection mechanism," in Computational Science and Engineering, 2009. CSE'09. International Conference on, vol. 3. IEEE, 2009, pp. 244–251.

[17] J. Hunker and C. W. Probst, "Insiders and insider threats an overview of definitions and mitigation techniques," Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, vol. 2, no. 1, pp. 4–27, 2011.

[18] L. Greitzer and D. A. Frincke, "Combining traditional cyber security audit data with psychosocial data: towards predictive modeling for insider threat mitigation," in Insider Threats in Cyber Security. Springer, 2010, pp. 85–113.

[19] A. Liu, C. Martin, T. Hetherington, and S. Matzner, "A comparison of system call feature representations for insider threat detection," in Information Assurance Workshop, 2005. IAW'05. Proceedings from the Sixth Annual IEEE SMC. IEEE, 2005, pp.340–347.

[20] S. Sinclair and S. W. Smith,"Preventative directions for insider threat mitigation via access control," in Insider Attack and Cyber Security. Springer, 2008, pp. 165–194.

[21] M. A. Maloof and G. D. Stephens, "ELICIT: A system for detecting insiders who violate need-to-know," in Recent Advances in Intrusion Detection. Springer, 2007, pp. 146–166.

[22] Ryan, Jake, Meng-Jang Lin, and Risto Miikkulainen. "Intrusion detection with neural networks." In Advances in neural information processing systems, pp. 943-949. 1998.

[23] Debar, Herve, Monique Becker, and Didier Siboni. "A neural network component for an intrusion detection system." In Research in Security and Privacy, 1992. Proceedings., 1992 IEEE Computer Society Symposium on, pp. 240-250. IEEE, 1992.

[24] Veeramachaneni, Kalyan, Ignacio Arnaldo, Vamsi Korrapati, Constantinos Bassias, and Ke Li. "AI$^{2:}$ training a big data machine to defend." In Big Data Security on Cloud (Big Data Security), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS), 2016 IEEE 2nd International Conference on, pp. 49-54. IEEE, 2016.

[25] Nousiainen, Sami, Jorma Kilpi, Paula Silvonen, and Mikko Hiirsalmi. Anomaly detection from server log data. Technical report, 2009.

[26] Rodriguez, Aitor, and Mario de los Mozos. "Improving network security through traffic log anomaly detection using time series analysis." Computational Intelligence in Security for Information Systems 2010 (2010): 125-133.

[27] Zhu, Xia. Resilient control and intrusion detection for scada systems. University of California, Berkeley, 2011.

[28] Andrysiak, Tomasz, Łukasz Saganowski, Michał Choraś, and Rafał Kozik. "Network traffic prediction and anomaly detection based on ARFIMA model." In International Joint Conference SOCO'14-CISIS'14-ICEUTE'14, pp. 545-554. Springer, Cham, 2014.

[29] Model, ARIMA-GARCH. "Detection of Network Attacks Using Hybrid." In Dependability Problems and Complex Systems: Proceedings of the Twelfth International Conference on Dependability and Complex Systems DepCoS-RELCOMEX. July 2-6, 2017, Brunów, Poland, vol. 582, p. 1. Springer, 2017.

[30] https://webscope.sandbox.yahoo.com/catalog.php?datatype=s&did=70.

[31] Chatterjee, Samprit, and Ali S. Hadi. *Sensitivity analysis in linear regression*. Vol. 327. John Wiley & Sons, 2009.

[32] Majumder, Navonil, Soujanya Poria, Alexander Gelbukh, and Erik Cambria, "Deep Learning-Based Document Modeling for Personality Detection from Text." IEEE Intelligent Systems 32.2 (2017): 74-79.

[33] Gers, Felix A., Jürgen Schmidhuber, and Fred Cummins. "Learning to forget: Continual prediction with LSTM." (1999): 850-855.

■

About the Authors

Dr. Ratnik Gandhi is an Assistant Professor with School of Engineering and Applied Science, Ahmedabad University. Before joining Ahmedabad University he was a postdoctoral fellow with Tel Aviv University, Israel and Tata Institute of Fundamental Research (TIFR), Mumbai. He obtained his PhD and MTech in Information and Communication Technology from Dhirubhai Ambani Institute (DA-IICT), Gandhinagar, in 2011 and 2005 respectively, and his BE in Computer Engineering from Dharamsinh Desai University, Nadiad, in 2002. His research interests are Streaming Algorithms and Algorithmic Game Theory.

Dr. Mehul S Raval currently serves as an Associate Professor at Ahmedabad University. He is an alumnus of College of Engineering Pune. He has research interests in machine learning, pattern recognition, computer vision and image processing. He is a senior member of CSI and a distinguished speaker for Region III of CSI.

Dr. Sanjay Chaudhary is a Prof. and Asso. Dean at School of Engg. and Applied Science, Ahmedabad University. Earlier, he worked as a Professor and Dean (Academic Programs) at Dhirubhai Ambani Inst. of Information and Communication Technology (DA-IICT), Gandhinagar, India. His research areas are Distributed Computing, Cloud Computing, Data Analytics, and ICT Applications in Agriculture and Rural Development.