MID_II SOLUTION

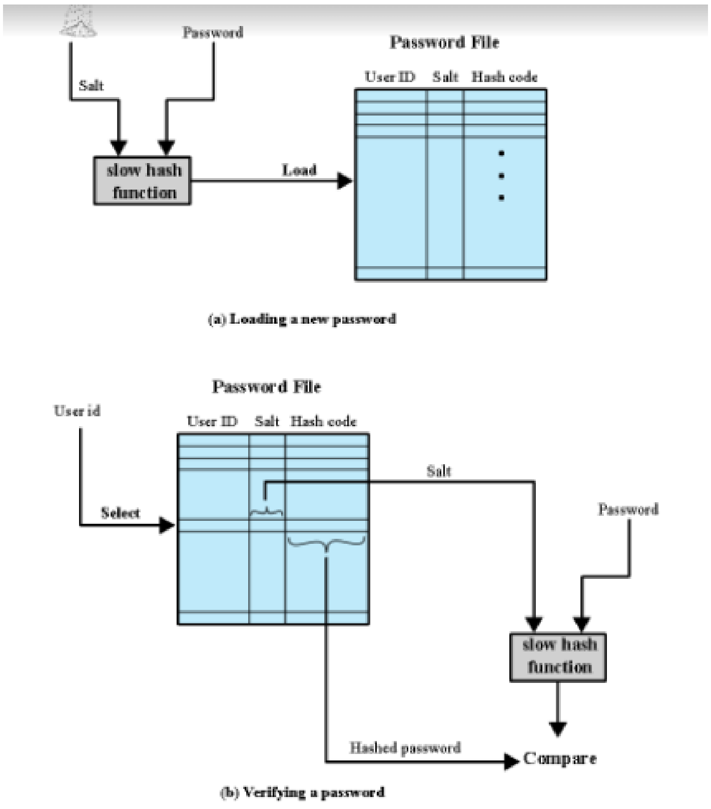
Time allowed: 60 minutes **Max. Points**: 24

Question # 1: Suppose your organization's employee management system is affected because of the employees' weak password issue. Discuss at least three types of possible password attacks, that could be the cause. **[03 points]**

1) Dictionary attacks
2) Rainbow attacks
3) Brute force attacks
4) Other related attacks

And their details.

Question # 2: Illustrate Unix Password Scheme with the help of a diagram. **[03 points]**

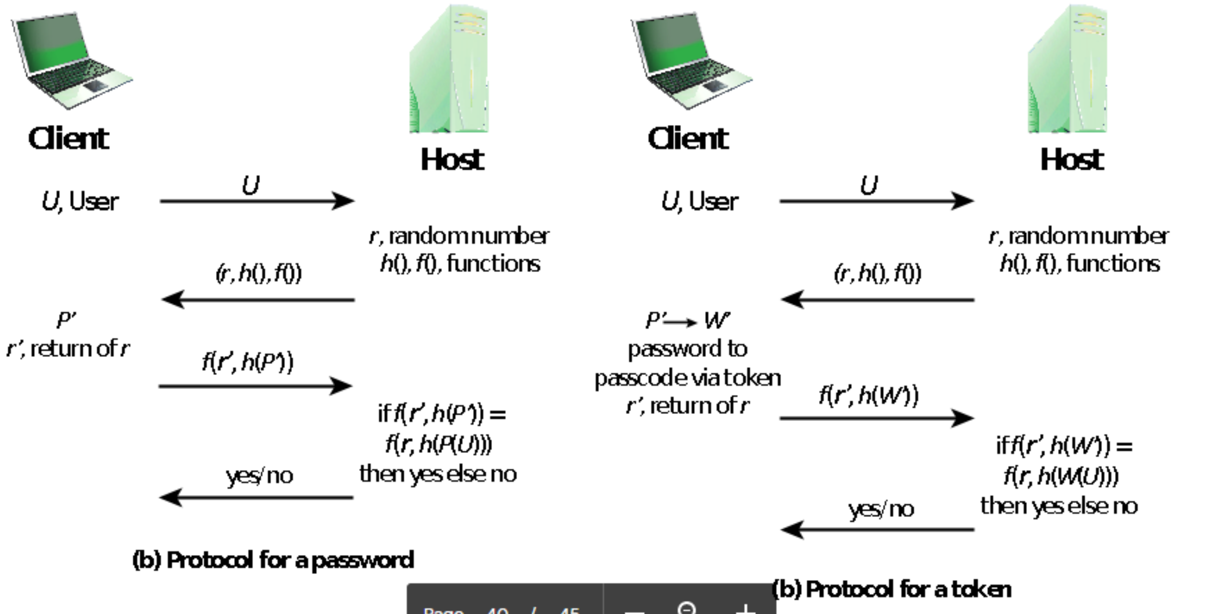


(a) Loading a new password

(b) Verifying a password

Figure 3.3 UNIX Password Scheme

Question # 3: Illustrate Challenge-response protocol for remote user authentication with the help of a diagram. **[03 points]**



<u>Question # 4</u>: Explain the SQL injection attack avenues "Second order Injection". **[03 points]**

Second-order injection: Second-order injection occurs when incomplete prevention mechanisms against SQL injection attacks are in place. In second-order injection, a malicious user could rely on data already present in the system or database to trigger an SQL injection attack, so when the attack occurs, the input that modifies the query to cause an attack does not come from the user, but from within the system itself.

<u>Question # 5:</u> Why and where you need to have database encryption? **[03 points]**

Database encryption is a process to convert data in the database to "cipher text" (unreadable text) using an algorithm. You need to use a key generated from the algorithm to decrypt the text. The database encryption process is highly recommendable, especially for businesses dealing with financial, health care, or e-commerce. Recently cyber attacks, data theft, or data breaches have been rampant; therefore, there is an increasing concern over private data. People are very aware of data privacy, security and want their data to be protected and used only when required.

<u>Question # 6:</u> An example of cascaded authorizations phenomenon is shown in Figure 1. Suppose Chris revokes the right of David, redraw the figure to show the effects and explain your answer. **[03 points]**

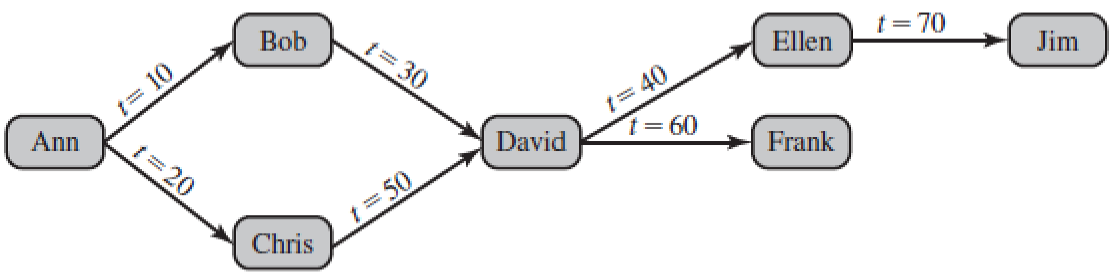
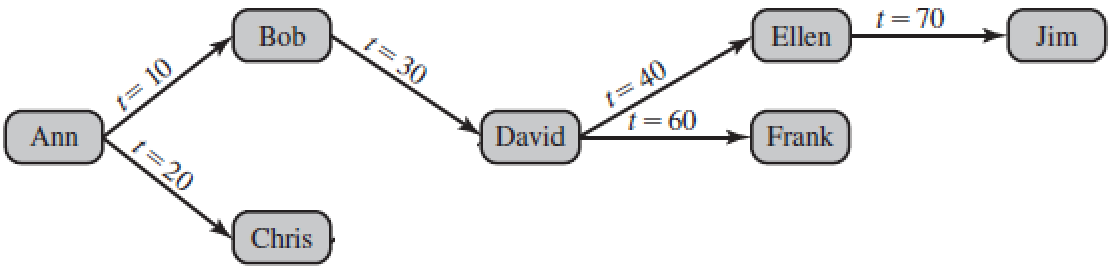


Figure 1: Cascaded Authorizations

SOLUTION:

1) As Ellen got right from David before David got right from Chris, Ellen's chain remain as it is.

2) After revoking right of David from Chris, the right of David from Bob is still there, hence, Frank remains as it is.
3) The resulting diagram is shown below:



Question # 7: The following SQL statement is sent to the database to add a new user to the database, where the content of the $name and $passwd variables are provided by the user, but the EID and Salary field are set by the system. How can a malicious employee set his/her salary to a value greater than 80000? **[03 points]**

```
$sql = "INSERT INTO employee (Name, EID, Password, Salary)
      VALUES ('$name', 'EID6000', '$passwd', 80000)";
```

SOLUTION:

Let's assume the user wants username as john and password as iheartburgers. By setting $name to john and $passwd to iheartburgers', 2000000)# a malicious employee can set his/her salary to 2Million

Question # 8: You are a security expert and are asked to train the company's IT staff about virus components and phases (malware). Precisely discuss how would you explain these concepts to the staff. **[03 points]**

A computer virus has three parts. More generally, many contemporary types of malware also include one or more variants of each of these components:
- **Infection mechanism:** The means by which a virus spreads or propagates, enabling it to replicate. The mechanism is also referred to as the **infection vector**.
- **Trigger:** The event or condition that determines when the payload is activated or delivered, sometimes known as a **logic bomb**.
- **Payload:** What the virus does, besides spreading. The payload may involve damage or may involve benign but noticeable activity.

During its lifetime, a typical virus goes through the following four phases:
- **Dormant phase:** The virus is idle. The virus will eventually be activated by some event, such as a date, the presence of another program or file, or the capacity of the disk exceeding some limit. Not all viruses have this stage.
- **Propagation phase:** The virus places a copy of itself into other programs or into certain system areas on the disk. The copy may not be identical to the propagating version; viruses often morph to evade detection. Each infected program will now contain a clone of the virus, which will itself enter a propagation phase.
- **Triggering phase:** The virus is activated to perform the function for which it was intended. As with the dormant phase, the triggering phase can be caused by a variety of system events, including a count of the number of times that this copy of the virus has made copies of itself.

Execution phase: The function is performed. The function may be harmless, such as a message on the screen, or damaging, such as the destruction of programs and data files.