Chapter 13
A Systematic Mapping of Security Mechanisms

Gayathri RajaKumaran
VIT University, India

NeelaNarayanan Venkataraman
VIT University, India

ABSTRACT

In the Internet Era, millions of computer systems are connected to the Internet and the number is increasing infinitely. Maintaining proper Control and configuration for all such networked systems has proved to be impossible. This loophole makes the Internet systems vulnerable to various type of attacks. The objective of this research is to systematically identify a wide list of attacks in transport, session and application layers (Host layers). 148 effective controls are identified for the security attacks in addition to the 113 standard controls. The identified controls are analyzed in order to map and categorize them to the corresponding security layers wise.

INTRODUCTION

Internet is a dynamic environment in terms of both topology and emerging technology. Internet contains millions of connected computer networks that are accessible through the set of communication protocols; one among them is the Transmission Control Protocol / Internet Protocol (TCP/IP). Diverse categories of end users scattered throughout the globe are accessing Internet services for electronic mail, personal interaction, entrepreneurial ventures, e-commerce, and e-business and so on. However, along with its advantages and immense benefits, the internet is facing security risks. The key design feature of the internet makes it vulnerable to various kinds of attacks. Attack is an attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset. This is done by exploiting vulnerabilities in a computer system. The person who is involved in launching such attacks are categorized as attacker, hacker or cracker based on their motive. The need for attacking the computer system has changed over the years. Few years back, attacks are launched “by hand” as there are no sophisticated tools. But in recent years, more automatic attack generation tools are introduced.
which makes the attack easy to launch. Intruders are utilizing the automated tools to coordinate large scale distributed attacks by targeting hundreds of hosts. Hence all such drawbacks make the Internet open to severe security attacks like eavesdropping, sniffing, IP spoofing, ARP poisoning and Distributed Denial Of Service (DDoS) attack. Security professionals are involved in developing an effective countermeasure to nullify the attacks. But the solutions are proven to be efficient only for known or identified attacks. The drawback in implementing the solution is, most of the Internet users are unaware that their system is under attack. Hence categorization of attacks and key points for attack identification plays a vital role. This motivation drives us to carry out a comprehensive study aimed at systematically identifying, analyzing and classifying the security attacks in the host layer.

A mapping study provides systematic and objective procedure for identifying the nature and extent of the empirical study data that is available to a specific research domain. The mapping process consists of the activities searching for relevant publications, definition of a classification scheme and mapping of publications.

INTERNET INFRASTRUCTURE ATTACKS

Attacks on the Internet infrastructure can lead to more destruction because different components have implicit relationship with each other. To provide solution for these attacks, Internet infrastructure attacks are broadly classified into the below four categories (Gayathri & Neelanarayanan, 2013):

- DNS Hacking,
- Route table poisoning,
- Packet mistreatment,
- Denial of Service.

The attacks are classified according to the above major category. Few of the attacks are listed below:

- Interruption,
- Modification,
- Fabrication,
- Replication,
- Link state,
- Distance vector,
- Interruption.

The impact caused only by the major attacks and general solution measures are tabulated. In this survey, all possible solutions are not provided related to the real time scenario. The attacks considered are restricted to types of DDoS, packet mistreating and link state attacks. The vulnerabilities caused by each attacks and its corresponding impact are not considered.

Present data security (Chakrabarthi & Manimaran, 2002) measures ensure confidentiality and integrity of data. Various solutions and drawbacks are identified in this survey specific to the transport and network layers. Major components in this analysis process are: