ENHANCED MOVING TARGET DEFENSE MECHANISMS TO HANDLE CYBER ATTACKS

CHAPTER 1

1. INTRODUCTION

1. INTRODUCTION

Recent OpenNet initiatives and experience of pentagon clearly indicate the explosion of cyber attacks and cyber threats. The unexpected growth rate of cyber attacks in cyber space challenges the entire community.

1.1. Cyberspace

Cyberspace is a globally interconnected information or infrastructure which is critical and essential for modern society [71]. Cyber security comprises of numerous interconnected components and software assurance. The former extends the boundary of physical security to the domain of cyberspace while the later depends on the technology to provide desirable solutions that can be implemented in the cyberspace. Cyber attacks are very alarming today challenging the economy and the security of a Nation.

1.2. Cyber Attacks

Cyber attacks[18][51] is a process by which an individual or group of persons trying to access a system illegally to exploit data or information. Disruption of integrity or authenticity of data or information is termed as computer network attack or cyber attack. The malicious code written for this purpose alters the logic of the program and performs certain unwanted activities. The process of hacking [77]involves the scanning of the Internet to get the systems which contain poor security control and looking for systems which are mis-configured. Once the hacker infects the system, he/she can remotely operate the infected system and the commands can be sent to make the system to act as a spy for the attackers that can be used to disrupt the services of the other systems. The hacker will expect the infected system to have some flaws such as bugs in software, deficient in anti-virus, flawed system configuration so that other systems can be infected through this system. Cyber attack[15] [16] aims to steal or hack the information of any organization or government offices.

Different types of cyber attacks [2][39] are

- Virus.
- Malware, Worms and Trojan horse.

- Botnet and Zombie.
- Scareware.
- Cloud Computing attacks and
- Social Network Attacks.

Attackers use different methods to capture data. They include

- Unauthorized access to secured data.
- Disabling of system Logs.
- Software alteration by the Intruders.
- Installation of Malicious Software.
- Active probes for new systems by Infected Systems.

The main causes behind these attacks [35][47] are budget cuts, no proper security in network applications, cloud computing, static system and heterogeneous targets. Cyber attacks can be classified based on their behaviour too.

1.3 Classification of Cyber Attacks

The cyber attacks are commonly classified [62][64][65] into two categories. The classification is shown in figure 1.1.

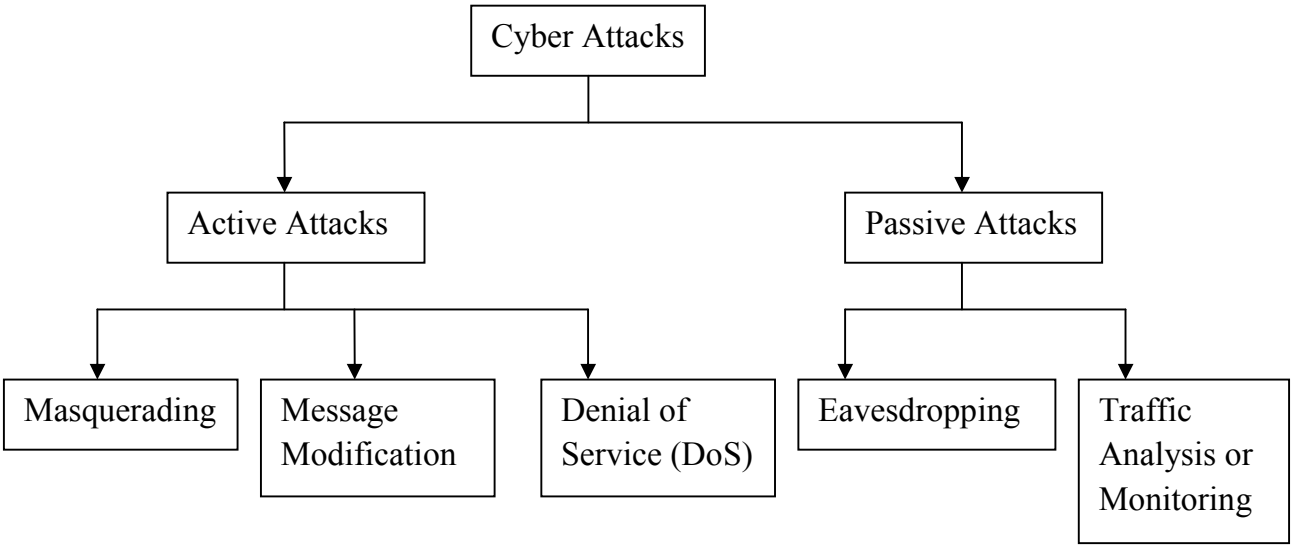

Figure.1.1. Cyber attack Classification

1.3.1. Active Attacks

An active attack[61] permits the attacker to transmit data to all the parties, or block the data transmission with single or multi directional. The attacker may try to terminate the data sent by the parties in the network as the attacker is located between the intercommunicating parties. The attacker then attempts to take the place of the client when the authentication procedure has been performed because the source of the data cannot be authenticated by the server without validation of the information received. Without much effort, a computer is placed as a liaison between the two subnets. This intermediate placement of an entity is the vulnerable point of active attacks. The active attack is classified into three types namely,

- Masquerading
- Message Modification
- Denial of Service

Masquerading

The attacker will masquerade as an authorized person and will benefit easy access to the data available in the network.

Message Modification

Adding, altering, changing, modifying, deleting the data will be done by the attacker.

Denial of Service (DoS)

The accessing of the data available in the network will be prohibited by the attacker to the authorized users. The availability of the system and services for the entire network will be prevented for the authorized users. The traditional way of attack causes the flow of packets to the centralized unit and blocking the same from others accessing the network.

1.3.2. Passive Attacks

A passive attack[12] is an attack in which an unauthorized attacker eavesdrops the communication between two parties in order to steal information stored in a system by

wiretapping or by similar means. When compared to active attack, it does not attempt to meddle with the database but it may still constitute a criminal offense. The passive attacks are:

- Eavesdropping
- Traffic analysis or monitoring

Eavesdropping

The message content will be monitored while communicating.

Traffic analysis or monitoring

The pattern of communication will be monitored at the time of data transmission. Depending on the types of attacks, many attack handling mechanisms are also available in the literature.

1.4. Cyber Attack Handling Mechanisms

Some of significant cyber attack handling mechanisms are:

- Scientific Approach
- Add-on Approach
- Dead-end Approach
- Game Changing Approach

Figure.1.2 shows the some of the significant cyber attack handling mechanisms.

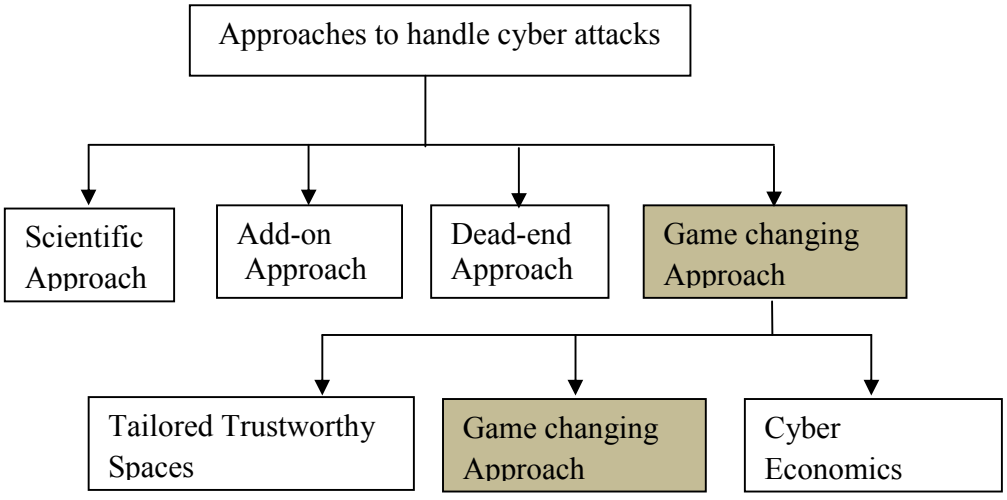

Figure .1.2 Cyber Attack Handling Mechanisms

Scientific Approach

A scientific approach combines fundamental understanding with experimentation, theory and modeling for maximizing intellectual resources and to prioritize research needs. This approach focuses on the use of science and mathematics for the developing system architecture and methods of protection of systems from attacks that are superior to traditional methods.

Add-on Approach

Add on approach is a kind of a method that deals with a particular attack to prevent the valuable source of data; wherein, it has the capability of adding a new feature if there is a need.

Dead-end Approach

This is another kind of approach which is the reverse of the add-on approach where no updating or alteration can take place once the approach is developed.

Game Changing Approach

Game changing approach [26] will ensure that uniform levels of security will be provided across eco system, according to the needs of the users thereby benefiting the entire computing environment. Some of the game changing approaches are

- Tailored Trustworthy Spaces
- Moving Target Defense Mechanisms
- Cyber economics

Of the four cyber attack handling methods, the game changing approach is a significant one due to the handling of attacks as, "Attack only work once if at all". Every cyber attack handling mechanism is different from the other methods with their own advantages and limitations. Therefore the initial problem is formulated as given below.

This research work concentrates on Moving Target Defense Mechanisms.

Moving target defense mechanisms are dynamic in a way that is manageable for the defender, but makes it extremely difficult for the attacker. It is opposed to the traditional approach that adds complexity to the systems which may lead to increase in the risk. Therefore, a moving target focuses on increasing complexity in a way which is beneficial for the user and not a liability.

The major benefit of moving target defense is to decrease attack surface area to adversaries while simultaneously shifting it. It differs widely from other game changing approaches as it focuses on maximum performance in a compromised environment rather than total security. Moving target defense makes the operating networks and systems function in a less deterministic and homogeneous manner, thereby changing the traditional reactive patching and upgrading methods to secure vulnerable systems and also increasing the cost of attacks.

1.5. Problem Statement

Given the situation of cyber attacks, device a mechanism to increase the accuracy of detection without compromising the QoS (**Q**uality **o**f **S**ervice) like end to end delay, throughput, packet delivery ration, latency and routing overheads.

1.6. Problem Justification

Dennis Blair, Former Director of OpenNet Initiative stated in 2010 that, "Malicious cyber activity is growing at an unprecedented rate and countrys' effort towards cyber security is not strong enough". During the year 2010, pentagon declared that they are experiencing with 5000 cyber attacks per day and stated that scalable trust is essential for personal, private, public and national levels.

With the above challenges in handling the cyber attacks, the major objective of this research work is formulated. The primary and secondary objectives are formed after thorough literature study. The primary objective is to device a ubiquitous mechanism to handle known and unknown cyber attacks through value added services that can cater to the requirements of users and the computing environment.

1.7. Secondary Objectives of the Thesis

The secondary objectives of the research work are to:

- Improve the quality of service in terms of end-to-end delay, latency, packet delivery ratio and throughput
- Reduce the number of retransmissions of data packets
- Save time
- Improve the accuracy of detection
- Appropriate security application and
- Enhance storage security

A research methodology is devised to meet the above objectives as discussed in the subsequent chapters. Significant contributions of the research work are presented.

1.8. Significant Contributions

Following are the significant contributions of this research work:

- The accuracy level of detection of cyber attacks is increased
- A new application is developed to secure data by introducing data chunking in non-sequential storage.
- An integrated method is proposed to improve security
- Enhanced click dynamics is proposed to ensure user authentication
- Secure hash based game theory method is proposed to defend against cyber attacks.

1.9. Organization of the Thesis

The thesis is organized as follows:

Chapter 1 presented various cyber attacks, attack handling mechanisms, the problem statement and justification. The objectives of the thesis along with contributions are also presented. Finally the organization of the thesis is given.

Chapter 2 presents the review of literature for problem domain. The various cyber attack handling mechanisms for known and unknown attacks are presented in detail in this chapter.

Chapter 3 explains the entire research methodology in various steps. The Proposed approach, general steps involved, consolidated and conceptual view of the proposed approach is presented in detail.

In chapter 4, the first steps of the proposed research design is discussed in detail.

In Chapter 5 details about the secure hash based game theory method is presented

Chapter 6 illustrates about the enhanced click dynamics which ensures user authentication.

Chapter 7 presents in detail about the new application developed to secure the data or files using enhanced data chunking method.

Chapter 8 describes about the integrated method proposed to improve the level of security, Comparison and evaluation of the proposed methods in terms of accuracy of detection of cyber attacks is also given.

Finally, conclusion and future directions are given in Chapter 9.

1.10. Chapter Summary

In this chapter, the cyber attacks and cyber attacks handling mechanisms are described. Apart from the justification, the primary and secondary objectives of this research work are discussed in detail. Significant contributions of this research work are also given briefly. Four different methods of moving target defense mechanisms are taken into consideration in this research work as they play a major role in securing the data or information. The four methods discussed are enhanced in terms of detection accuracy and QoS parameters. Chapter 2 discusses the existing moving target defense mechanisms and their applications in detail.

These methods provide detection and prevention of data from cyber attacks. The main concept behind these moving target defense mechanisms is “an attack works if at all only once” so the proposed approaches will confuse the attackers and the attacker will

find difficulties in hacking, accessing or modifying the information. The stability, durability, accessibility, security can be achieved while using those four different approaches.