Chapter 7
Framework for Threat Analysis and Attack Modelling of Network Security Protocols

Nachiket Athavale
Kashibai Navale College of Engineering, India

Shubham Deshpande
Kashibai Navale College of Engineering, India

Vikash Chaudhary
Kashibai Navale College of Engineering, India

Jatin Chavan
Kashibai Navale College of Engineering, India

S. S. Barde
Kashibai Navale College of Engineering, India

ABSTRACT

Nowadays everything is computerized including banking and personal records. Also, to boost business profits, businessmen have changed their way of operations from physical way to electronic way, for example Flipkart. But as these developments benefit the developer they also increase the chance of exposing all of customer's personal details to malicious users. Hackers can enter into the system and can steal crucial or sensitive information about other authentic users and in case of banks leads to frauds. Security thus, becomes an important issue for all companies and banks. Intrusion detection systems help such companies by detecting in real time whether an intrusion is carried on or not. Here the authors are developing a signature based intrusion detection system which will scan incoming packets and send a warning message to system administrator. Also, the authors are implementing a framework and provide it to all the users so that developing intrusion detection based system similar to ours. The advantage of using framework is that it can be upgraded and re-defined whenever it is needed.

DOI: 10.4018/978-1-5225-9866-4.ch007

INTRODUCTION

Computers have revolutionized all sectors and fields of our society. All physical documentation has been replaced with computerized documents. For the convenience of customers, banks have offered online banking services, businessmen keep crucial data about their products on computers and online shopping are just some of the examples of the benefits of computers and Internet. But the rise in computerization also gave rise to people becoming skilled in stealing this crucial data for personal or financial reasons. Several measures have been developed to stop this virtual thief from stealing their crucial data. But for administrators to stop attacks they have to know whether an attack is taking place or not. And for that an Intrusion Detection System is necessary.

Now what an Intrusion Detection System will truly do is scan incoming network packets and match them with fixed patterns of well-known attacks to find if detection has taken place or not. The system will also find IP Address of the attacking individual's device if it is in the network. Different companies have different architectures and set up and might have specific attacks to deal with. So, these companies might want to develop their own Intrusion Detection Systems. Taking this thought forward the authors are going to develop a framework, an open source project which might be further developed by anyone however they might wish and for whatever purpose.

So, with the rise in computer age, malicious people also started to use their skills to steal crucial data and to counter them a system which detects when an attack occurs and informs network administrator. Also, the system will be a framework which can be enhanced and modified according to people's choice.

MOTIVATION

With advancements in the technology, most of the tasks that were supposed to be done by humans are now getting done by computers. Such evolution has begun a new era wherein everything is computerized including day-to-day tasks. To boost the performance organizations have changed their way of doing operations from physical way to digitization. Banking systems provides various ways with which a user can communicate with the bank from any remote location. User can transfer, deposit money with just a click.

Also, a user can access his confidential information from any location. However, this increases the chance of misusing the intellectual data by breaching the security by hackers. With technology evolutions, it becomes difficult to maintain user's intellectual information safe as it may be stored at remote locations. So, securing such remote storage from hackers becomes an ultimate goal for the organizations. Hackers or attackers can enter into the system and steal the information or can manipulate the sensitive data. Hackers make use of various techniques with which they can enter into the system illegally and achieve their goal. In sensitive areas like banking security is of great importance, because if someone hacks the net-banking passwords then he can do whatever with the account. Security thus becomes the most important issue in such sectors.

Developing a perfect secured system is not possible, because:

- Most of the security systems have some limitations
- Possibility abuses by privileged users inside the organization
- Not all kinds of intrusions are known
- A system cannot detect all types of attacks fully