Research Open Journal of Wireless Networks and Applications
Vol. 1, No. 1, May 2013, PP: 01 - 06
Available online at http://www.scitecpub.com/Journals.php

Research article

Pattern Classification of Wireless Network Security: Threats, and Countermeasures

***SanaUllah, **Shakeel Nouman, ***Dr. Yasir Abrar**

*Network Engineer, Planning & Development Department, Lahore, Pakistan
**Assistant Chief (Coord / IT), Planning & Development Department, Lahore, Pakistan
***Veterinary Doctor, Governor House Punjab, Lahore, Pakistan

E-Mail: sn_gcu@live.com; almani41@gmail.com

Abstract

The security of computer networks plays a vital role in modern computer technology. In order to provide high protection against Threat, a number of software has been developed to resolve the threats. Intrusion Detection System has recently become a prominent topic for research due to its capacity of detecting threats from network users. Wireless networking has many advantages, but it has great threat of new security pattern which alters the organization's profile due malicious attacks. Many network security applications rely on pattern Classification to extract the threat from network traffic. Effective management of the threats associated with wireless technology needs a sound and thorough assessment of risk given the environment and development of a plan to alleviate identified threats. We develop a framework to access the various threats associated with the use of wireless Networks. Therefore it is very essential to develop faster and more reliable pattern Classification algorithm for network wireless security.

Keywords: - Threat detection, Pattern Classification, Wireless Network Security

Introduction

Local Area network is expanding at a tremendous speed with the growth of Internet. This situation helps to improve the quality of services and expediency of the human life. The number of Threats into computer systems is growing and raising concerns about computer security. So computer networks can be protected against threats by the means of restriction policies. Microsoft has defined security as "The protection of information assets through the use of

technology, processes, and training (1). Wireless networking presents many advantages Productivity improves because of increased accessibility to information resources. Network configuration and reconfiguration is easier, faster, and less expensive. However, wireless technology also creates new threats and alters the existing information security risk profile.

The objective of this paper is to provide a mechanism in making such decisions by providing them with a basic understanding of the nature of the various threats associated with wireless networks security. Intrusion detection which refers to a certain class of system attack detection problems is a relatively new research area in computer and information security (2).

In general IDS can be categorized into two ways: (i) misuse (ii) Error detection approaches. Misuse detection system can reliably identify Threats in relation to the known pattern classification of discovered. It is very necessary that security experts needs to define accurate rules or patterns, which control the applications of misuse detection systems. However, emergent intervention of security experts is required to define accurate rules or patterns, which limit the applications of misuse detection systems, identify deviations from normal network behaviors and alert for potential unseen attacks (3).

The popularity of wireless Networks is a testament primarily to their convenience, cost efficiency, and ease of integration with other networks and network components. Wireless Network technology, while replete with the conveniences and advantages described above has its share of downfalls. For a given networking situation, wireless Networks may not be desirable for a number of reasons. Most of these have to do with the inherent limitations of the technology. A study by eMarketer indicates an average loss of $10 billion per year due infractions in computer security (4). The disadvantages of using a wireless network are: Security, Range, Reliability, and Speed. So, machine learning techniques have been used to capture the normal usable patterns and classify the behavior as either normal or abnormal (5). While the pattern classification algorithms are applied to wireless network security, the speed of pattern classification usually becomes a bottleneck. This paper proposes a pattern classification mechanism which overcomes the shortcomings of traditional algorithms and provide a technique to overcome the threats in the wireless networks.

Wireless Network Attacks

Accidental Attacks

When a user turns on a computer system and it clasps on to a wireless access point from a neighboring company's overlapping network, the user may not even know that this happened in the computer.

Malicious Attacks

When wireless devices can be actively made by crackers to connect to a company network through their cracking laptop instead of a company access point (AP).

Ad-Hoc Networks

Ad-hoc networks are defined as peer-to-peer networks between wireless computers that do not have an access point in between them.

MAC Spoofing

MAC spoofing) occurs when a cracker is able to listen in on network traffic and identify the MAC address of a computer with network privileges.

Denial of Service

A Denial-of-Service attack (DoS) occurs when an attacker continually bombards a targeted AP (Access Point) or network with bogus requests, premature successful connection messages, failure messages, and/or other commands.

Network Injection

In a network injection attack, a cracker can make use of access points that are exposed to non-filtered network traffic, specifically broadcasting network traffic such as “Spanning Tree” (802.1D), OSPF, RIP, and HSRP.

Caffe Latte Attack

The Caffe Latte attack is another way to defeat WEP. It is not necessary for the attacker to be in the area of the network using this exploit. By using a process that targets the Windows wireless stack, it is possible to obtain the WEP key from a remote client.

Methodology

Pattern recognition undergoes an important developing for many years. Pattern recognition includes a lot of methods which are impelling the development of numerous applications in different field.

Statistical Pattern Recognition

The Statistical methods have been commonly used for pattern recognition. Statistical approaches have a number of advantages. It can provide accurate notification of malicious activities that typically occur over extended periods of time and are good indicators of impending denial-of-service attacks (6). However, it also has drawbacks. It can be difficult to determine thresholds that balance the likelihood of false positive alarms with the likelihood of false negative alarms. In addition, this method need accurate statistical distributions, but, not all behaviors can be modeled using purely statistical methods. The statistical pattern recognition deals with features only without consider the relations between features (7).

Data Clustering

Data clustering is a technique for finding patterns in unlabeled data with many dimensions. It is an unsupervised method. The main advantage of data clustering is the ability to learn from and detect intrusions in the audit data,

while not requiring the explicit descriptions of various attack classes. The method of data clustering can be partitioned into two classes, one is hierarchical clustering and the other is partition clustering.

Fuzzy Set

It is collection of things that belongs to definition. Any item either belongs to that set or does not belong to that set. The fuzzy logic provides the partial membership in set theory to integrate with the association rules and frequent episodes which solved the above problem. Fuzzy rule-based systems inspired by the fuzzy set theory have been successfully applied to solve many complex and non-linear problems. The application of fuzzy sets in pattern recognition started in 1966, where two basic operations – abstraction and generalization. Pattern Recognition system based on fuzzy sets theory can imitate thinking process of human being widely and deeply.

Artificial Neural Networks

An Artificial Neural Network (ANN) is an information processing paradigm that is inspired by the way biological nervous systems, such as the brain, process information. The key element of this paradigm is the novel structure of the information processing system. It is composed of a large number of highly interconnected processing elements (neurones) working in unison to solve specific problems. The Artificial Neural Network methodology enables us to design useful nonlinear systems accepting large numbers of inputs, with the design based solely on instances of input-output relationship. The first Artificial Neural Network model was proposed in 1943. Today it is developing very fast. Basically it is a data clustering method based on distance measurement. This approach applies biological concepts to machines to recognize patterns. Pattern Recognition using Artificial Neural Network is a very attractive since it requires minimum priory knowledge, and with enough layers and neurons, an Artificial Neural Network can create any complex decision region.

Structural Pattern Recognition

The recognition of patterns is required in many application areas. The type of data that is analyzed varies greatly. Examples of one-dimensional data include speech signals, electrocardiograms, and seismic data. Examples of two-dimensional data include scanned document images, medical images, and satellite images. Three-dimensional data arises in image sequences, in crystallography, and in tomography. The goal of pattern-recognition research is to develop general, domain-independent techniques for data analysis.

Structural Pattern Recognition emphases on the description of the structure, namely explain how some simple sub-patterns compose one pattern. The syntax analysis and structure matching are the two main methods in structural pattern recognition. The basis of syntax analysis is the theory of formal language, the basis of structure matching is some of special technique of mathematics based on sub-patterns. The structural pattern recognition handles with symbol information. This method can be used in applications with higher level, such as image interpretation. Pattern

Recognition of multidimensional objects can be done by structural pattern recognition with static classification or artificial neural networks.

Support Vector Machine (SVM)

Vector Machines (SVMs), a new generation learning system based on recent advances in statistical learning theory. SVMs deliver state-of-the-art performance in real-world applications such as text categorization, hand-written character recognition, image classification, bio sequences analysis, etc., and are now established as one of the standard tools for machine learning and data mining.

Approximate reasoning approach to Pattern Recognition

Approximate reasoning approach to pattern recognition consists of two concepts- one is fuzzy applications and the other is compositional rule of inference can cope with the problem for rule based pattern recognition (8).

Pattern Recognition System

The intrusion detection system suffers from various risky alarms and by misusing the intrusion detection system; it lacks to detect new attack types. Pattern Recognition techniques have been found to strike a fine balance in this trade off. The use of pattern recognition and classification has grown in the past few years to solve threats which come from hackers. They are able to filter noise and extract features from traffic to facilitate classification. Pattern classification is a consists of series of steps, starting with the input, moving to segmentation, data extraction and translation and finally classification (9).

The aim of pattern classification is to utilize the information acquired from pattern analysis to discipline the computer in order to accomplish the classification. The next step following Data extraction is classification. It is the process of using the data set to classify the traffic as normal or illegitimate traffic. The classifications can be divided into three categories: normal, Denial of Service and Scan. Numerical values were assigned the three categories based on their probability.

Conclusion

Wireless networking provides several opportunities to increase productivity and reduce costs. It also changes an organization’s overall computer security risk profile. It is impossible to totally eliminate all threats associated with wireless Networks, it is possible to achieve a reasonable level of security by adopting a systematic approach to assessing and managing risk. It also stressed the importance of training and educating users in safe wireless networking procedures.

References

[1] Available online Weblink,www.microsoft.com/security/glossary.mspx

[2] Dit Yeung Y, Yuxin D. Host-based Intrusion Detection using Dynamic and Static Behavioral Models. The journal of Pattern Recognition 36 (2003).

[3] Chi-Ho T, Sam K, Hanli W. Genetic-fuzzy rule mining approach and evaluation of feature selection techniques for anomaly intrusion detection. The journal of Pattern Recognition 40 (2007).

[4] Weblink,http://www.cisco.com/en/US/netsol/networking-solutions-networking-basic09186a00800a3549.html

[5] Mohammad Saniee A, Jafar H, Zeynab B, Muna S. A Parallel Genetic Local Search Algorithm for Intrusion Detection in Computer Networks, Engineering Applications of Artificial Intelligence 20 (2007).

[6] Giacinto, Fabio R, Luca D. Fusion of Multiple Classifier for Intrusion Detection in Computer Networks, Pattern Recognition Letters 24 (2003).

[7] Steven L, Scott A. Bayesian Paradigm for Designing Intrusion Detection Systems: Computational Statistics & Data Analysis. 45 (2004)

[8] Liu, Sun, Wang. Pattern Recognition: an overview, IJCSNS. June 2006

[9] Yang W and Hidetsune K. High Performance Pattern Matching Algorithm for Network Security, IJCSNS. Vol.6 No.10, Oct 2006.

[10] Zachary Baker K and Viktor Prasanna K. High-throughput Linked-Pattern Matching for Intrusion Detection Systems. ANCS'05, Oct 26-28, 2005, Princeton, New Jersey, USA