Extra: Malicious Logic: Malicious Logic is a set of instructions that causes site security policy to be violated. In SCI terms this is analogous to a violation of natural laws.

Extra: Diff formal verification and Penetration Testing

Formal Verification: Preconditions – Program - Post Condition

Penetration Testing: System characteristics, environment & state – program / system – system state

Mock 4: Formal Verification: Mathematically verifying that a system satisfies certain constraint. Penetration Testing: Testing to verify that a system satisfies the certain constraint. Penetration testing is a testing technique, not a verification technique. It can prove the presence of vulnerabilities but absence of vulnerabilities.

**Consider the following situation at Annapurna (the cafeteria at M.U.M.)**

**A diner must show a badge or purchase a meal before eating at Annapurna.   
 Each diner uses a tray. If the number of trays washed in a day does not equal   
 the number of diners counted by the door checker, then somebody has cheated   
 Annapurna and eaten for free.**

**By analogy, this is an example of which of the following:**

Misuse modeling

**Consider the following policy implemented by Annapurna (the cafeteria at   
 M.U.M.)**

**A student usually accesses only the dining room and the dish room. If a student   
 is found in the kitchen this is reported (he/she may be trying to put some   
 chicken in the soup).**

**By analogy, this is an example of which of the following:**

The student here is a process. The places he/she can visit are like files and programs. Entering kitchen is like a process attempting to access file that its specification says that it shouldn’t. This is specification based modeling.

**Consider the following information about Annapurna, the cafeteria at MUM.**

**From past experience Annapurna has determined that each student on the   
 average drinks one pint of milk per day. Based on this information they budget   
 for X gallons of milk per day. If on some day, all X gallons have been used   
 before the midday meal, there is reason to suspect that someone is stealing   
 milk.**

**By analogy, Annapurna is doing what kind of modelling here?**

Anomaly modeling is statistical in nature. The phrase “each student on the average drinks one pint of the milk per day” indicates the statistical nature of this.

A system has classified and unclassified documents in it. An employee is accused of using a word processing program during the last month to secretly save copies of classified documents. Discuss if and how, each of 3 forms of intrusion detection (Anomaly, Misuse and Specification) could be used to argue against this accusation.

4

a) Users are classified into four classes. Moving information from one class to another requires approval of more than user.

**Principle of separation of privilege**

b) Each Server has the minimum amount of knowledge of the network necessary to perform its task

**Principle of least privilege**

c) In the Drib Corporation, the four servers in the DMZ zone are all on separate computers.

**Least Common Mechanism**

d) The use of write-once media in the log server. (Deny all modifications to write-once media)

**Principle of Fail-Safe defaults**

e) Configuration of firewalls should be simple so that administrators will feel comfortable doing it.

**Principle of Psychological Acceptability**

The use of write-once media in the log server. (Can't alter it and can only destroy it if they have access to the room containing the log server).

**Principle of least privilege**

**6 What do you mean by a distinguished name?** How will it look like for a person named Jack Davis who works at IBM in QA dept?

A distinguished name identifies a principal. It consists of a series of fields, each with a key and a value.

/O=IBM/OU=Quality Assurance/CN=Jack Davis/

**7 Is cryptography used in the Drib system for integrity, confidentiality, or both?** Justify

Both. Here Integrity is main concern and confidentiality is secondary with regard to updating the web server since most of the data is public and displaying on public web page (open design). Only the commercial transaction data is considered private. So cryptography is primarily used to ensure used to ensure data integrity(I,e Turdy makes no changes during transfer) and secondarily for confidentiality.

**8. Explain in short the difference between authentication and authorization.**

Authentication: Binding of a principal to a representation of identity internal to the system.

Authorization: Access control checks for resource allocation based on the assumptions that binding.

**9. In the dribble corporation, the IP address of outer firewall is x, that of the DMZ web server is y and that of the DMZ DNS server is z. Which of these IP addresses are known to the external Internet users.**

Since DMZ purely separating internal network from external network, external internet user will get IP address x.

**10. Which statistical model is likely to be used to detect someone guessing passwords.**

Threshold metric

**11a. A manipulation detection code is based on timestamps**

**False**: It is based on permission bits which included in the signature and a keyless cryptographic checksum. But not Timestamp which is used to prevent replay attacks.

**11b. The access control policy that is implemented in the internal drib network is originator controlled.**

**False:** It is mandatory: Employees do not have an ability to let users in certain user group read their files. For example: the corporate employee does not have the ability to give the customer service employee access to files that contain financial data.

11c. Vulnerability of a system increases when threats high.

**True**: Since threat is a possible danger that might exploit a vulnerability to breach security?

11d. Security logging is the analysis of records to present information about the system in a clear and understandable manner.

**False**. Security logging is the recording of events or statistics to provide system use and performance.

11e. A Programming language has no effect on whether or not a program is vulnerable to a buffer overflow attack.

**False**. Since it modifies the data beyond its buffer, the program behaves abnormally.

Buffer Overflow: A buffer overflow occurs when a program or process tries to store more data in a buffer than it was intended to hold.

|  |  |
| --- | --- |
| **Formal Verification** | **Penetration Testing** |
| **Mathematically verifying that a system satisfies certain constraints** | **Testing to verify that a system satisfies certain constraints.** |
| **Precondition: states assumptions about the system** | **Hypothesis stating system characteristics, environment and state relevant to vulnerability** |
| **Postconditions: result of applying system operations of preconditions input. Postcondition satisfies constraint.** | **Result is compromised system state. Apply tests to try to move system from state in hypothesis to compromised system state.** |
|  |  |