RESEARCH ARTICLE OPEN ACCESS

A Systematic Review on Intrusion Detection Systems for Mobile Devices

Bhavkanwal Kaur [1], Puspendra Kumar Pateriya [2]
School of Computer Science and Engineering
Lovely Professional University
Jalandhar-144402
India

ABSTRACT

In the recent years the use of mobile devices has increased drastically, so does the security concerns associated with it. To deal with the security threats to the mobile devices, many applications came into existence like firewall, Anti-virus. But in many cases these also fail to provide security in case of severe attack being done by an intruder. So more secure systems were introduced, which are known as Intrusion Detection Systems (IDS). In the beginning traditional IDSs were introduced which were in providing security to the devices which are static inside a particular network and do not change their networks but these IDSs failed to provide security to the mobile devices. So in order to provide security to the mobile devices, mobile Intrusion Detection Systems were introduced. In this paper we have surveyed the different existing mobile IDS and their advantages and limitations.

Keywords:- Intrusion Detection System, mobile IDS, traditional IDS

I. INTRODUCTION

Intrusion Detection System is the system which oversees the every packet passing through either a network or a particular device and checks for the intrusive patterns in it.[1] In the beginning we had only traditional IDS which were usually deployed at the gateway of a particular network to keep an eye on all the ingoing and the outgoing traffic. Every packet passing through it should satisfy the predefined pattern and if not, the packet is either dropped or blocked. IDS is mainly categorized into two types, Host based Intrusion Detection System(HIDS) and Network based Intrusion Detection System(NIDS). Host based IDS is installed on one particular host, means on one device only. It basically observe and supervise the insides of the data processing machine as well as the information packets present on its network interfaces. Network based Intrusion Detection System is distinct from HIDS as in NIDS it monitors the whole of network traffic which means that the traffic from all the devices a particular network. As like HIDS, it matches the new pattern of the traffic with the old one to detect anomalies. Whenever it finds an attack it, an alarm is generated. It also maintain log files and check patterns due to which the system is being compromised. IDS is not the solution to all security issues, there are many issues in which it fails to provide security. Consider that the network is very much congested, in that case IDS will not be able to keep a watch on all the network packets because of high traffic during congestion.IDS are generally constructed in two ways, Active and Passive. When an IDS just the sense the activity and maintains the log information about it , then it is a passive IDS but if along with doing all this, it also gives response to the attack done, then it is a active IDS.

The services provided by traditional IDS are not able to do detection for mobile devices. Nowadays, there are broad range of services provided by mobile devices over numerous network connections and is able to reserve a large amounts of private to professional data. So, these days use of mobile devices are at its peak. The usage can vary from exchanging pictures via blue-tooth to sharing a crucial information through mail exchange. Although mobile devices are most reliable for communication, they are most susceptible to attacks. The physically possible attacks that could be done on a mobile device is either someone can steal a mobile device or cloning of the SIM card. In software based attacks, Malware attacks like viruses, worms, key-loggers are the most common attacks on the mobile devices. In order to provide protection against such attacks various schemes were designed like anti-virus, biometrics, encryption and firewall. In the late 90s, there were techniques available to provide protection against traditional attacks only. Later, research extended to providing protection against battery based attacks, mobile agent based attacks. But these existing IDS were able to encounter only a single vulnerability like battery based IDS can only identify attacks done on the battery of the device.[2] So none of these devices were able to provide protection against multiple attacks.

In this paper, we present a brief discussion on mobile IDS, their distinct types, how they perform their task in doing detection, their pros and cons.

II. MOBILE IDS

The main features of a mobile device are: it is able to access different networks, low memory and lower processing power and distinct group of services. The existing IDS are not compatible with the mobile devices.[3] Network based IDS monitor the traffic of a particular network but a mobile device is the one which roam in different networks. In case of Host based IDS , they are too hard to be managed by mobile devices. The first attack ever happened on a mobile device was ”telephony service fraud” which occurred in 1995 .[4] This attack refers to theft of a mobile device or cloning of the SIM card. Then the attacker can enjoy all the services provided by the original SIM card. He can see all your SIM data and information like files, messages and can also make calls, use Internet but the all the bill has to be paid by the original user. Until the user does not get any notification, he is unaware of the fact that his card has been cloned.The major concern is this attack can be used by a criminal or an attacker to make a contact to its other parties without being traced.

By the time an improvement was made in the features of the mobile devices like increase in the processing power, as a result email services became feasible and large data files can be stored or exchanged but increase in facilities also increased the security threats to these mobile devices such as DOS attacks, information disclosure and malware attacks.

III. SIGNATURE BASED DETECTION IN MOBILE IDS

Signature based detection in mobile IDS is used to encounter malware or DOS attacks. The work in this field began in 2000. It si basically classified into two classes, mobile agent based mobile IDS and battery based mobile IDS.[5]

A. Mobile Agent Based Mobile IDS

This is generally developed for ubiquitous computing surroundings, means those surroundings in which we can have different types of mobile devices like smart phones, laptops, personal digital assistants and many more. The operation of this IDS is make the mobile agent to visit each and every mobile device in the network by traversing from one device to another and collect all mischievous activities from all devices. This IDS system is good for devices with low processing power. On the other hand determining a threat on a particular node in the network will contribute in protecting the whole of the network from a security attack. This scheme was proposed by Kannadiga in 2005.[6] But it has various limitations. In this signatures are created by performing malicious exercises on static nodes. So this is more suitable for a particular host than for a device which is dynamic in nature. Since mobile devices move from one node to another, it provides no more protection to the device when the device leaves a particular network. Thus it fails to provide protection against malware attacks.

Battery Based Mobile IDS

Battery is the lifeline of every electronic device and we need good battery power to keep the system working efficiently. Now if the system does not have much power to execute various processes on time, it may lead to loss of the information and can even cause the device to stop various services. And the attacker makes the use of this limitation. The attacker may perform an attack by draining the battery of the system as a result various services of the device may stop.

Generally, sleep deprivation attacks are performed on the battery of the device which leads to the exhaustion of the battery power.[7] Such attacks make battery of the device to get drained out faster than it what would be with the normal consumption. The attacker usually makes best efforts such that the battery do not get a chance to enter the power saving mode and make the battery to exhaust completely by keeping it busy. The attacker can use three strategies to do that:

1) Malignant power attacks
2) Benign power attacks
3) Service Request attacks

In malicious power attacks, the attacker makes the processor to consume more power than it’s actual consumption. In benign power attacks, the processor is made to execute a genuine or authenticated job but the job is of very high power consumption. Such tasks are given to the processor repeatedly, as a result the power of the battery drains out.

In service request attack, the victim is asked for providing services repeatedly over a network. Now even if device may not provide the services but still it will consume power in deciding whether to provide services or not.

To tackle, these attacks done on the battery, three proposals were made: Gibraltar, Battery Based Intrusion Detection Model and Power Secure Architecture. All of these have almost the same working principle. As we know that the consuming power of each device is different, so the pattern of attacks performed on each device will also be different.[8], [9] So on each of the device the patterns of battery consumption are recognized and signatures are constructed according to that. The signatures of every device would be different. Now, the IDS system constantly keep an eye on all the activities of the battery of the device and compares it with the signatures in order to detect the intrusions. However this is a good scheme to detect the malware attack but detection of a malware signature is not an easy task.

IV. BEHAVIOR BASED MOBILE IDS

There are many facilities being provided by the mobile devices but the way people use these facilities is quite different. Every service provided by the mobile device is used in a completely different way by every person, so the pattern of the attack made on any particular mobile device vary from person to person. Behavior based mobile IDSs are are mostly used for detecting telephony fraud, cloning of the SIM card or device being stolen or lost. Behavior based IDS are all network based because the performance of particular device is observed by the service providers of the network.

These are generally categorized into three groups:

1) Migration Itinerary Based Mobile IDS
2) Telephony Based Mobile IDS
3) Migration Mobility Based Mobile IDS

Migration Itinerary based mobile IDS is used to detect traditional attacks happening on the system when a system migrates from one network to another. This does not keep a check on the activity of the mobile device within a particular network rather it keeps a check on the device from the network cell, from where it started the journey to the end of the destination. So, basically it observes the patterns that the mobile device routes through the different networks and maintains a database of all the routes that the device takes. It checks the patterns and sees that which are the routes which are most commonly taken the person who owns the mobile device and which are the most favorite routes of that person. It stores these patterns as the valid routes taken by the person. Now, if the mobile device of the person got stolen then, the thief will take a completely different route and it is an attack detected by the IDS.[10] This scheme still have a lot of limitations like it is not able to detect any malware or attacks related to the data. It is not able to detect any attack if the person is walking who is carrying a mobile device. It only detects when the person is traveling in any vehicle.

IDS system which is made for detecting telephony based attack, checks the calling data of the user, both incoming and outing. It checks out the date of the call made, its start time and end time, the number on which the call is being made in order to detect any fraud, cloning of the SIM card or when the mobile device got stolen. By collecting all this information, certain records are maintained which contains the patterns of most called numbers , calling duration and timings. A particular threshold is maintained up to which a deviation from such patterns is acceptable. But if the deviation very much abrupt and is greater than the threshold then it is an attack. There are many type of telephony based mobile IDS, like Stormann, Notare, which are based on supervised learning while devices like Samfat and Molva are based on unsupervised learning. These are really a good IDS system because it generates very less false positives. But the major drawback is, it is only based on detecting telephony based attacks and provide no detection against any other type of network based attacks. Also they cannot detect malware or attacks related to the data. This IDS system is generally operated by the network service provider, so there is o responsibility of the mobile device.[11]

Since the mobile device travels from one network to another it is very much prone to the migration based attacks. Migration mobility based IDS was designed to provide attack detection services when a device migrates from one cell to another. Its is almost similar to the migration itinerary based mobile IDS.It also maintains a particular threshold, when a particular task crosses that threshold, it is an attack. Various mobility based IDS were developed which give the best performance, with almost 95 percent accuracy and 5 percent false positives. There is one such system mentioned in [12], which even keeps a check on the patterns of the user on the working days and weekends along with accuracy.But again, the major drawback is t only detects the attack when the user is traveling at the speed of at least 60 miles in one hour. If the person is on foot, then the attack pattern is undetectable. But it is very beneficial for the people who are regular travelers.

V. CONCLUSION AND FUTURE SCOPE

This paper is all about a small review on the types pf mobile IDS available. Here we discussed about the advantages and the limitations of the behavior and signature based mobile IDS.Currently available IDS are not able to provide detection over a wide range. We need devices which can detect patterns over larger area and were able to control malware or data related attacks.

REFERENCES

[1] H.-J. Liao, C.-H. R. Lin, Y.-C. Lin, and K.-Y. Tung, "Intrusion detection system: A comprehensive review," *Journal of Network and Computer Applications*, vol. 36, no. 1, pp. 16–24, 2013.

[2] D. C. Nash, T. L. Martin, D. S. Ha, and M. S. Hsiao, "Towards an intrusion detection system for battery exhaustion attacks on mo- bile computing devices," in *Pervasive Computing and Communications Workshops, 2005. PerCom 2005 Workshops. Third IEEE International Conference on*. IEEE, 2005, pp. 141–145.

[3] D. Michalopoulos and N. Clarke, "Intrusion detection system for mobile devices," *Advances in Networks, Computing and Communications 4*, p. 205.

[4] F. Li, N. Clarke, M. Papadaki, and P. Dowland, "Behaviour profiling on mobile devices," in *Emerging Security Technologies (EST), 2010 International Conference on*. IEEE, 2010, pp. 77–82.

[5] H. Wu, S. Schwab, and R. L. Peckham, "Signature based network intru- sion detection system and method," Sep. 9 2008, uS Patent 7,424,744.

[6] P. Kannadiga, M. Zulkernine, and S. I. Ahamed, "Towards an intrusion detection system for pervasive computing environments," in *Information Technology: Coding and Computing, 2005. ITCC 2005. International Conference on*, vol. 2. IEEE, 2005, pp. 277–282.

[7] T. Martin, M. Hsiao, D. Ha, and J. Krishnaswami, "Denial-of-service attacks on battery-powered mobile computers," in *Pervasive Computing and Communications, 2004. PerCom 2004. Proceedings of the Second IEEE Annual Conference on*. IEEE, 2004, pp. 309–318.

[8] G. A. Jacoby, T. Hickman, S. P. Warders, B. Griffin, A. Darensburg, and D. E. Castle, "Gibraltar a mobile host-based intrusion protection system," 2006.

[9] G. A. Jacoby, R. Marchany, and N. Davis, "Battery-based intrusion detection a first line of defense," in *Information Assurance Workshop, 2004. Proceedings from the Fifth Annual IEEE SMC*. IEEE, 2004, pp. 272–279.

[10] J. Hall, M. Barbeau, and E. Kranakis, "Anomaly-based intrusion detection using mobility profiles of public transportation users," in *Wireless And Mobile Computing, Networking And Communications, 2005.(WiMob'2005), IEEE International Conference on*, vol. 2. IEEE, 2005, pp. 17–24.

[11] Y. Moreau, H. Verrelst, and J. Vandewalle, "Detection of mobile phone fraud using supervised neural networks: A first prototype," *Artificial Neural NetworksICANN'97*, pp. 1065–1070, 1997.

[12] B. Sun, Z. Chen, R. Wang, F. Yu, and V. C. Leung, "Towards adaptive anomaly detection in cellular mobile networks," in *Consumer Commu- nications and Networking Conference, 2006. CCNC 2006. 3rd IEEE*, vol. 2. IEEE, 2006, pp. 666–670.