International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-3 Issue-2, December 2013

An Overview of Database Centred Intrusion Detection Systems

Ajayi Adebowale, Idowu S.A, Otusile Oluwabukola

Abstract*— Intrusion detection systems have become a major component of network security infrastructures. Modern day intrusion detection systems are to be reliable, extensible, adaptive to the flow of network traffic and to have a low cost of maintenance. Over the years researchers have looked upon data mining as a means of enhancing the adaptability of an intrusion detection system, as it enables the IDS to discover patterns of intrusions and define valid bounds of network traffic. Despite the effectiveness of data mining based IDS it is riddled with challenges; instrumenting components such as data transformations, model deployment, and cooperative distributed detection remain a labor intensive and complex engineering endeavor. This has lead to research efforts into integrating this technology with traditional database systems. This paper gives an overview of database centered intrusion detection systems.

Keywords: Database systems, Data mining, Intrusion detection systems, Network security.

I. INTRODUCTION

The threat and actuality of intrusion is real and the current dependence on networked systems makes it imperative for organizations to effect security strategies to help combat intrusions efficiently and effectively. Intrusions are defined as attempts aimed at compromising the integrity, confidentiality and availability of network resources. Intrusions could come from attackers accessing the systems from the Internet, authorized users of the systems who attempt to gain additional privileges for which they are not authorized, and authorized users who misuse the privileges given them. An intrusion detection system (IDS) monitors networked devices and looks for anomalous or malicious behavior in the patterns of activity in the audit stream.

II. CATEGORIES OF INTRUSION DETECTION SYSTEMS

Intrusion detection systems are categorized based on their source of data collection and on the strategy employed in detecting intrusions. Based on the source of audit data, IDS are either host based or network based. While from the strategy perspective, IDS are either misuse based or anomaly based. In host based IDS's, sensors are placed on every host on a network. These sensors monitor the hosts individually for signs of intrusion and raise alerts accordingly. This method is quite expensive and is more effective than network based IDS. Network based IDS has its sensors placed between the internet service provider and the clients or a gateway router.

It is from this position that the sensors collects network traffic data and analyses it for signs of intrusions. Misuse based IDS stores the signatures of known exploits and matches it with collected network traffic. An alarm is raised when a network connection or a series of network connections match the signature of a known exploit. A shortcoming of this approach is that it cannot detect previously unknown attacks. Anomaly detection IDS on the other hand tries to establish a profile for normal network activity and flags any deviation from this normal profile as an intrusion. The problem with this method is the occurrence of false positives as previously unseen normal network behaviour is flagged as an intrusion since it does not fit into the established profile.

III. DATABASE INTRUSION DETECTION SYSTEMS

Database Management Systems (DBMS) represent the ultimate layer in preventing malicious data access or corruption and implement several security mechanisms to protect data [7]. Traditional commercial implementations of database security mechanisms are very limited in defending successful data attacks. These traditional database protection techniques like authorization, access control mechanisms, inference control, multi-level secure databases, multi-level secure transactions processing, database encryption among others mainly address how to protect the security of a database, especially its confidentiality. However, in practice, these techniques may be fooled by knowledgeable attackers who thwart the security mechanisms and gain access to sensitive data. On the other hand, authorized but malicious transactions can make a database useless by impairing its integrity and availability [12].

Neither network-based nor host-based IDSs can detect malicious behavior from users at the database level, or more generally, the application level, because they do not work at the application layer [11]. Nevertheless, existing host-based intrusion detection systems use the operating system log or the application log to detect misuse or anomaly activities. These methods are not sufficient for detecting intrusion in database systems [9]. The inability of host-based intrusion detection in database intrusion detection can be attributed to the fact that users who seek to gain database privileges will likely be invisible at the operating systems level, and thus be invisible to the host-based intrusion detectors. Therefore, SQL injection [18] and other SQL-based attacks targeted at databases cannot be effectively detected by network-based or host-based IDSs [11].

Manuscript published on 30 December 2013.
***** Correspondence Author (s)

Ajayi Adebowale*, Computer Science Department, Babcock University Ilishan Remo, Ogun state, Nigeria.

Idowu S.A, Computer Science Department, Babcock University Ilishan Remo, Ogun state, Nigeria.

Otusile Oluwabukola, Computer Science Department, Babcock University Ilishan Remo, Ogun state, Nigeria.

Database IDSs try to detect or possibly prevent the intrusions to RDBMSs which mainly is accomplished by malicious transactions either by outsiders or insiders like disgruntled employees who misuse their privileges; as nowadays the greatest threats are from internal sources; which means the perimeter-based security solutions may not be enough. Additionally, most organisations solely implement network-based security solutions that are designed to protect network resources; despite the fact that the information is more often the target of the attack. Database intrusion detection systems identify suspicious, abnormal or downright malicious accesses to the database system [17]. Given the data-centric nature of the intrusion detection process [15], leveraging existing RDBMS infrastructure for intrusion detection can be both efficient and effective.

IV. DATA MINING IN DATABASE INTRUSION DETECTION SYSTEMS

An important application of Data Mining techniques in database intrusion detection system is discovering the data dependencies among data-items in the database. In [10], data dependency is defined as the data access correlations between two or more data items. The techniques employed use Data Mining approach to generate data dependencies among data items. These dependencies generated are in the form of classification rules, i.e., before one data item is updated in the database what other data items probably need to be read and after this data item is updated what other data items are most likely to be updated by the same transaction. Transactions that are not compliant to the data dependencies generated are flagged as anomalous transactions [10].

In [9] also, the identification of malicious database transaction is accomplished by using data dependency relationships. Typically before a data item is updated in the database some other data items are read or written. And after the update other data items may also be written. These data items read or written in the course of updating one data item construct the read set, pre-write set, and the post-write set for this data item. The proposed method identifies malicious transactions by comparing these sets with data items read or written in user transactions [9].

In [10], the author has come up with a comparison between existing approach for modeling database behavior [1] and transaction characteristics [5, 13] to detect malicious database transactions. The advantage of their approach is that it is less sensitive to the change of user behaviors and database transactions. It is observed from real-world database applications that although transaction program changes often, the whole database structure and essential data correlations rarely change.

Figure 1 shows a Database-centric Architecture for Intrusion Detection (DAID) proposed for the Oracle Database. This RDBMS-centric framework can be used to build, manage, deploy, score, and analyze Data Mining-based intrusion detection models [2].

In [21] and subsequently [22] an elementary transaction-level user profiles mining algorithm is proposed which is based on user query frequent item-sets with item constraints.

Srivastava, A., et al. in [19] and [20] propose an intrusion detection algorithm named weighted data dependency rule miner (WDDRM) for finding dependencies among the data items. The main idea is that in every database, there are a few attributes or columns that are more important to be tracked or sensed for malicious modifications as compared to the other attributes. The algorithm takes the sensitivity of the attributes into consideration. Sensitivity of an attribute signifies how important the attribute is for tracking against malicious modifications.

V. DATABASE CENTRIC ARCHITECTURE

(Campos & Milenova, 2005) presented how to create and deploy data mining-based Intrusion Detection Systems in Oracle Database 10g

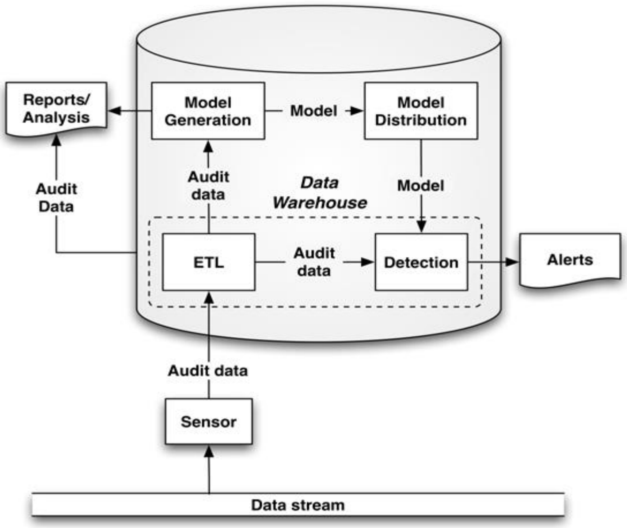

Figure1. Database centric architecture for intrusion detection

In DAID (Figure 1), all major operations take place in the database itself. DAID also explicitly addresses data transformations, an essential component in analytics. DAID has the following major components:

- Sensors
- Extraction, transformation and load (ETL)
- Centralized data warehousing
- Automated model generation
- Automated model distribution
- Real-time and offline detection
- Report and analysis
- Automated alerts

The activity in a computer network is monitored by an array of sensors producing a stream of audit data. The audit data are processed and loaded in a centralized data repository (ETL). The stored data are used for model generation. The model generation data mining methods are integrated in the database infrastructure – no data movement is required. The generated intrusion detection models can undergo scheduled distribution and deployment across different database instances. These models monitor the incoming audit data. The database issues alerts when suspicious activity is detected. The models and the stored audit data can be also further investigated using database reporting and analysis tools.

The key aspect to the described data flow is that processing is entirely contained within the database. With the exception of the sensor array, all other components can be found in modern RDBMSs.

VI. CONCLUSION

This paper presented an overview of database centered intrusion detection systems. The advent of the big data paradigm has led to investigations into database-centric platforms for building information fusion applications. These platforms offers many advantages which includes: tight integration of individual components, security, scalability, and high availability. Current trends in RDBMSs are moving towards providing all key components for delivering comprehensive state-of-the-art information fusion applications. By leveraging an existing RDBMS-based technology stack, a full-fledged information fusion application like a data mining based intrusion detection system can be developed in a reasonably short time and at a low development cost.

REFERENCES

[1] D. Barbara, R. Goel, and S. Jajodia, Mining malicious data corruption with hidden markov models. in Research Directions in Data and Applications Security, 2002.
[2] M. Campos and B. Milenova, Creation and Deployment of Data Mining-Based Intrusion Detection Systems in Oracle Database 10g. 2005
[3] D. Carter and A. Katz, Computer Crime: An Emerging Challenge for Law Enforcement. FBI Law Enforcement Bulletin, 1997: p. 1-8.
[4] C. Chung, M. Gertz, and K. Levitt, DEMIDS: A Misuse Detection System for Database Systems. In Third Annual IFIP TC-11 WG 11.5 Working Conference on Integrity and Internal Control in Information Systems, 1999.
[5] C. Chung, M. Gertz, and K. Levitt, Misuse Detection in Database Systems Through User Profiling.
[6] B. Elisa, et al., Intrusion Detection in RBAC-administered Databases, in Proceedings of the 21st Annual Computer Security Applications Conference. 2005, IEEE Computer Society.
[7] J. Fonseca, M. Vieira and H. Madeira, Monitoring Database Application Behavior for Intrusion Detection. 12th Pacific Rim International Symposium on Dependable Computing, 2006.
[8] A. Honig, A. Howard, E. Eskin and S. Stolfo, Adaptive Model Generation, an Architecture for the Deployment of Data Mining-Based Intrusion Detection Systems, In D. Barbarà and S. Jajodia (eds.), Applications of Data Mining in Computer Security, Kluwer Academic Publishers, Boston, MA, 2002, pp. 154-191.
[9] Y. Hu and B. Panda, A Data Mining Approach for Database Intrusion Detection. ACM Symposium on Applied Computing, 2004.
[10] Y. Hu, and B. Panda, Identification of Malicious Transactions in Database Systems. Proceedings of the Seventh International Database Engineering and Applications Symposium (IDEAS'03), 2003.
[11] X. Jin and S. Osborn, Architecture for Data Collection in Database Intrusion Detection Systems. 2007.
[12] W. Lee and S. Stolfo, A Framework for Constructing Features and Models for Intrusion Detection Systems, ACM Transactions on Information and System Security, 3(4), 2000, pp. 227-261.
[13] V. Lee, J. Stankovic and S. Son, Intrusion Detection in Real-time Database Systems Via Time Signatures. In Proceedings of the Sixth IEEE Real Time Technology and Applications Symposium, 2000.
[14] W. Low, J. Lee, and P. Teoh: detecting intrusions in databases through fingerprinting transactions.
[15] U. MATTSSON, A Practical Implementation of a Real-time Intrusion Prevention System for Commercial Enterprise Databases.
[16] P. Ramasubramanian, and A. Kannan, Intelligent Multi-agent Based Database Hybrid Intrusion Prevention System. 2004.
[17] F. Rietta, Application Layer Intrusion Detection for SQL Injection. ACM Symposium on Applied Computing, 2006
[18] A. Spalka, And J. Lehnhardt, A Comprehensive Approach to Anomaly Detection in Relational Databases. 2005.
[19] A. Srivastava, S. Sural, and A. Majumdar, Weighted Intra-transactional Rule Mining for Database Intrusion Detection. 2006.
[20] A. Srivastava, S. Sural, and A. Majumdar, Database Intrusion Detection using Weighted Sequence Mining. JOURNAL OF COMPUTERS, 2006. 1(4).
[21] Y. Zhong, and X. Qin, Database Intrusion Detection Based on User Query Frequent Itemsets Mining with Item Constraints. Conference InfoSecu04, 2004.
[22] Y. ZHONG, and X. QIN, Research On Algorithm Of User Query Frequent Itemsets Mining. Proceedings of the Third International Conference on Machine Learning and Cybemetics, Shanghai, 2004.

Ajayi Adebowale holds a B.Sc. degree in Mathematics (Computer Science) and an M.Sc degree in Computer science from University of Agriculture Abeokuta, Nigeria and Babcock University, Nigeria respectively. He is currently working on his Phd at Babcock University and his research interests include Knowledge discovery in databases, Machine learning and Information security. He can be contacted at deboxyl@gmail.com

Sunday Idowu PhD is a Professor of computer science in the School of Computing and Engineering Babcock University, Ilishan-Remo, Ogun State, Nigeria. He holds a Masters degree in Software Engineering, and PhD in computer science from Andrews University, MI, USA and University of Ibadan, Oyo State, Nigeria, respectively. His research areas are Software Engineering, Web Application Development and Security. He has published works in several journals of international repute. He can be contacted at saidowu07@gmail.com

Otusile Oluwabukola Received a B.Sc and M.Sc degree in Computer Technology from Babcock University and she is currently working on her PhD in Computer science. Her current research interests include Network Management, and Information Systems Security. She can be contacted at buhkieotusile@yahoo.com