E-Content of
INTERNET TECHNOLOGY AND WEB DESIGN

Chapter: 11.4 Internet security and Management concepts

Topic: 11.4.1 Internet security and Management concepts

Internet security and Management concepts

- In internet, as you know that we are basically connecting our computer system to another computer system.
- There is every likelihood that while doing this, some unauthorized person can also get into it and access data.
- Manipulating security becomes more important when we use computer as commercial transaction.
- User need to make sure that message are private and financial transactions are secure.

Authentication

- It is the process of determining identify of a user who is attempting to access a system.
- Also for security purpose, the verification and identify of a person or process is necessary.
- Thus, it is the verification of the user's claim of identity by passwords, personal challenge, response calculation or random password generator.

Authentication methods

- There are two primary models for token based user authentication systems.
    - One time password systems: The user token displays a “current password” which the user enters in any context that would require a conventional password.
    - The server system can calculate the password on demand and verify the authentication request.
    - Challenge/ Response systems: The user first receives a challenge generated by the authentication server.
    - The challenge is then copied by the user into his token.

  - ➢ The token then calculate and displays a response which depends on the challenge.
  - ➢ The user then copies this response back into the application prompting for authentication information.

- The server system calculates the expected response and compares with the response submitted by the user.
- Since challenges are generated random by the server, attacks associated with replaying authentication information are an issue for well-designed system.
- As the result, the server does not need to retain the information regarding which “passwords” have been used.
- Some of the authentication methods are given in the following subsections.

Passwords

- Passwords are the most common form of computer security.
- Some networks require multiple level of passwords to gain access to various servers or databases.

Callback

- Call is a security feature that works like when a user dials into a communication server and enters the user name and password.
- The communication server then hangs up the modem connection, searches its database to authentication the user and then calls the user back at a pre-defined number.

Packet Filters

- Packet filters allow network administrators to limit a user's access to specific services on the network.
- For example, a user may allowed to send electronic mail but not copy data files from the network.

Authentication servers

- They can be set up in variety of ways, depending on the security scheme of the network they are serving.
- The basic process of authenticating a user includes the following steps:

- A user dials into a network through a communication server or Network Access Server (NAS).
- The NAS forwards the user identification and password to the Authentication server.
- Then the authentication server validate the user and provides access privileges to the network.

RADIUS (Remote Authentication Dial-up User Service)

- RADIUS is a system of distributed security that solves the problems associated with meeting the security requirements of remote computing.
- The solution eliminates the need of hardware and provides access to a variety of state of the art security solutions.
- Distributed security separates user authenticated data and authorization from the communications process and creates a single central location for user authentication data.
- RADIUS is freely available distributed security system developed by Lucent Technologies.
- RADIUS provides an open and scalable client-server security system.

Authorization

- Authorization is the process of determining how an authenticated user is permitted to use specific resources.
- An authorization mechanism automatically enforces a management policy regarding resources object use.
- For example, in a computer system, resources typically includes data files, operator commands, transaction I/O devices and program process.
- The specific rules for authorizing access to data objects usually enforce confidentiality and integrity by either granting or denying access to read, modify or create data records and by controlling the creation or deletion of data objects.
- While authentication control who can access network resources, authorization says what they can do once they have access the resources.
- Authorization grants privileges to processes and users.

- Authorization lets a security administrators control part of a network, for example, directories and files on servers.

Auditing and Accountability

- Auditing is the process of data collection and analysis that allows administrators and others, such as IT auditors, to verify that the users and authorization rules are producing the intended results are defined in a company's business and security policy.
- Individual accountability for attempts to violate the intended policy depends on monitoring relevant security events, which initiates the auditing feedback reporting loop.
- The monitoring process can be implemented as a continuous automatic function, as an occasional verification that proper procedures are being followed.
- The auditing information may be used by security administrators, internal audit personnel, external auditors, government regulatory officials and in legal proceedings.
- To effectively analyze the security of a network and to respond to security incidents, procedures should be established for collecting network activity data.