

**(A)** Logic Bombs (usually an insider job)

A program that performs an action that violates the site security policy when some external

event occurs

Example: program that deletes company’s payroll records when one particular record is deleted

– The “particular record” is usually that of the person writing the logic bomb

– Idea is if (when) he or she is fired, and the payroll record deleted, the company loses

all those records

Rabbits, Bacteria

A program that absorbs all of some class of resources

Example: for UNIX system, shell commands:

while true

do

mkdir x

chdir x

done

Exhausts either disk space or file allocation table (inode) space

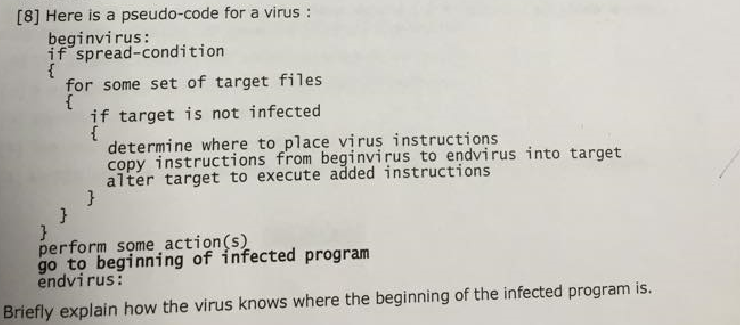
**(B)**

• Distinguish between data, instructions  
Data vs. Instructions  
• Malicious logic is both  
 – Virus: written to program (data); then executes (instructions)  
• Approach: treat “data” and “instructions” as separate types, and require certifying   
 authority to approve conversion  
 – Keys are assumption that certifying authority will not make mistakes and assumption that   
 tools, supporting infrastructure used in certifying process are not corrupt

**\*Note: need better answer**

**(C)**

**Encrypted Viruses**• A virus that is enciphered except for a small deciphering routine  
 - Detecting virus by signature now much harder as most of virus is enciphered  
 **Polymorphic Viruses (Cheaters take note!)**• A virus that changes its form each time it inserts itself into another program  
• Idea is to prevent signature detection by changing the “signature” or instructions used for  
 deciphering routine



The first phase, in which the virus inserts itself into a file, is called the insertion

phase. The second phase, in which it performs some action, is called the execution

phase.

As this code indicates, the insertion phase must be present but need not always be executed.

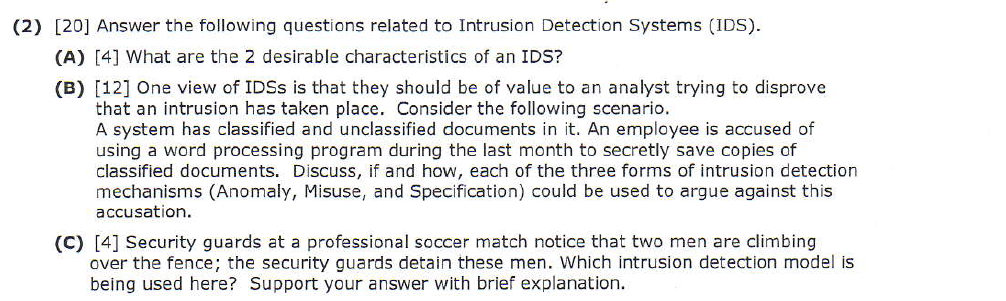
For example, the Lehigh virus would check for an uninfected boot file (the

spread-condition mentioned in the pseudocode) and, if one was found, would infect

that file (the set of target files). Then it would increment a counter and test to see if the

counter was at 4. If so, it would erase the disk. These operations were the action(s).

**\*Note: need better answer**



**(A)**

– **No anomalies**: User will process actions to conform statistically predictable pattern  
 – **No misuse**: User, process actions do not include sequences of actions that subvert the security   
 policy

**(B)**

**Anomaly detection**  
 – What is usual, is known  
 – What is unusual, is bad

Saving copies of classified documents is not unusual and there is no policy or mechanism in place to protect saving hence there is no anomaly and there is no intrusion.

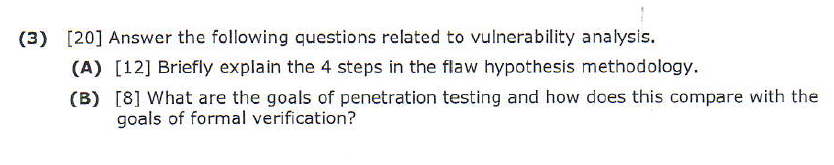
**Misuse detection**  
 – What is bad, is known  
 – What is not bad, is good  
There is no clear policy that saving copies of classified documents is bad. So the operation is not recognized as bad hence it is not misused and there is no intrusion.

**Specification-based detection**  
 – What is good, is known  
 – What is not good, is bad

There is no clear specification regarding the saving copies of classified documents if it is good or bad. Hence based on the specification there is no intrusion.

**(c)**

Specification-based intrusion detection model is used. From the model we know what is good is known and what is not good, is bad. It is known that outside men is not allowed without ticket in professional soccer match. This act is not good hench is bad. So the security guard detain these men based on Specification-based model.



**(A)**

The Flaw Hypothesis Methodology was developed at System Development Corporation

and provides a framework for penetration studies. It consists of

four steps.

**1. Information gathering**. In this step, the testers become familiar with

the system’s functioning. They examine the system’s design, its

implementation, its operating procedures, and its use. The testers become

as familiar with the system as possible.

**2. Flaw hypothesis**. Drawing on the knowledge gained in the first step, and

on knowledge of vulnerabilities in other systems, the testers hypothesize

flaws of the system under study.

**3. Flaw testing**. The testers test their hypothesized flaws. If a flaw does not

exist (or cannot be exploited), the testers go back to step 2. If the flaw is

exploited, they proceed to the next step.

**4. Flaw generalization**. Once a flaw has been successfully exploited, the

testers attempt to generalize the vulnerability and find others similar to it.

They feed their new understanding (or new hypothesis) back into step 2

and iterate until the test is concluded.

~~A fifth step is often added [935, 936]:~~

~~5. Flaw elimination. The testers suggest ways to eliminate the flaw or to use~~

~~procedural controls to ameliorate it.~~

**(B)**

**Penetration testing goals:**

- Testing to verify that a system satisfies certain constraints  
 - Hypothesis stating system characteristics, environment, and state relevant to vulnerability  
 - Result is compromised system state  
- Apply tests to try to move system from state in hypothesis to compromised system state

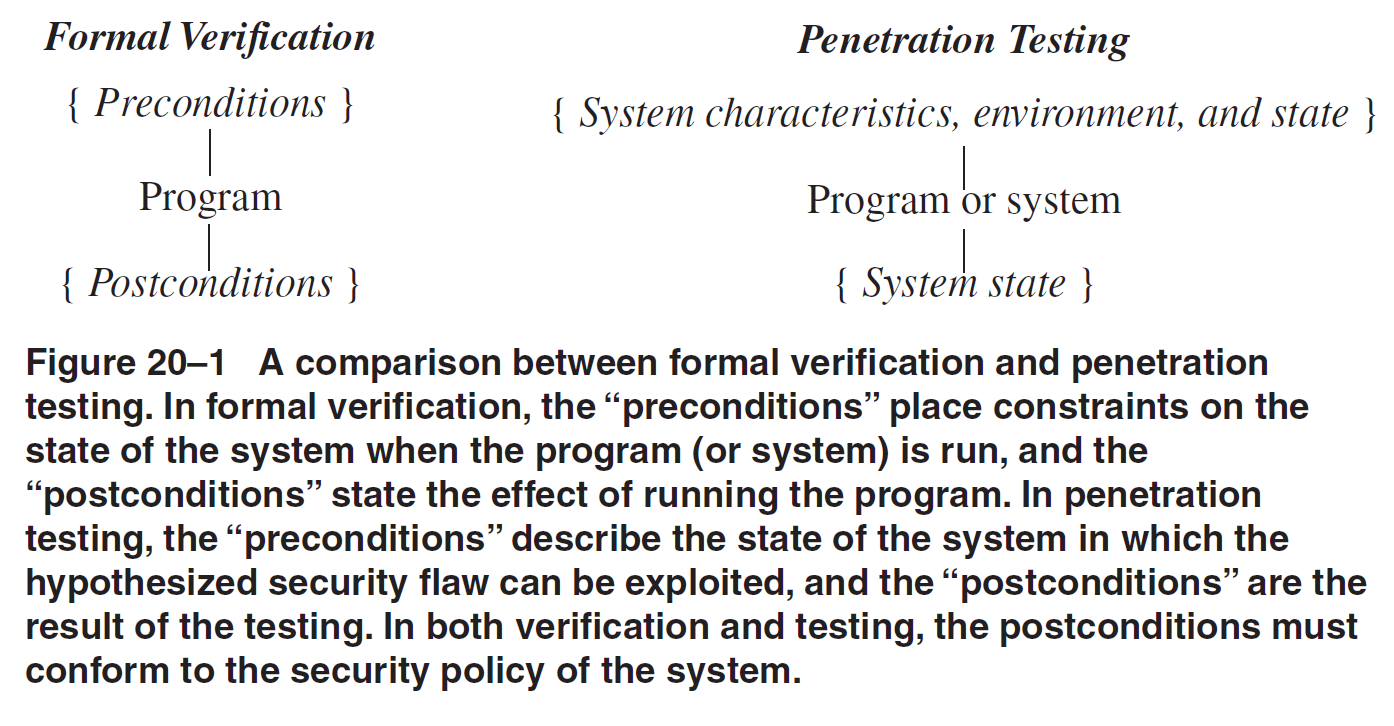
-Penetration tester had a bad day if he does not find a bug

**Formal verification**

- When tester finds a bug he had a bad day

- Mathematically verifying that a system satisfies certain constraints

- Post conditions satisfy constraints is required



~~Penetration testing is a testing technique, not a proof technique. It can never~~

~~prove the absence of security flaws; it can only prove their presence. In theory, formal~~

~~verification can prove the absence of vulnerabilities. However, to be meaningful,~~

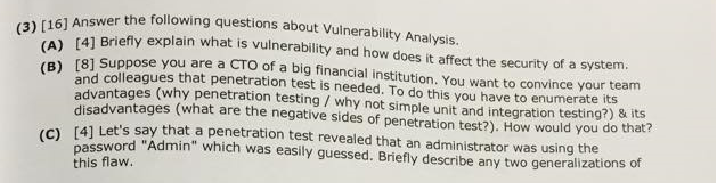
~~a formal verification proof must include all external factors. Hence, formal verification~~

~~proves the absence of flaws within a particular program or design and not the~~

~~absence of flaws within the computer system as a whole. Incorrect configuration,~~

~~maintenance, or operation of the program or system may introduce flaws that formal~~

~~verification will not detect.~~



**(A)**When someone breaks into a computer system, that person takes advantage of

Lapses in procedures, technology, or management (or some combination of these factors),

Allowing unauthorized access or actions. The specific failure of the controls is

Called a vulnerability or security flaw; using that failure to violate the site security

Policy is called exploiting the vulnerability. One who attempts to exploit the vulnerability

Is called an attacker.

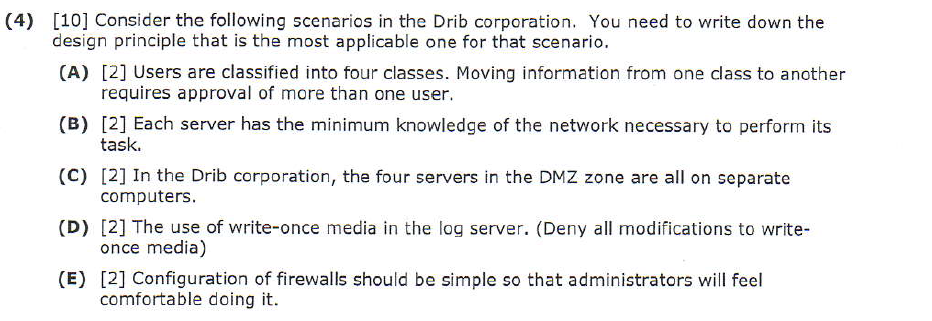
**(B)**

**(C)**

-Check other system accounts for obvious or default passwords

-Check password program to see if it allows a user to selec easy passwords to guess.

-Users of system are not properly trained (security is not a top priority for them)



(A) The principle of separation of privilege dictates that moving data from one

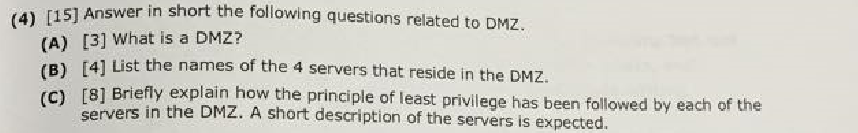
class to another requires approval of more than one user.

(B) Principle of least privilege ~~Separation of privilege~~

(C) Least common mechanism: firewall software, mail server software, DNS software are all  
on separate machines.

**(D)** Principle of Fail-Safe defaults

**(E)** Principle of Psychological Acceptability



(A) The DMZ is a portion of a network that separates a purely internal network from an external network.

(B)

-DMZ Mail server

-DMZ WWW server

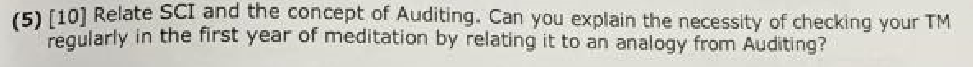
-DMZ DNS server

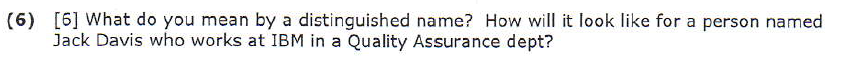
-DMZ Log Server

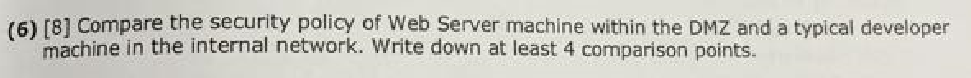
(C)

**DMZ Mail server**  
When an email message is received from Internet:  
a. Reassembles message  
b. Checks for malicious content  
c. Changes addresses of outer firewall (which is how mail server is known to outside world)  
to that of internal mail server and forwards the mail to the internal mail server  
  
To send a message from the internal network to the Internet  
a. Reassembles message  
b. Checks for malicious content (and maybe for proprietary information).  
c. All internal addresses are replaced with "drib.org" (the name of the outside firewall).  
  
**DMZ WWW Server**Does not contact any servers or information sources on the internal network and it contains  
no confidential data.  
  
Is accessed from the Internet using address of outer firewall.  
  
~~Developers release updates to the web site to an internal machine named WWW-Clone. Developers  
are \*\*\*not\*\*\* allowed access to the DMZ WWW server. A system administrator uses SSH to  
transfer from WWW-Clone to DMZ WWW server.  
  
DMZ WWW server invokes a simple program to validate customer data and encrypt it. Encrypted  
with the public key of the CSG (Customer Service Group). System administrator connects to WWW   
server using SSH to copy encrypted file to internal CSG network.~~  
**DMZ DNS server**Contains entries for the following:  
a. DMZ mail, Web and log hosts  
b. Internal trusted administrative host (how administrator connects using SSH)  
c. Outer firewall  
d. Inner firewall  
  
The limited information in the DNS server reflects the principle of least privilege. It  
only contains entries needed so that systems in the DMZ can talk to each other.  
  
**DMZ Log Server**All DMZ machines have logging turned on. On separate machine to reduce chance that attacker  
can delete log files.  
  
Log machine writes logs to a file and to a write-once media.  
  
~~System administrator can use SSH to copy logs from DMZ log server to internal network or  
can go to the log server and retrieve the write-once media.~~  
  
**In summary,** each of the four servers has the minimum amount of knowledge of the network that  
is needed to perform their function.











The administrator’s connection uses the Secure Shell (SSH) protocol and differs

from the other protocols in that a direct connection through the SSH port is allowed

(that is, no SSH proxies). This allows the address of the administrative server to leave

the internal network. However, the firewall filter ensures that the SSH connection can

go only to one of the DMZ servers. This use of cryptography provides message secrecy

and integrity as well as strong (cryptographic) authentication of the endpoints.37 Because the

requisite public keys are embedded into the system when SSH is configured, the issue

of an infrastructure for public key distribution is finessed.

**\*Note: need better answer**



**Authentication** is the process of ascertaining that somebody really is who he claims to be.

**Authorization** refers to rules that determine who is allowed to do what. E.g. Adam may be authorized to create and delete databases, while Usama is only authorised to read.

The two concepts are completely orthogonal and independent, but both are central to security design, and the failure to get either one correct opens up the avenue to compromise.

**Alternate Answer (Copied from some quiz):**

Authentication is the binding of an identity to a subject.

Authentication binds a principal to a representation of identity internal to the computer.

Authentication is identity verification of an external entity using one or more options like 'what the entity knows or has or is'

Authorization verify the role of an entity whether the entity allows to access specific resource/area or not. Authorization is happened after successful authentication.

For example, login process is authentication, allowing customer to access admin section is authorization.



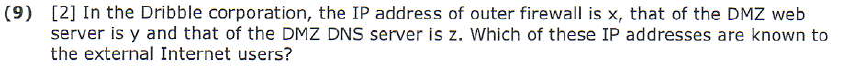
**Cookies**

A cookie is a token that contains information about the state of a transaction on a network.

**Session**

**Hidden fields**

**Query strings**



Outer firewall allows public to access Web and mail servers. But public uses same IP address

for both, namely the IP address of the outer firewall. Here x will be known to external internet user.



**Same as below**



A threshold metric statistical model will be used.

A minimum of m and a maximum of n events are expected to occur (for some event and some values m and n). If, over a specific period of time, fewer than m or more than n events occur, the behavior is deemed anomalous.

~~EXAMPLE: Microsoft Windows NT 4.0 allows the system to lock a user out after~~

~~some number n of failed login attempts [479]. This is an intrusion detection system~~

~~using the threshold metric with the lower limit 0 and the upper limit n. The attempted~~

~~logins are deemed anomalous after n failed attempts to log in.~~

Determining the threshold complicates use of this model. The threshold must

take into account differing levels of sophistication and characteristics of the users.

For example, if n were set to 3 in the example above for a system in France, and the

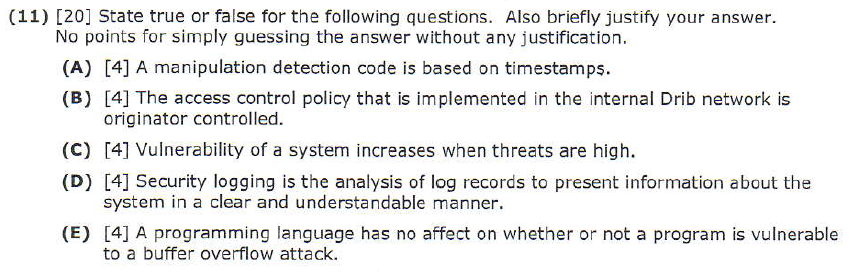
primary users of that system were in the United States, the difference in the

keyboards would result in a large number of false alarms. But if the system were

located in the United States, setting n to 3 would be more reasonable. ~~One approach~~

~~is to combine this approach with the other two models to adapt the thresholds to~~

~~observed or predicted behavior.~~



**(A) False,** Mechanisms using manipulation detection codes (or MDCs) apply some function to a

file to obtain a set of bits called the signature block and then protect that block. If, after

recomputing the signature block, the result differs from the stored signature block, the

file has changed, possibly as a result of malicious logic altering the file. This mechanism

relies on selection of good cryptographic checksums

**(B)False,** Mandatory access control policy is implemented in the internal Drib network. Employee do not have the ability to let users in certain user group read their files. For example, a corporate employee does not have the ability to give a customer service employee access to files that contain financial data.

