CS381 Exercise 16

Name: Zhang Yupeng

Student ID: 5130309468

1. What is the purpose of access control?

Solution:

Access control refers to exerting control over who can interact with a resource. It decide what you are allowed to do, the focus of access control is policy.

The goal of access control is to protect resources from unauthorized access.

2. Describe the different methods of access control

Solution:

1. **Access matrix:**

   It contains a set of subjects S, a set of objects O, a set of rights R.

   It has one row for each subject and one column for each subject/object, the elements are right of subject on another subject or object.

2. **ACL:**

   ACL is an access control associated with the resource. It can prevent and revoke access, however, it cannot limit or grant access.

3. **Capability list:**

   Capability list is an access control associated with the user. It can prevent, limit and grant access. It can revoke but not likely expected.

3. Describe the different types of firewall

Solution:

1. **Packet Filtering Firewall:**

   This kind of firewall apply a set of rules to each incoming and outgoing IP packet and then forwards or discards the packet. Filtering rules are based on information contained in a network packet including

source IP address, destination IP address and so on.

It's simple, transparent and fast, however, it do not examine upper-layer data and has limited logging functionality. It do not support advanced user authentication schemes. Moreover, it's vulnerable to attacks and exploits that take advantage of problems within the TCP/IP specification and protocol stack. It's susceptible to security breaches caused by improper configuration.

2. **Application-level gateways:**

   This kind of firewall is a gateway that is configured to be a web proxy will not allow any ftp, gopher, telnet or other traffic through. It acts as a relay of application-level traffic.

   The advantage of it is that it's more secure than packet filters and only scrutinize a few allowable applications. It's easy to log and audit all incoming traffic at the application level. However, there is additional processing overhead on each connection.

3. **Stateful Inspection Firewalls:**

   Stateful packet filters examine each IP packet in context: it keep track of client-server sessions and check each packet validly belongs to one, hence, they are better able to detect bogus packets out of context. This kind of firewalls allow incoming traffic to high-numbered ports only for those packets that fit the profile of one of the entries in the directory

4. **Circuit-level gateways:**

   This kind of firewalls setup two TCP connections: one is between itself and a TCP user on an inner host, the other is between itself and a TCP user on an outside host.

   Once created, it usually relays traffic without examining contents and typically used when trust internal users by allowing general outbound connections.