Chapter 4

Classification of Network Attacks and Countermeasures of Different Attacks

C. V. Anchugam
Government Arts College (Autonomous), India

K. Thangadurai
Government Arts College (Autonomous), India

ABSTRACT

Network security has become more important and the growing rate of network attacks together with hacker, cracker, and criminal enterprises are increasing, that impact to the availability, confidentiality, and integrity of vital information data. In order to understand and defend against network attacks, it is necessary to understand the kind of attack. This chapter focuses on the provisioning of a method for the analysis and categorization of both computer and network attacks, thus providing assistance in combating new attacks, improving computer and network security as well as providing consistency in language when describing attacks. Attacks are thus attempts by unauthorized individuals to access or modify information, to deceive the system so that an unauthorized individual can take over an authorized session, or to disrupt service to authorized users. During this chapter we tend to area unit providing the elucidation against black hole attack that relies on fuzzy rule in case study section.

INTRODUCTION

In today’s information age, information sharing and transfer has increased exponentially. The information should be vulnerable and guarded to unauthorized access and interception. With the event of network techniques the problem of network security becomes a lot of of and a lot of necessary throughout storage and transmission of information. With the rapid development of computer network and information technology, the Internet has been suffering from a variety of security attacks over the past few years. Fast Internet growth and increase in number of users make network security essential in recent decades.

DOI: 10.4018/978-1-4666-8761-5.ch004
Network security has become more important to personal computer users, organizations, and also the military. Security became a significant concern and also the history of security permits a higher understanding of the emergence of security technology. The growing rate of network attacks together with hacker, cracker, and criminal enterprises are increasing, that impact to the availability, confidentiality, and integrity of vital information data. Attacks over the years have become both progressively numerous and sophisticated, and the defender cannot understand. In order to understand and defend against network attacks, it is necessary to understand the kind of attack.

Taxonomy of network attacks is designed to be useful to information bodies such as CERTs (Computer Emergency Response Teams) who have to handle and categorize an ever increasing number of attacks on a day to day. Information bodies could use the taxonomy to communicate more effectively because the taxonomy would supply a common classification scheme.

**BASIC SECURITY CONCEPTS**

It seems that every other day there is a story in the newspapers about a computer network being compromised by hackers. In fact, not too long ago the United States Department of Defense (DoD) was the victim of a successful hacker raid; hackers were able to penetrate DoD computers during a two-week period before they were detected. Fortunately, the computers contained only non-classified personnel and payroll information, so national security was not threatened. More recently, Yahoo, Amazon.com, eBay, and some other popular World Wide Web (WWW) sites were targets of what appears to have been a coordinated “denial-of-service” attack. During a three- or four-day period, the sites were overwhelmed with massive bombardments of false traffic from multiple sites. As a result, the sites were shut down for hours at a time. These attacks illustrate how pervasive the threat from outside hackers has become.

At the same time, every organization that uses computers faces the threat of hacking from individuals within the organization. Employees or former employees with malicious intent or who want to obtain information such as employee salaries or view other employee’s files are also a threat to an organization’s computers and networks. Computerworld recently ran a story about a programmer employee of a company who allegedly launched a denial-of-service attack against his own company, a provider of on-line stock trading services. Apparently, this programmer was in negotiations with the company for more compensation.

He became frustrated with the progress of the negotiations and decided to demonstrate to the company its vulnerability by launching an attack on its systems from the Internet. He was intimately familiar with the company’s systems and software, and his inside knowledge enabled him to hit the firm in a manner that shut it down. In fact, the attack disrupted stock trading services at the company for three days. The U.S. Secret Service was eventually employed, and the attack was traced to the employee, who was subsequently arrested. Every organization should monitor its systems for possible unauthorized intrusion and other attacks. This needs to be part of the daily routine of every organization’s IT unit, as it is essential to safeguarding a company’s information assets.

The most reliable way to ensure the safety of a company’s computers is to refrain from putting them on a network and to keep them behind locked doors. Unfortunately, however, that is not a very practical solution. Today, computers are most useful if they are networked together to share information and resources, and companies that put their computers on a network need to take some simple precautions to reduce the risk of unauthorized access. Every year, corporations, governments, and other organizations...