Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 6, June 2015, pg.249 – 253

RESEARCH ARTICLE

A Study on Various Security Attacks in Wireless Networks

Garima Rathee
Student, PDM College of Engineering, Bahadurgarh, Haryana

Parveen Bano
Assistant Professor, PDM College of Engineering, Bahadurgarh, Haryana

Sugandha Singh
Associate Professor & HOD (CSE Deptt.), PDM College of Engineering, Bahadurgarh, Haryana

Abstract: As a network provides the information sharing among public and private users, It increases the communication criticalities. The criticalities are identified in terms of associated attacks. These attacks are performed by internal or external users to give information loss or to reveal the communicating information. To take the significant decision about communication approach, it is required to identify the associated attacks at early stage. In this present work, a study on the network attacks is defined. The paper has discussed type of security attacks that a network suffers. In this paper, some of the common network attacks are explained in detail.

Keywords: Attacks, WormHole, Grayhole, Blackhole

I. INTRODUCTION:

Network attack is usually defined as an intrusion on your network infrastructure that will first analyse your environment and collect information in order to exploit the existing open ports or vulnerabilities - this may include as well unauthorized access to your resources. In such cases where the purpose of attack is only to learn and get some information from your system but the system resources are not altered or disabled in any way, we are dealing with a passive attack. Active attack occurs where the perpetrator accesses and either alters, disables or destroys your resources or data. Attack can be performed either from outside of the organization by unauthorized entity **(**Outside Attack**)** or from within the company by an "insider" that already has certain access to the network **(**Inside Attack**)**. Very often the network attack itself is combined with an introduction of a malware components to the targeted systems.

A resource (both physical or logical), called an asset, can have one or more vulnerabilities that can be exploited by a threat agent in a threat action.

The result can potentially compromisesthe Confidentiality, Integrity or Availability properties of resources (potentially different that the vulnerable one) of the organization and others involved parties. The so-called CIA triad is the basis of Information Security. A Threat is a potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm. That is, a threat is a possible danger that might exploit a vulnerability. A threat can be either "intentional" (i.e., intelligent; e.g., an individual cracker or a criminal organization) or "accidental" (e.g., the possibility of a computer malfunctioning, or the possibility of an "act of God" such as an earthquake, a fire, or a tornado).A set of policies concerned with information security management, the information security management systems (ISMS), has been developed to manage, according to Risk management principles, the countermeasures in order to accomplish to a security strategy set up following rules and regulations applicable in a country.

An attack should led to a *security incident* i.e. a *security event* that involves a *security violation*. In other words, a security-relevant system event in which the system's security policy is disobeyed or otherwise breached. An organization should make steps to detect, classify and manage security incidents. The first logical step is to set up an Incident response plan and eventually a Computer emergency response team.

In order to detect attacks, a number of countermeasures can be set up at organizational, procedural and technical levels. Computer emergency response team, Information technology security audit and Intrusion detection system are example of these.

A) Wireless Local Area network(WLAN)-

A **wireless local area network** (**WLAN**) is a wireless computer network that links two or more devices using a wireless distribution method (often spread-spectrum or OFDM radio) within a limited area such as a home, school, computer laboratory, or office building. This gives users the ability to move around within a local coverage area and still be connected to the network, and can provide a connection to the wider Internet. Most modern WLANs are based on IEEE 802.11 standards, marketed under the Wi-Fi brand name.

Wireless LANs have become popular in the home due to ease of installation and use, and in commercial complexes offering wireless access to their customers; often for free. New York City, for instance, has begun a pilot program to provide city workers in all five boroughs of the city with wireless Internet access.

Wireless LANs have a great deal of applications. Modern implementations of WLANs range from small in-home networks to large, campus-sized ones to completely mobile networks on airplanes and trains. Users can access the Internet from WLAN hotspots in restaurants, hotels, and now with portable devices that connect to 3G or 4G networks. Oftentimes these types of public access points require no registration or password to join the network. Others can be accessed once registration has occurred and/or a fee is paid.

- *Types of WLAN-*

The IEEE 802.11 has two basic modes of operation: ***adhoc*** mode and **infrastructure** mode. In *ad hoc* mode, mobile units transmit directly peer-to-peer. In infrastructure mode, mobile units communicate through an access point that serves as a bridge to other networks.

- *Performance and Throughput-*

WLAN, organised in various layer 2 variants (IEEE 802.11) has different characteristics. Across all flavours of 802.11 maximum achievable throughputs are either given based on measurements under ideal conditions or in the layer 2 data rates. This however does not apply to typical deployments in which data is being transferred between two endpoints of which at least one is typically connected to a wired infrastructure and the other endpoint is connected to an infrastructure via a wireless link.This means that typically data frames pass an 802.11 (WLAN) medium and are being converted to 802.3 (Ethernet) or vice versa.

Due to the difference in the frame (header) lengths of these two media, the packet size of an application determines the speed of the data transfer. This means that an application which uses small packets (e.g. VoIP) creates a dataflow with a high overhead traffic (e.g. a low goodput).

Other factors which contribute to the overall application data rate are the speed with which the application transmits the packets (i.e. the data rate) and of course the energy with which the wireless signal is received.

B) Security threat-

In computer security a **threat** is a possible danger that might exploit a vulnerability to breach security and thus cause possible harm.

A threat can be either "intentional" (i.e., intelligent; e.g., an individual cracker or a criminal organization) or "accidental" (e.g., the possibility of a computer malfunctioning, or the possibility of a natural disaster such as an earthquake, a fire, or a tornado) or otherwise a circumstance, capability, action, or event.

- A **passive attack** monitors unencrypted traffic and looks for clear-text passwords and sensitive information that can be used in other types of attacks. **Passive attacks** include traffic analysis, monitoring of unprotected communications, decrypting weakly encrypted traffic, and capturing authentication information such as passwords. Passive interception of network operations enables adversaries to see upcoming actions. Passive attacks result in the disclosure of information or data files to an attacker without the consent or knowledge of the user.
- In an **active attack,** the attacker tries to bypass or break into secured systems. This can be done through stealth, viruses, worms, or Trojan horses. Active attacks include attempts to circumvent or break protection features, to introduce malicious code, and to steal or modify information. These attacks are mounted against a network backbone, exploit information in transit, electronically penetrate an enclave, or attack an authorized remote user during an attempt to connect to an enclave. Active attacks result in the disclosure or dissemination of data files, DoS, or modification of data.
- A **distributed attack** requires that the adversary introduce code, such as a Trojan horse or back-door program, to a “trusted” component or software that will later be distributed to many other companies and users Distribution attacks focus on the malicious modification of hardware or software at the factory or during distribution. These attacks introduce malicious code such as a back door to a product to gain unauthorized access to information or to a system function at a later date.
- An **insider attack** involves someone from the inside, such as a disgruntled employee, attacking the network Insider attacks can be malicious or no malicious. Malicious insiders intentionally eavesdrop, steal, or damage information; use information in a fraudulent manner; or deny access to other authorized users. No malicious attacks typically result from carelessness, lack of knowledge, or intentional circumvention of security for such reasons as performing a task

II. LITERATURE SURVEY

In Year 2011, T.Subbulakshmi performed a work," Detection of DDoS Attacks using Enhanced Support Vector Machines with Real Time Generated Dataset". The focus of this paper is to generate the Distributed Denial of Service (DDoS) detection dataset and detect them using the Enhanced Support Vector Machines. The DDoS dataset with various direct and derived attributes is generated in an experimental testbed which has 14 attributes and 10 types of latest DDoS attack classes. Using the generated DDoS dataset the Enhanced Multi Class Support Vector Machines (EMCSVM) is used for detection of the attacks into various classes.

In Year 2007, Vera Marinova-Boncheva performed a work," Applying a Data Mining Method for Intrusion Detection". Every networked computer, to varying degrees, is vulnerable to malicious computer attacks that can result in a range of security violations, such as, unauthorized user access to a system or the disruption of system services. In this paper Author would like to show how a data mining tool like XLMiner™ can also contribute to intrusion detection by extracting classification rules.

In Year 2012, Neelam Sharma performed a work," Layered Approach for Intrusion Detection Using Naive Bayes Classifier". In this paper Author propose layered approach for improving the minority attack detection rate without hurting the prediction performance of the majority attacks. The proposed model used Naive Bayes classifier on reduced dataset for each attack class. In this system every layer is separately trained to detect a single type of attack category.

In Year 2012, C.I. Ezeife performed a work," NeuDetect: A Neural Network Data Mining Wireless Network Intrusion Detection System". This paper proposes NeuDetect, which applies a classification rule mining Neural Network technique to wireless network packets captured through hardware sensors for purposes of real time detection of anomalous packets. The proposed system, NeuDetect, solution approach is to find normal and anomalous patterns on pre-processed wireless packet records by comparing them with training data using Back-propagation algorithm.

In Year 1999, Wenke Lee performed a work," Mining in a Data-flow Environment: Experience in Network Intrusion Detection". Author discuss the KDD process in “data-flow” environments, where unstructured and time dependent data can be processed into various levels of structured and semantically rich forms for analysis tasks. Author present procedures for analyzing frequent patterns from lower level data and constructing appropriate features to formulate higher level data.

LTC Bruce D. Caulkins performed a work," A Dynamic Data Mining Technique for Intrusion Detection Systems". Author report the findings of Presented research in the area of anomaly-based intrusion detection systems using data-mining techniques described in section 3.3 to create a decision tree model of Presented network using the 1999 DARPA Intrusion Detection Evaluation data set. After the model was created, Author gathered more data from Presented local campus network and ran the new data through the model.

In Year 2010, K C Nalavade performed a work," Intrusion Prevention Systems: Data Mining ApproachPresented proposed model combines the knowledge discovery and the intrusion detection so that best action can be taken against the attack. Also this knowledge will be helpful to make the systems efficient and secure. Thus Author propose the prevention technology for the security of networks and host users using data mining algorithms.

In Year 2008, C.I. Ezeife performed a work," WIDS: A Sensor-Based Online Mining Wireless Intrusion Detection System". This paper proposes WIDS, a wireless intrusion detection system, which applies data mining clustering technique to wireless network data captured through hardware sensors for purposes of real time detection of anomalous behavior in wireless packets. The proposed mining based technique for wireless network intrusion detection contributes by reducing the need for training data, reducing false positives and increasing the effectiveness of attack detection on networks with few (one to twenty) connections.

In Year 2002, Klaus Julisch performed a work," Mining Intrusion Detection Alarms for Actionable Knowledge". In this paper, Author mine historical alarms to learn how future alarms can be handled more efficiently. First, Author investigate episode rules with respect to their suitability in this approach. Author report the difficulties encountered and the unexpected insights gained. In addition, Author introduce a new conceptual clustering technique, and use it in extensive experiments with real-world data to show that intrusion detection alarms can be handled efficiently by using previously mined knowledge.

In Year 2012, Guanhua Yan performed a work," Towards a Bayesian Network Game Framework for Evaluating DDoS Attacks and Defense". In this work, Author propose a non-standard game-theoretic framework that facilitates evaluation of DDoS attacks and defense. Presented framework can be used to study diverse DDoS attack scenarios where multiple layers of protection are deployed and a number of uncertain factors affect the decision making of the players, and it also allows us to model different sophistication levels of reasoning by both the attacker and the defender.

In Year 2012, Neelam Sharma performed a work," Layered Approach for Intrusion Detection Using Naive Bayes Classifier". In this paper Author propose layered approach for improving the minority attack detection rate without hurting the prediction performance of the majority attacks. The proposed model used Naive Bayes classifier on reduced dataset for each attack class. In this system every layer is separately trained to detect a single type of attack category.

In Year 2004, Yi Hu performed a work," A Data Mining Approach for Database Intrusion Detection". In this paper Author proposed a data mining approach for detecting malicious transactions in a Database System. Presented approach concentrates on mining data dependencies among data items in the database. A data dependency miner is designed for mining data correlations from the database log.

In Year 2002, Jerzy Bala performed a work," Application of a Distributed Data Mining Approach to Network Intrusion Detection". In this approach, classification rules are learned via tree induction from distributed data to be used as intrusion profiles. Agents, in a collaborative fashion, generate partial trees and communicate the temporary results among them in the form of indices to the data records.

In Year 2006, Yu Liu performed a work," A Bayesian Game Approach for Intrusion Detection in Wireless Ad Hoc Networks". In this paper, Author propose a game theoretic framework to analyze the interactions between pairs of attacking/defending nodes using a Bayesian formulation. Author study the achievable Nash equilibrium for the attacker/defender game in both static and dynamic scenarios. The dynamic Bayesian game is a more realistic model, since it allows the defender to consistently update his belief on his opponent’s maliciousness as the game evolves.

III. CLASSIFICATION OF ATTACKS

1. Gray Hole Attack

Gray hole attack is an active attack type, which lead to dropping of messages. Attacking node first agrees to forward packets and then fails to do so. Initially the node behaves correctly and replays true RREP messages to nodes that initiate RREQ message. Afterwards, the node just drops the packets to launch a (DoS) denial of service attack. If neighboring nodes that try to send packets over attacking nodes lose the connection to destination they may want to discover a route again, broadcasting RREQ messages. Attacking node establishes a route, sending RREP messages. This process goes on until malicious node succeeds in its purpose.

2. Black Hole Attack

The difference of Black Hole Attack compared to Gray Hole Attack is that malicious nodes never send true control messages initially. To carry out a black hole attack, malicious node waits for neighboring nodes to send RREQ messages. When the malicious node receives an RREQ message, without checking its routing table, immediately sends a false RREP message giving a route to destination through itself, assigning a high sequence number to settle in the routing table of the victim node, before other nodes send a true one. Therefore requesting nodes assume that route discovery process is completed and ignore other RREP messages and begin to send packets through the malicious node. Malicious node attacks all RREQ messages from other source nodes also and takes over all routes. Therefore all packets are sent to a point when they are not forwarded anywhere.

3. Worm hole attack

The wormhole attack is quite severe, and consists in recording traffic from one region of the network and replaying it in a different region. It is carried out by an intruder node X located within transmission range of legitimate nodes A and B, A and B are not themselves within transmission range of each other. Intruder node X merely tunnels control traffic between A and B (and vice versa), without the modification presumed by the routing protocol – e.g. without stating its address as the source in the packets header – so that X is virtually invisible.

IV. CONCLUSION

In this paper, an exploration to the various kinds of security threats is provided. The paper also includes the classification of different kind of associated attacks. The paper has provided the detailed description of these common network attacks along with their effect on network.

REFERENCES

[1] T.Subbulakshmi," Detection of DDoS Attacks using Enhanced Support Vector Machines with Real Time Generated Dataset", IEEE-ICoAC 2011 978-1-4673-0671-3/11©2011 IEEE

[2] Vera Marinova-Boncheva," Applying a Data Mining Method for Intrusion Detection", International Conference on Computer Systems and Technologies - CompSysTech'07

[3] Neelam Sharma," Layered Approach for Intrusion Detection Using Naive Bayes Classifier", ICACCI'12, August 3-5, 2012, Chennai, T Nadu, India. ACM 978-1-4503-1196-0/12/08

[4] C.I. Ezeife," NeuDetect: A Neural Network Data Mining Wireless Network Intrusion Detection System", IDEAS10 2010, August 16-18, Montreal, QC [Canada]; Editor: Bipin C. DESAI; ACM 978-1-60558-900-8/10/08

[5] Wenke Lee," Mining in a Data-flow Detection", KDD-99 San Diego CA USA

[6] LTC Bruce D. Caulkins," A Dynamic Data Mining Technique for Intrusion Detection Systems".

[7] K C Nalavade," Intrusion Prevention Systems: Data Mining Approach", International Conference and Workshop on Emerging Trends in Technology (ICWET 2010) – TCET, Mumbai, India ICWET'10, February 26–27, 2010, Mumbai, Maharashtra, India. ACM 978-1-60558-812-4

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

[9] Klaus Julisch," Mining Intrusion Detection Alarms for Actionable Knowledge", SIGKDD '02 Edmonton, Alberta, Canada ACM 1-58113-567-X/02/0007

[10] Guanhua Yan," Towards a Bayesian Network Game Framework for Evaluating DDoS Attacks and Defense", CCS'12, October 16–18, 2012, Raleigh, North Carolina, USA. ACM 978-1-4503-1651-4/12/10

[11] Neelam Sharma," Layered Approach for Intrusion Detection Using Naive Bayes Classifier", ICACCI'12, August 3-5, 2012, Chennai, T Nadu, India. ACM 978-1-4503-1196-0/12/08

[12] Yi Hu," A Data Mining Approach for Database Intrusion Detection", 2004 ACM Symposium on Applied Computing SAC '04, March 14-17, 2004, Nicosia, Cyprus. ACM 1-58113-812-1/03/04

[13] Jerzy Bala," Application of a Distributed Data Mining Approach to Network Intrusion Detection", AAMAS'02, July 15-19, 2002, Bologna, Italy. ACM 1-58113-480-0/02/0007

[14] Yu Liu," A Bayesian Game Approach for Intrusion Detection in Wireless Ad Hoc Networks", GameNets'06, October14, 2006, Pisa, Italy. ACM 1-59593-507-X/06/10