### CMPSC 443, Homework 5

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.
2. Draw the access matrix. Fill in the access matrix with the maximal number of read permissions possible for the three files.
3. Suppose we want to implement this model using (1) an ACL, (2) a capability list (C-list). Show what the lists look like.
4. List two advantages of ACLs over C-lists and two advantages of C-lists over ACL.

**》》》**

1. Answer: (1) Fill the access matrix with the maximal number of read permissions possible for the three files.

|  |  |  |  |
| --- | --- | --- | --- |
|  | *O1* | *O2* | *O3* |
| *Cartman* | *R* |  | *R* |
| *Butters* |  | *R* | *R* |
| *Public* |  |  | *R* |

Note that it is okay (no points taken off) to show all the permissions in the table, but this question asks about read permission only.

**b.**

ACL:

*O1 O2 O3*

*Cartman: R Butters: R Cartman: R*

*Cartman: W Butters: W Butters : R*

*Cartman: Own Butters: Own Public: R*

*Public: W*

*Public: Own*

*C-list:*

*Cartman: O1/R, O1/W, O1/Own, O3/R*

*Butters: O2/R, O2/W, O2/Own, O3/R*

*Public: O3/R, O3/W, O3/Own.*

**c.**

*ACL's provide for superior access review on a per-object basis*

*C-list provides for superior revocation facilities on a per-object basis*

1. (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 .



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

>>>Answer:

* 1. In DAC, you can draw N tables (each table corresponds to one job position), where rows stand for users and columns stand for permissions. Each cell in a table represents a relationship between a user and a permission. The question is: totally how many cells do we need? The answer is



* 1. In RBAC, you can draw two tables. The first table T1 shows the relationships between users (rows) and job positions (columns), and the second table T2 shows that between job positions(rows) and permissions (columns). Now for T1, for each job position i, Ui users are defined, which mean Ui cells are not empty. Hence, the total number of relationships (i.e., non-empty cells) will be Sum (Ui) for i from 1 to N from T1. Similarly, for T2, one can derive the total number of non-empty cells are Sum (Pi) for i from 1 to N. Combining both tables, we get the result



1. (12 pts) The high water mark principle and low water mark principle both apply in the realm of multilevel security.
   1. What is MLS?
   2. Define the high water mark principle and the low water marker principle in the context of MLS.
   3. Is BLP consistent with a high water mark principle or a low water mark principle, both, or neither? Justify your answer.
   4. Is Biba’s Model consistent with a high water mark principle or a low water mark principle, both, or neither? Justify your answer.

MLS: an access control system where both system resources and subjects are assigned certain security levels, and subjects are denied/approved the access based on the security levels. (you can also use the definition in slide #27)



1. (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)
2. Why is it necessary to update the expected file use percentages? (3pts)
3. 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)
4. 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)

>>>

a. User changes over time, so if these values do not change, you will soon get many

false alarms.

b. Trudy can simply “go slow" and eventually convince the IDS that her actions are

normal.

c. In this example, S =0:118, which exceeds the threshold of 0:1 given in the book.

Therefore, this would be considered abnormal.

Please refer to the slides to compute the updated values for H0 through H3.

1. (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

1. (8pts) Explain the two types of IDS systems by approaches and list two advantages of one against the other.

>>> Misuse (Signature) detection and anomaly detection.

Signature detection:

1. Simple
2. Detect known intrusion efficiently

Anomaly detection:

* 1. able to detect some unknown intrusion (or variations of known intrusion)
  2. no need to maintain/update growing attack signatures.

1. (9 pts) Explain the same origin policy (3pts) and how it is exploited by cross-site scripting (XSS) attacks (6pts).

>>> Problem usually occurs when sites don’t sanitize user input to strip HTML

* Example: chat room (or MySpace or blog sites) that let users enter comments
* The “comments” can include JavaScript code
* This JavaScript code can transmit the user’s authentication cookies to some other site

>>>based on the same origin policy, the javascript code injected by an attacker to a website can access the cookie placed by that website

1. (8 pts) Explain what is SQL Injection attack and why it can happen?

**>>>(according to Wikipedia) SQL injection** is a [code injection](https://en.wikipedia.org/wiki/Code_injection) technique, used to [attack](https://en.wikipedia.org/wiki/Attack_(computing)) data-driven applications, in which [SQL](https://en.wikipedia.org/wiki/SQL) statements are inserted into an entry field for execution.

>>> The reason it can happen is because the server side logic has vulnerability, not checking and sanitizing user input.

1. (10pts) Firewall concepts.
2. List the tree types of firewalls and describe their differences (e.g., locations in network stack, content they look at)
3. Compare these firewalls in terms of advantages and disadvantages.

>>> (1) packet filter – network layer, inspect IP address, port number

stateful packet filter – transport layer, remember TCP connections and flag bits

application proxy - application layer, check application content (i.e., data payload)

>>> (2) packet filter – high speed but cannot see connections and data payload.

Stateful packet filter – do all packet filter can do and also keep track of connections, but slower than packet filter and cannot see data payload either

Application proxy – complete view of connections and application data, able to filter virus, but slow.

1. (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 |

1. Describe the effect of each rule.
2. 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.

1. 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.** Rules A and B allow inbound SMTP connections (incoming email)

Rules C and D allow outbound SMTP connections (outgoing email)

Rule E is the default rule that applies if the other rules do not apply.

**b.** Packet 1: Permit (A); Packet 2: Permit (B): Packet 3: Permit (C)

Packet 4: Permit (D)

**c.** The attack could succeed because in the original filter set, rules B and D allow

all connections where both ends are using ports above 1023.