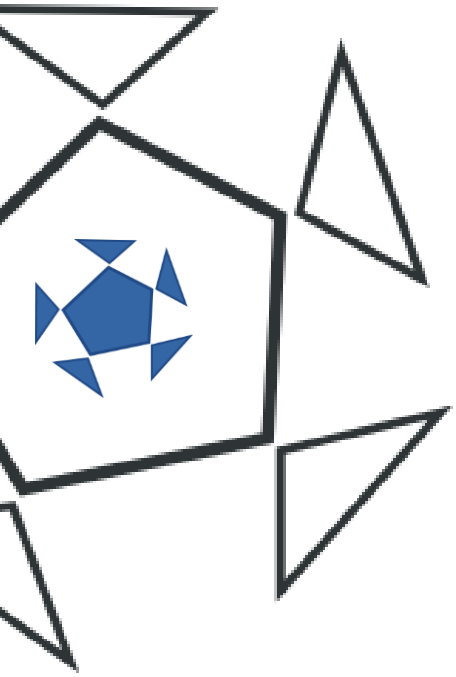
Raza's Simplified

# Chapter 8



# SECURITY

In this Chapter

- Introduction
- Components of Security

# Introduction

An OS takes care of security and protection of assets. Assets include hardware and software. OS contains many routines to protect files, data, devices, processes, memory, network connections and OS itself. All these are protected from unwanted intervention from other processes.

For a system, a protection mechanism is defined. This protection mechanism applies given protection policies.

The protection policy can be defined at two levels:

- Within the OS
- By the network administrator

Here, an important thing is to be discussed that security is not always fool proof. It always contains some weaknesses. The task of an attacker is to find that weakness and then exploit it. Task of system admin is to find that weakness and remove it or apply a solution for it.

We cannot implement a very rigid and strict security policy and methods. Doing so will not allow users to work freely. They will remain busy in authenticating themselves.

Similarly, OS cannot have a very light or loose policy. It will allow unauthorized people to gain access into our systems.

We must find a balanced security policy. This policy should allow the users to work freely and deny any unauthorized access or action.

The level to which the system's resources are always protected as described in protection policies is called its security level.The steps taken to manage the threats and dangers to the protection policies are called security measures.

# Components of Security

Following components are included as part of security:

1. Authentication

2. Prevention
3. Detection
4. Identification
5. Correction

## Authentication

Authentication means to recognize the user and its rights in the system.

So, basically it means to identify the identity of the user. This user may be running a process on a given system or he may be doing some other tasks.

An OS uses some special information to recognize a user. This information is expected to be known only by that user. A user can use different types of information for this purpose.

For example, user's account number, name, date of birth, phone number, pet's name, etc.

But such information is not secret. For example, many people would be aware of one's date of birth. So, it is not useful to base recognition on such type of public information. We need some private information, known only to the user, to have a practical authentication system.

### *Use of Passwords as Part of Authentication*

Passwords are the most popular way to authenticate a user. They are actually a confidential piece of information known only to the user and the system. A system stores users' passwords in a secure way after encrypting it.

1. Characteristics of a password
2. A password is formed by using different symbols.
3. A password should be formed by combining letters, special characters and numbers.
4. It should be long enough. Many systems put a limit on password length. For example 8 or 10 characters.

5. It should be fairly complex. Complexity can be increased by including different combinations of characters.
6. Passwords should be case sensitive.
7. Many people make a password by shortening a long sentence. For example, if their sentence is 'This is a sample sentence no. 2', the password will be 'Tiass#2' or 'Tiassn.2'.

### *Using One Time Passwords*

Such passwords are used one time for authentication. At the next login, a new password must be provided. In this way, if an intruder has guessed the password in anyway, he still cannot use it.

Such authentication systems are based on a seed value and a function. The seed value is an input to the function. The function takes this value and calculates a result.

The user is also aware of the function and user is provided with the seed value. Seed is generated randomly so no one knows which value will be provided the next time. User applies the function to the seed on his own and enters the result into the system. If both result match, the system authenticates and logs the user in. Otherwise, login is denied.

For example, suppose the function is $x^2$ where x is the seed. At a login request by a user, the generated value of x (seed) is 2. Then the user must enter 4 to login, because $2^2=4$.

The function must be complex and it must be kept secret.

### *Smart Cards*

Many systems require the users to swap a smart card through a scanning machine. These machines authenticate a user on the basis of both smart card and the password. Sometimes password is also called passcode. User enters the passcode and it is given to the card. Then the card performs calculation on the basis of current time and the passcode. The result is presented to the machine as a password. The authenticating machine also performs the same calculation

and compares it with that of the card. If both results are same, the login is granted. An attacker will need both passcode and the card to gain entry into the system.

## *Weaknesses, Vulnerabilities and Threats for Passwords*

### Password Theft

It means that an unauthorized person becomes aware of our password.

People can become aware of your password simply by looking at the keys being pressed while entering the password in the system.

Many users write their passwords so that they don't forget it. But the paper containing the password is dropped somewhere or is stolen by someone. Sometimes, they leave the paper in their drawer or they write it on the back of their keyboard. All this makes password theft an easy thing.

An attacker who knows you personally may try your favorite words, name of your pet, or model of your car.

On the other hand a malicious program called **sniffer** is installed on the network by some cracker. It keeps tracking the transmitted data and copies the usernames and passwords when they are transmitted to its database over the network.

#### Solution

1. A password must not be easily guessable. Do not use your date of birth, name of spouse, model of car or other public information as a password.
2. Passwords should be changed regularly. Set a time period and change the password after every expiry of that time.
3. Always keep your password secret. Never write it somewhere. Never tell it to someone.
4. If you have to tell someone your password, then change it immediately.
5. Never use the same password on more than one systems. If you do that, and one password on one system is disclosed to someone with bad intentions, then the other systems will also be compromised.

6. Hide your keyboard while you are typing the password. Never let others allow guess the password with the movement of your fingers. You can ask them gently to excuse you while entering password.

## Brute Force Attack

It is a very successful password guessing method. A cracker links with a password protected system and runs an application. This application tries to guess password by trying every possible combination of characters. If a computer can try one combination every millisecond, then it can try about 8.5 million passwords in a day. In a day such a machine can guess all 6 digit passwords. It will take about a month to try all passwords with only lower case English alphabets. If we increase the length of password, the likelihood that it will be guessed easily decreases.

Usually, if there are 100 combinations to try, then there is a 50% chance that the password is in first 50 combinations.

### *Solution*

A simple and effective way is to limit the failed login attempts. And after that, lock or disable the account. We find it in all modern systems, Google, ATM machines and Facebook allow only limited number of failed attempts and after this the account is locked. ATM machines do not even eject back the card. Now even if the user enters the correct password, it is rejected. User must go to the administrator and ask for account reactivation.

## Physical Authentication

Many times, the authentication systems based on passwords are not suitable. In such situations, we use some physical gadgets to recognize a user.

But to be effective, the user using such gadgets must have physical access to the system.

Such gadgets include keys or access cards. They can be stolen. The advantage is that the system will not need to remember passwords. The stolen items can be deactivated.

The authentication can also be done on the basis of unique physical characteristics of a user.

1. Retina scanners scan the eye retina of the user.
2. Finger print and full hand scanner can scan the lines on palm.
3. Facial recognition software can recognize a user on the basis of its face.
4. Voice patterns are also used to recognize a user.
5. In future, there will be some systems which would note even the typing pace of the user to recognize him.

## Prevention

Prevention means to take measures before an intruder bypasses the security to gain access into the system. Entering a system is called penetration and a program entering a system is called an intruder.

Many steps are taken to prevent intrusion. These steps are called preventive measures. Following is a list of such measures:

a. Before creating and applying a password, it should be checked for complexity and length and only those passwords should be allowed to be used which qualify a reasonable criteria. Many systems have built in authentication modules which check the passwords against certain criteria before setting them. They also check for repeating patterns in the passwords and make history of used passwords.

b. Passwords should be changed at regular intervals. In case of any suspicion, password should be changed immediately.

*c.* Data should be encrypted. *Encryption means to change the form of data according to some set method*. Encryption can be applied when data is stored or transmitted. Many software exist which can easily and successfully encrypt and decrypt data. *Encrypted data is called cipher and decrypting it is called deciphering.*

d. From time to time, the unused and duplicated services should be closed. Such services provide a possible way of intrusion. An attacker can enter a system by exploiting such services.

e. Configure and use an internal firewall. The firewall allows or rejects access to a resource on the basis of the origin of the request.

f. Many national and international bodies exist which serve to find vulnerabilities in current systems and their remedies. You should keep in touch with them and find useful information according to your circumstances.

## Detection

*Detection means to locate damage caused by a successful attack*. It is necessary because the next step called correction can be performed only when we know where the damage has occurred. The detection is performed when the system has been compromised and the attacker was successful in penetrating the system.

Detection also avoids many possible future penetrations. It requires continuous monitoring of the system and then a system would fully recover from damage.

For this, we can use an auditing system. An auditing system keeps track of events. They record the user's activities, duration and login and logout times. While looking at such records, we can discover an unusual and suspicious activity, the user involved and its time.

Antiviruses, virus checkers and antispyware can check for an intrusion and abnormal codes in the files and programs.

A process which has been in the system active for a very long time indicates a suspicious situation.

Many software are available which can record the state of system in database. We can use them and compare the current state to detect any abnormal activity. They can be used to compare different critical system files against their states in different times.

## Correction

Correction means to recover from the damage caused by a successful penetration.

Backups are most commonly used method. Backup means an extra copy of the data maintained for the sake of recovering from a data loss. The backups should be taken regularly. They should be stored away from the production system.

Sometimes, the backup may itself be compromised. In that case, a complete restoration of the system would be needed. If a complete image of the system along

with the installed programs is available, the restoration process will be easy and simple.

All information related to system security should be reset. Passwords must be reset.

The weakness or vulnerability that allowed the previous attack to be a success must be removed. To do this, we may need to reconfigure the system, end a running service, install a patch for a system error.

# Identification

It means to find the origin of attack. It is necessary to discourage future attacks and bring the attacker to justice. It is quite a difficult thing to do.

Auditing information can be used. But sometimes an attacker interferes with auditing logs and removes the attack records.

When a network is accessed using modems, the record of every incoming call is maintained and it can be used to trace the intruder. This record is maintained against caller id.

On a network, all offered services can be provided after authenticating a user. A mail or an FTP server can refuse a request coming from an un-recognized user. So, if the mail server is found generating a virus infected email, the user causing it can be found.

## *Categorizing Threats*

Threat to computer resources can come from users or software. We categorize them according to the user or the malicious activity performed by them.

## *Categories by User/Attacker*

An attacker is a person who gains undesirable access to the system resources. He can be a hacker/cracker or an authorized user performing the harmful activities. We categorize them as follows:

a. Masquerader

b. Misfeasor

C. Clandestine user

### Masquerader

It is an unauthorized user who gets the rights of an authorized user and performs harmful activities.

### Misfeasor

This user is an authorized user. But it receives more rights than it is authorized to use, or it uses the rights for unauthorized purposes.

### Clandestine user

This user gets the rights equal to a system administrator and begins to bypass security, protection and detection mechanisms of the system.

## *Threats from Software*

Software is used by the hackers and crackers to gain access to the systems. Badly designed software with inappropriate settings can perform destructive actions.

Hackers also make their own software and use them to perform illegal operations.

Following is a list of different types of malicious software. But not all people agree with these definitions. They think a replicating and destructive program is a virus. Some say a malicious program of any kind is a virus. Still some others say that it is an attachable file.

## *Logic Bomb*

This is a malicious program which waits for a certain situation or condition to occur. It is like a time bomb, which does not explode until its timer gives a signal.

For example, a logic bomb will activate when the date is 15-Apr-2009.

Sometimes people working in some organization also install a logic bomb to avenge their management. For example, an employee who feels that he will be fired soon from the organization would install a logic bomb on the salary processing system. This bomb would activate when the name of the employee is not in the monthly payroll, indicating he is fired and so destroying all data on that system.

## *Trojan Horse*

This program shows something useful to the user and performs a dangerous action in the background. Many Trojans perform destructive actions directly. Many times they destroy the system in background.

Normally, Trojans steal information. For example, they would display a clock on desktop but silently would take the login information to the author of the Trojan.

### *Worm*

These types of programs attack systems on network. They replicate on the victim and also try to find other systems and upload themselves there. The worms find a bug in the networking software and exploit it. They find some sort of remote execution command and execute themselves through it. Then the worms try to break the passwords of other machines and login to remote computer. They continue to discover new system on network using the account lists.

### *Virus*

A virus is a malicious program which performs harmful activities and also tries to replicate itself as much as possible.

This word has become a norm and people call every type of malicious program a virus.

A virus can destroy data, format disks or direct an illegal operation.

Virus attaches to an executable file, macro, OS file or can reside in boot sector.

Viruses are much dangerous for DOS and windows if the OS files are allowed to be altered by the users.

### *Bacteria*

These types of programs do not do any harmful action. But they duplicate themselves and reside everywhere in system memory. As a result, the hosts run out of memory and denial of service results. This situation is called DoS attack.

### *Trap Door*

This is a point in the system left by a previous attacker or by the developer to invade the system in future. The regular security mechanisms are ignored and the attacker logins to perform malicious actions.

On systems running UNIX, some attacks were a success due to the trapdoors involved. The attacker replaced the original login system with its own login system. This new login system was able to log in again the attacker when the

user name is 'toor', which is the reverse of 'root'. The toor then got the rights of superuser and performed whatever the attacker liked.

### *Stuxnet*

This virus is known to be the first virus used in warfare. It is reported that it was used against nuclear assets of Iran by Israel and destroyed one of her nuclear facility.

This virus especially targets the production machinery developed by Siemens and overrides security protocols of it. This machinery was in use by the Iran so the virus was a success.

For more info, visit;

http://en.wikipedia.org/wiki/Stuxnet