Review of WiFi Miner Intrusion detection system

Kalyani Tukaram Bhandwalkar [1]

[1] *Assistant professor, Computer Engineering, PREC,Loni, Ahmednagar, Maharashtra, India*

---***---

Abstract - *The traditional prevention techniques such as user authentication, data encryption, avoiding programming errors and firewalls basically form the first line of defense for computer security. These systems propose a security vulnerability evaluation. However, intruders have their way in these vulnerabilities and bypass the preventive security tools. Thus there is a need for second level of defense which is constituted by tools such intrusion detection system (IDS). In network security, Intrusion Detection System plays a reasonable supplementary role for the firewall. It improves the security and reliability of the computer and helps protect computers from network attacks. Here some of the pattern mining algorithms of current Intrusion Detection System are discussed. Intrusion detection in wireless networks has become a vital part in wireless network security systems .Currently, almost all devices are Wi-Fi capable and can access WLAN. Here an Intrusion Detection System, WiFi Miner is discussed.*

Key Words: *WiFi Miner, Intrusion detection system, Anomaly detection systems, Misuse detection systems*

1. INTRODUCTION

Now days the network has expanded to very large scales and the data exchange between the networks and the tremendously amount of the network traffic is expanded all over the world. On the other hand, very large numbers of computers stay connected to Internet. These computers store very important data such as emails, documents, pictures and videos. The computers have become a favorite target for attacks that requiring more complex analysis to detect it, this is due to the growth of the Internet users exchanging the user data. The Intrusion Detection System (IDS) becomes an important part of any modern network as it ensures the security issue of information systems.

The timely accurate detection of intrusion has always been an exclusive goal for information security researchers. Intrusion detection system is the system that monitor the events occurring in a computer system or network by analyzing them for signs of possible incidentss of violation of computer security policies.

Intrusions attempts to compromise the confidentiality, integrity, availability, or to bypass the security mechanisms of a computer system or network. Intrusions have many causes, such as attackers gaining unauthorized access to systems from the Internet, and authorized users of systems who misuse their privileges or attempt to gain additional privileges for which they are not authorized etc. The primary responsibility of an ID is to detect unwanted and malicious activities.

Types of IDS

Intrusion detection system can be broadly classified based on its analysis method is as shown in figure 1.

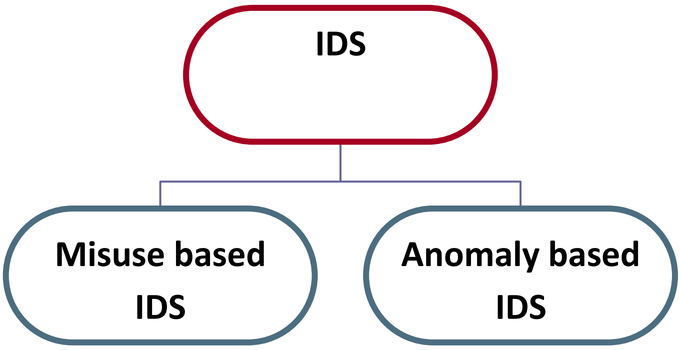

Fig .1 Types of IDS

1.1 Misuse Detection

An IDS can use signature-based detection, relying on known traffic data to analyze potentially unwanted traffic [19]. They work by looking for a specific signature on a system. Identification engines perform well by monitoring these patterns of known misuse of system resources. They perform a pattern matching between network traffic captured and attack signature. If the matching succeeds, then the system generates an alarm and attack signature. If the matching succeeds, then the system generates an alarm. The main advantage of signature detection paradigm is that it can accurately and efficiently detect instances of known attacks. The main disadvantage is that it cannot detect the newly invented attacks.

Advantages:

- Misuse detectors are very effective at detecting attacks without generating an overwhelming number of false alarms.
- Misuse detectors can quickly and reliably diagnose the use of a specific attack tool or technique. This can help security managers prioritize corrective measures.
- Misuse detectors can allow system managers, regardless of their level of security expertise, to track security problems on their systems, initiating incident handling procedures.

Disadvantages:

- Misuse detectors can only detect those attacks they know about therefore they must be constantly updated with signatures of new attacks.
- Many misuse detectors are designed to use tightly defined signatures that prevent them from detecting variants of common attacks. State-based misuse detectors can overcome this limitation, but are not commonly used in commercial IDSs.

1.2 Anomaly detection

An IDS that looks at network traffic and detects data that is incorrect, not valid, or generally abnormal is called anomaly-based detection[19]. This paradigm takes the attitude that something that is abnormal is probably suspicious. The construction of such a detector starts by creating a model of what constitutes normal for the observed network, and then deciding on what percentage an activity must be flagged as abnormal. The main advantage of anomaly detection is that it does not require prior knowledge of intrusion and can thus detect new intrusions. The main disadvantage is that it may not be able to describe what an attack is and may have high false positive rate.

Advantages:

- IDSs based on anomaly detection detect unusual behavior and thus have the ability to detect symptoms of attacks without specific knowledge of details.
- Anomaly detectors can produce information that can in turn be used to define signatures for misuse detectors.
-

Disadvantages:

- Anomaly detection approaches usually produce a large number of false alarms due to the unpredictable behaviors of users and networks.
- Anomaly detection approaches often require extensive “training sets” of system event records in order to characterize normal behavior patterns.

2. LITRATURE REVIEW

There are various pattern mining algorithms which inspired many extensions and techniques for IDS. ADAM, MADAMID, MINDS, all these systems are designed for wired network environment. ADAM was one of the early researches that featured a system applying data mining techniques to the problem of network intrusion detection, using association rule mining Apriori algorithm[1]. One limitation of these systems is that some of them are currently off-line but a more effective intrusion detection system should be real time, to minimize chances of compromising network security. Another limitation in some models is that they compute only frequent patterns in connection records. However, many intrusions like those that embed all activities within a single connection do not have frequent patterns in connection data. These types of intrusions might go undetected in these models.

3. WIFI MINER IDS

The proposed WiFi Miner system framework comprises of three main modules. They are: Input Module, Preprocessor Module, and Anomaly Detection Module. [1]

3.1 Input Module: It consists of properly configured hardware sensors, collects network traffic data from hardware wireless sensors attached to the system, which capture data from airwaves as most of the wireless attacks may occur before data are in wired network and Access Points. [1]

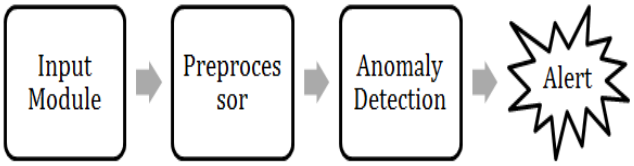

Fig.2 WiFi Miner IDS

3.2 The Preprocessor Module: It converts the raw data to readable format with the help of CommView for WiFi software, which is used to extract sensed data from the hardware sensor's firebird database and saved in a .csv file (csv stands for Comma Separated Values where attributes values are simple text separated by commas). With CommView, necessary features can be extracted for analyses to detect anomalies and extracted records stored as text file are processed directly by WiFi Miner system. These records may also be logged into database tables for more offline processing and possible tracking of anomalous records. The focus of our approach is online processing, that is independent of training data. After the data are preprocessed, they are sent to the Anomaly Detection Module.[1]

3.2 Anomaly Detection Module: The core algorithm (Online Apriori-Infrequent) for finding infrequent patterns or anomalies.Detail algorithm is given in [1].

4. CONCLUSIONS

WiFi Miner captures packets from wireless network through hardware sensors. There is real time detection of intrusive or anomalous packets. Proposed IDS uses Apriori-Infrequent based algorithm. The system is different from existing wireless intrusion systems, since it eliminates the need for hard-to- get training data and detects intrusions in real time. Also, like other existing wireless intrusion systems, it captures the packets from airwaves while wired IDSs use net-ow data from routers. Thus, the major contribution of the system is that it can detect anomalous packets in real time without any training phase with a reduced time complexity in comparison to traditional Apriori based systems.

REFERENCES

[1]Ahmedur Rahman, C.I. Ezeife, A.K. Aggarwal "WiFi Miner: An Online Apriori-Infrequent Based Wireless Intrusion Detection System"2012.

[2]R. Agrawal and R. Srikant. Fast algorithms for mining association rules in large databases. In Proceedings of the 20th International Conference on very Large Databases Santiago, Chile, pages 487–499, 1994.

[3] D. Barbara, J. Couto, S. Jadodia, and N. Wu. Adam: A testbed for exploring the use of data mining in intrusion detection. ACM SIGMOD RECORD: Special Selection on Data Mining for Intrusion Detection and Threat Analysis, 30(4), 2001.

[4]L. Ertoz, E. Eilertson, A. Lazarevic, P. Tan, J. Srivastava, V. Kumar, and P. Dokas. The MINDS - Minnesota Intrusion Detection System in Next Generation Data Mining, chapter 3. MINDs, 2004.

[5]J. Han and M. Kamber. Data Mining: Concepts and Techniques. Morgan Kaufmann Publishers, New York, 2000.

[6] J. Han, J. Pei, Y. Yin, and R. Mao. Mining frequent patterns without candidate generation: A frequent-pattern tree approach. International Journal of Data Mining and Knowledge Discovery, 8(1):53–87, Jan 2004.

[7]T. Imielinski, A. Swami, and R. Agarwal. Mining association rules between sets of items in large databases. In Proceedings of the ACM SIGMOD conference on management of data, pages 207 – 216. ACM, 1993.

[8]W. Lee and S. J. Stolfo. A framework for constructing features and models for intrusion detection systems. ACM Transaction on Information and System Security, 3(4):227–261, Nov. 2000.

[9]Q.-H. Li, J.-J. Xiong, and H.-B. Yang. An efficient algorithm for frequent pattern in intrusion detection. In Proceedings of the International Conference on Machine learning and cybernatics, pages 138–142, Nov. 2003.

[10]Y. Liu, Y. Li, H. Man, and W. Jiang. A hybrid data mining anomaly detection technique in ad hoc

networks. International Journal of Wireless and Mobile Computing, 2(1):37–46, 2007.

[11]V. Mahoney and P. K. Chan. Learning rules for anomaly detection of hostile network traffic. In Proceedings of the Third IEEE International Conference on Data Mining (ICDM), pages 601 – 604. IEEE, 2003.

[12] H. Mannila and H. Toivonen. Levelwise search and borders of theories in knowledge discovery. International Journal of Data Mining and Knowledge Discovery, 1(3):241–258, Jan 2004.

[13] V. Marinova-Boncheva. Applying a data mining method for intrusion detection. In ACM International Conference Proceeding Series. ACM, June 2007.

[14] R. J. Shimonski. Wireless attacks primer. A whitepaper published on windowssecurity.com section: Articles: Wireless security, July 2004.

[15]K. Yoshida. Entropy based intrusion detection. In Proceedings of the IEEE Pacific Rim Conference on Communications, Computers and Signal Processing, PACRIM, pages 28–30. IEEE, August 2003.

[16]H. Zhengbing, L. Zhitang, and W. Junqi. A novel intrusion detection system (nids) based on signature search of data mining. In 1st international conference on Forensic applications and techniques in telecommunications, information, and multimedia and workshop, January 2008.

[17]S. Zhong, T. Khoshgoftaar, and S. Nath. A clustering approach to wireless network intrusion detection. In Proceedings of the 17th IEEE International Conference on Tools with Artificial Intelligence (ICTAI), pages 190–196. IEEE, 2005.

[18] C.I. Ezeife,"WIDS: A Sensor-Based Online Mining Wireless Intrusion Detection System", ACM 978-1-60558-188-0/08/09

[19] B.Santos Kumar, T.Chandra Sekhara Phani Raju, M.Ratnakar, Sk.Dawood Baba, N.Sudhakar, ”Intrusion Detection System- Types and Prevention “,www.ijcsit.com