1. (12pts) Construct an access matrix for the following case. There are three users (Cartman, Butters, and Public) that own the files (o1, o2, and o3, respectively). An owner can read and write his own file. Cartman and Butters do not want Public or each other to read anything that they write, whereas Public allows everyone to read his file.

a. Draw the access matrix. Fill in the access matrix with the maximal number of read permissions possible for the three files.

b. Suppose we want to implement this model using (1) an ACL, (2) a capability list (C-list). Show what the lists look like.

c. List two advantages of ACLs over C-lists and two advantages of C-lists over ACL.

(a)

|  |  |  |  |
| --- | --- | --- | --- |
|  | O1 | O2 | O3 |
| Cartman | Own  rwx | x | rx |
| Butters | x | Own  rwx | rx |
| Public | x | x | Own  rwx |

(b)

ACLs:

|  |  |
| --- | --- |
|  | O1 |
| Cartman | Own, rwx |
| Butters | Own, x |
| Public | Own, x |

|  |  |
| --- | --- |
|  | O2 |
| Cartman | x |
| Butters | Own, rwx |
| Public | Own, x |

|  |  |
| --- | --- |
|  | O3 |
| Cartman | rx |
| Butters | rx |
| Public | Own, rwx |

C-lists:

|  |  |  |  |
| --- | --- | --- | --- |
|  | O1 | O2 | O3 |
| Cartman | Own  rwx | x | r x |

|  |  |  |  |
| --- | --- | --- | --- |
|  | O1 | O2 | O3 |
| Butters | x | Own, r, w, x | r, x |

|  |  |  |  |
| --- | --- | --- | --- |
|  | O1 | O2 | O3 |
| Public | x | x | Own, r, w, x |

(c)

Advantages of ACLs over Capability:

Naming objects:

ACL can attempt to name any object in the system as the target of an operation. Maybe in some cases the set of the accessible objects is not bounded whereas in capability a user can only name those objects for which a capability is held. It provides the least privilege principle and the set of the accessible objects is bounded.

Overhead:

ACL has significant overhead when processing large ACLs when compared to capability.

Advantages of Capability over ACLs:

Connectivity: In capabilities we never lose the connection between why we have a permission and the action that you try to take. Permission is not based on global data, the act of presenting a capability maintains the connection between when you are trying to do and why we are trying to do it.

Controlled Access: If we want to offer precisely controlled access to sensitive things, it is easy to do in capability. In the constructor we will create an object (capability) with method permitted action that go well beyond what we want, then return another object that proxies off of the first to only expose the things that we want to know. In this manner any exact permission that we need can easily be created.

2. (8 pts) Assume a system with job positions (i.e., roles). For job position, the number of individual users in that position is and the number of permissions required for the job position is .

a. For a traditional DAC scheme, how many relationships between users and permissions must be defined?

b. For a RBAC scheme, how many relationships between users and permissions must be defined?

(a) For a traditional DAC,

- There will be only one possible relationship

(b) For RBAC, there will be U\*P relationship between users and permissions Where U -> set of individuals, P -> set of permissions required.

- P->h one or more roles of user

- or user roles -> one or more P

3. (12 pts) The high water mark principle and low water mark principle both apply in the realm of multilevel security.

(a)What is MLS?

(b)Define the high water mark principle and the low water marker principle in the context of MLS.

(c) Is BLP consistent with a high water mark principle or a low water mark principle, both, or neither? Justify your answer.

(d)Is Biba’s Model consistent with a high water mark principle or a low water mark principle, both, or neither? Justify your answer.

(a) MLS is Multilevel Security. It is a class of system that has system resources at more than one security level and that permits concurrent access by users who differ in security clearance and need-to-know, but is able to prevent each user from accessing resources for which the user lacks authorization.

(b) High water mark principle: Process starts at lowest level and raises current clearance (up to maximum) to read data with label above current clearance

Low water mark principle: The Biba model is often formulated in terms of the low water mark principle, which is the dual of the high water mark principle already discussed: the integrity of an object is the lowest level of all the objects that contributed to its creation. This was the first formal model of integrity.

(c) BLP uses high water mark principle. Because it is no read up and no write down. It means that it can’t read data from higher level and can’t write data to lower level.  
(d) Biba’s model uses low water mark principle. Biba is for integrity, no read down and no write up. It means that start at highest level, decrease as necessary on read operation. So it uses low water mark principle.

4. (12 pts) Recall that the anomaly-based IDS example presented in the slides is based on file-use statistics. The expected file use percentages (the Hi values in the Table are periodically updated, which can be viewed as a moving average)

(a)Why is it necessary to update the expected file use percentages? (3pts)

(b)When we update the expected file use percentages, it creates a potential avenue of attack for Trudy. How and why is this the case? (3 pts)

(c) Suppose that at the time interval following the results in the second update of the table in the slides, Alice’s file use statistics are given by A0=0.05, A1=0.25, A2=0.25, and A3=0.45. Is this normal for Alice? Compute the updated values of H0 through H3. (4 pts)

Solution:

a)It was clearly stated the values must significantly change over time otherwise more number of false alarms would have come. If it changes always, risk from attackers also get reduced.

b) Even though we update the expected use file percentages, that means trudy changes the values the alice doesn't far from his behaviour. For example at some point alice may access file 1 and trudy is slightly less than alice values, but may for accessing second file trude may access because of high rate values, at some point any one either alice/trude, one of them mat restricted to only one file so that anomaly detector may become normal any one of them. So that's why potential avenue of attack for trudy happens.

c) Yes, as values are increasing. It is normal for alice.

H0=0.10, H1=0.38, H2=0.364,H3=0.156

5. (6pts) List the four goals of IDS systems.

Detect a wide variety of intrusions;

Detect intrusions in a timely fashion;

Present the analysis in a simple, easy-to-understand format;

Be accurate;

6. (8pts) Explain the two types of IDS systems by approaches and list two advantages of one against the other.

Two types: Signature-based IDS and Anomaly-based IDS.

Advantages of Signature-based IDS: Simple; Detect known attacks; Know which attack at time of detection; Efficient (if reasonable number of signatures)

Disadvantages of signature detection: Signature files must be kept up to date; Number of signatures may become large; Can only detect known attacks; Variation on known attack may not be detected

Advantages of Anomaly-based IDS: Chance of detecting unknown attacks; May be more efficient (since no signatures)

Disadvantages of Anomaly-based IDS: cannot be used alone; Must be used with a signature detection system; Reliability is unclear; May be subject to attack; Anomaly detection indicates something unusual; Lack of specific info on possible attack.

7. (9 pts) Explain the same origin policy (3pts) and how it is exploited by cross-site scripting (XSS) attacks (6pts).

SOP is the basic security model enforced in the browser. It permits scripts running on pages originating from the same site to access each other's methods and properties with no specific restrictions, but prevents access to most methods and properties across pages on different sites. The "origin" is defined using the domain name, application layer protocol, and (in most browsers) TCP port of the HTML document running the script.

A JavaScript program can only access data for the current web site. However, according to SOP，JavaScript from a site can access that site’s cookies. Because of the XSS bug, the JavaScript from that site contains malicious code. It can therefore steal cookies and send them to some other site, via (say) an IMG URL.

8. (8 pts) Explain what is SQL Injection attack and why it can happen?

SQL Injection refers to an injection attack wherein an attacker can execute malicious SQL statements (also commonly referred to as a malicious payload) that control a web application's database server.

The reason of SQL injection: During the process of program development, we do not pay attention to the specification of writing SQL statements and filtering special characters. As a result, the client can submit some SQL statements through global variables POST and GET.

9. (10pts) Firewall concepts.

(1) List the three types of firewalls and describe their differences (e.g., locations in network stack, content they look at)

(2) Compare these firewalls in terms of advantages and disadvantages.

(1) Packet Filter works at network layer. It filters based on Source IP address, Destination IP address, Source Port, Destination Port, Egress or ingress and Flag bits (SYN, ACK, etc.) And it used two default policies. The first one is discard: prohibit unless expressly permitted. The second one is forward: permit unless expressly prohibited.

Stateful Packet Filter adds state to packet filter. It operates at transport layer. It could remember TCP connections and flag bits. And it can also remember UDP packets (e.g., DNS requests).

Application Proxy looks at incoming application data. It works at application layer. It verifies that data is safe before letting it in.

(2) Packet Filter advantage is good performance. Its disadvantages are there is no state in it and it also doesn’t know the application data.

Stateful Packet Filter could remember TCP connections and flag bits. Its disadvantage is that it cannot check the application data. Moreover, it is slower than the Packet Filter.

Stateful Packet Filter could verify that data is safe before letting it in. But its disadvantage is speed.

10. (15pts) Understand firewall rules. SMTP (Simple Mail Transfer Protocol) is the standard protocol for transferring mail between hosts over TCP. A TCP connection is set up between a user agent and a server program. The server listens on TCP port 25 for incoming connection requests. The user end of the connection is on a TCP port number above 1023. Suppose you wish to build a packet filter rule set allowing inbound and outbound SMTP traffic. You generate the following rule set:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Rule | Direction | Src Addr | Dest Addr | Protocol | Dest Port | Action |
| A | In | External | Internal | TCP | 25 | Permit |
| B | Out | Internal | External | TCP | >1023 | Permit |
| C | Out | Internal | External | TCP | 25 | Permit |
| D | In | External | Internal | TCP | >1023 | Permit |
| E | Either | Any | Any | Any | Any | Deny |

a) Describe the effect of each rule.

b) Your host in this example has IP address 172.16.1.1. Someone tries to send e-mail from a remote host with IP address 192.168.3.4. If successful, this generates an SMTP dialogue between the remote user and the SMTP server on your host consisting of SMTP commands and mail. Additionally, assume that a user on your host tries to send e-mail to the SMTP server on the remote system. Four typical packets for this scenario are shown:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Packet | Direction | Src Addr | Dest Addr | Protocol | Dest Port | Action |
| 1 | In | 192.168.3.4 | 172.16.1.1 | TCP | 25 | ? |
| 2 | Out | 172.16.1.1 | 192.168.3.4 | TCP | 1234 | ? |
| 3 | Out | 172.16.1.1 | 192.168.3.4 | TCP | 25 | ? |
| 4 | In | 192.168.3.4 | 172.16.1.1 | TCP | 1357 | ? |

Indicate which packets are permitted or denied and which rule is used in each case.

c) Someone from the outside world (10.1.2.3) attempts to open a connection from port 5150 on a remote host to the Web proxy server on port 8080 on one of your local hosts (172.16.3.4) in order to carry out an attack. Typical packets are as follows:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Packet | Direction | Src Addr | Dest Addr | Protocol | Dest Port | Action |
| 5 | In | 10.1.2.3 | 172.16.3.4 | TCP | 8080 | ? |
| 6 | Out | 172.16.3.4 | 10.1.2.3 | TCP | 5150 | ? |

Will the attack succeed? Give details.

(a) Simple mail transfer protocol (SMTP) is used to transfer the mail between hosts through transmission protocol (TCP).

TCP connection set the connection between the user agent and server program.

Rule A: Rule A is defines the Remote host receiving the incoming email from external server, it permits the inbound SMTP connection.

Rule B: Rule B is defines the External server receiving the incoming email from remote host, it permits the inbound SMTP connection.

Rule C: Rule C is defines the External server transmits the outgoing email to remote host; it permits the Outbound SMTP connection.

Rule D: Rule D is defines the Remote host transmits the outgoing email to External server; it permits the Outbound SMTP connection.

Rule E: Rule E is defines the direction as either “In or Out” from any source address to any destination address with any destination port number. It doesn’t perform any action, So Rule E is default rule to set the action is denied.

(b) Packet Actions:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Packet | Direction | Source Address | Dest  Address | Protocol | Dest Port | Action |
| 1 | In | 192.168.3.4 | 172.16.1.1 | TCP | 25 | Permit Using Rule A |
| 2 | Out | 172.16.1.1 | 192.168.3.4 | TCP | 1234 | Permit Using Rule B |
| 3 | Out | 172.16.1.1 | 192.168.3.4 | TCP | 25 | Permit Using Rule C |
| 4 | In | 192.168.3.4 | 172.16.1.1 | TCP | 1357 | Permit Using Rule D |

(c) Typical packets actions:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Packet | Direction | Source Address | Dest  Address | Protocol | Dest Port | Action |
| 5 | In | 10.1.2.3 | 172.16.3.4 | TCP | 8080 | Permit Using Rule B |
| 6 | Out | 172.16.3.4 | 10.1.2.3 | TCP | 5150 | Permit Using Rule D |