Examination Paper

Spring Session 2014

Part A

1) The Biba model is for the purpose of integrity control while BLP is for the purpose of access control. Integrity control it means Biba model protects against unauthorised modification of information, while access control it means BLP model protects against unauthorised disclosure of information.

Part A

2) Phishing emails are typically sent in bulk because
The attacker cannot expect to fool most people;
the attacker just hope to fool some.

Part A

3) PAT (Port Address Translation) hides internal network addresses (TCP/IP) from outside world by mapping the external addresses to multiple internal addresses.

Part A

4) DNS-based phishing infers with poisoning of hosts file or polluting the user's DNS cache with incorrect information resulting in incorrectly configured DNS or corrupted DNS.

Part A

5) Two primary properties used in malware classification are based first on how it spreads or propagates to reach the desired targets, and then on the actions or payloads it performs once a target is reached.

SIM-2016-S3-CSCI262-S6a, Slide 12 or the textbook
Computer Security: Principle and Practice, 3ed ed, William Stallings, Lawrie Brown, 2015, Pearson Education Limited.

Part A

6) Aggregate functions provide computed / aggregated data, which is likely to be less sensitive than individual values. For example, the sensitivity level of an average salary in a department is lower than sensitivity level of the salaries of individual employees.

Part A

7) The three primary components of a virus are infection mechanism, which spread the payload, payload, which is what besides spreading the virus, and trigger, which is the condition to be met before the payload is activated.

Part A

8) Two applications of reverse engineering are malware and Digital rights management.

Part A

9) Two channel authentication uses two separate channels to accomplish targeted authentication. one channel is from the client to the server and the second channel is from server to client using a different channel (e.g., telephone, or a device, etc) to give targeted authentication. It is not enough to say two channels! ☺

Part A

10) A pseudonymising sanitizer removes information from the log such that the originator of the log can reconstruct the deleted information but preserves information and the relationship relevant for the analysis.

Part A

11)A master password is typically used to protect sensitive information such as other passwords and certificates. Master password is used in application such as “AntiPhish”, which is usually integrated into the web browser.

Part A

12)The C library function strcpy() is considered unsafe because it doesn't check for array boundary, so may result in buffer overflow.

Part A

13)Two classes of intruder that an intrusion detection system may attempt to find are:
Clandestine, who try to avoid the intrusion detection or auditing system and
Masquerader, who pretend to be a legitimate user.

Part A

14) An event being “Not known to be bad” likely refers to not being on a event description of activities considered to be violating security policies in the context of Intrusion detection system.

Part A

15) “Online” and “offline” attacks differ in that online require the connection to be active which may impose certain restriction while attempting to break the password while offline attack have unlimited chances to break the password.

Part A

16) One resource that can be targeted in a DOS attack is network bandwidth (for network) or memory storage and processor capacity (for computer).

Part B – Question 1 …1

1) Describe the three main bases of authentication. Give an example of each. Describe an advantage and a disadvantage of each, either generally or for the specific example given.

The three main bases of authentication are:

- **Something you know**, e.g., password. Advantage of this base is a user can set his/her own desired password. The disadvantage is that password can be forgotten.
- **Something you have**, e.g., a "device" or key card. Advantage of this base is that authentication is easy. The disadvantage is the device may be lost.

Part B – Question 1 …2

- **Something you are**, e.g., fingerprint or any other biometric data. The advantage is this token cannot be lost or forgotten. The disadvantage is that the body part that is associated to the biometric information may be damaged, for example, finger may be accidentally cut (injured), and hence may affects the fingerprint.

Part B – Question 2 …1

2) Describe the use of access control matrices and how they relate to capabilities and access control lists. Give an example to illustrate your explanation.

Access control matrix is used to restrict subject from accessing objects that the subject is not authorized to act on.

Capabilities is from the perspective of subject, and access control list is from the perspective of objects.

Part B – Question 2 …2

Access control matrix:

	x	y	z
Alice	rw	r	e
Bob	r	rw	

Access control list:

x : (Alice, rw), (Bob, r)

y: (Alice, r), (Bob, rw)

z: (Alice, x)

Capabilities:

Alice: (x, rw), (y, r), (z, e)

Bob: (x, r), (y, rw)

Part B – Question 3 …1

3) Explain what a Trojan Horse is. Describe two distinct methods of identifying a Trojan Horse and explain when and why each of those methods might be appropriate.

Trojan Horse are non-replicating program that openly exhibit one desirable behaviour, it might be a game for example, but have some real intent hidden from the user. This real intent could, for example, be to open ports on a machine to allow attackers access. A Trojan horse renames itself to the name of a valid system file. It can also be encrypted and polymorphic, and could install themselves in different ways to escape detection.

Part B – Question 3 …2

Two methods of detecting Trojan Horses:

- Monitoring – Make use of virus monitors to monitor known methods of virus activities, such as attempts to write to a boot sector, modify interrupt vectors, write to system files, etc. and detect abnormal behaviour of the system. This technique is able to detect the Trojan Horse before complete infection. The disadvantages is that to detect a high percentage of viruses, the sensitivity of the monitor must be set high and this may generate many false alarms.

Part B – Question 3 …3

Two methods of detecting Trojan Horses: (cont…)

- Signature scanning – the simplest and the most common approach to virus detection. With this technique, signature extraction is a non-trivial process. The infection is disassembled and the key portions are identified. Next, the key portions are combined to form a signature. The signature is then checked against a large library of programs to reduce the chance of false positives occurring when signature accidentally matches some library code. The advantage of this technique is that other than detecting Trojan Horse, it can also be used to detect logic bombs and other malicious software. The disadvantage is that scanning cannot find new viruses before their patterns are known. In addition, this technique is also ineffective against polymorphic viruses.

Part B – Question 4 …1

4) Name and describe the two types of errors that occur in authentication systems and in intrusion detection systems. Give an example of each. Explain how the interpretation of each differs between authentication systems and intrusion detection systems.

Part B – Question 4 …2

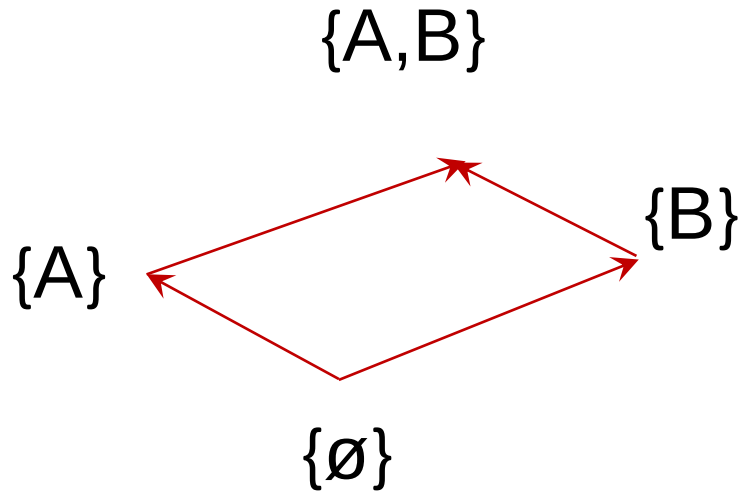
False negative and false positive.

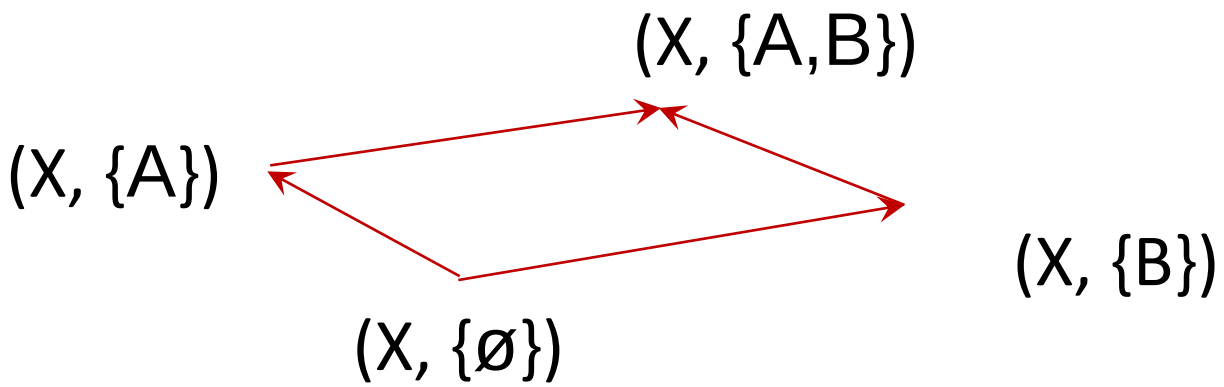
From authentication perspective, false negative and false positive concerns the likelihood of getting a result which is wrong, that is, an invalid user but falsely identify as valid (false negative) and a valid user but falsely identify as invalid (false positive). From intrusion detection perspective, false negative is when we do not make a match, but we should have, that is, there is an intrusion take place, but the system did not manage to identify/recognize it. A false positive is when make a match, but we should not have, that is, the system identify an intrusion, which is actually not.

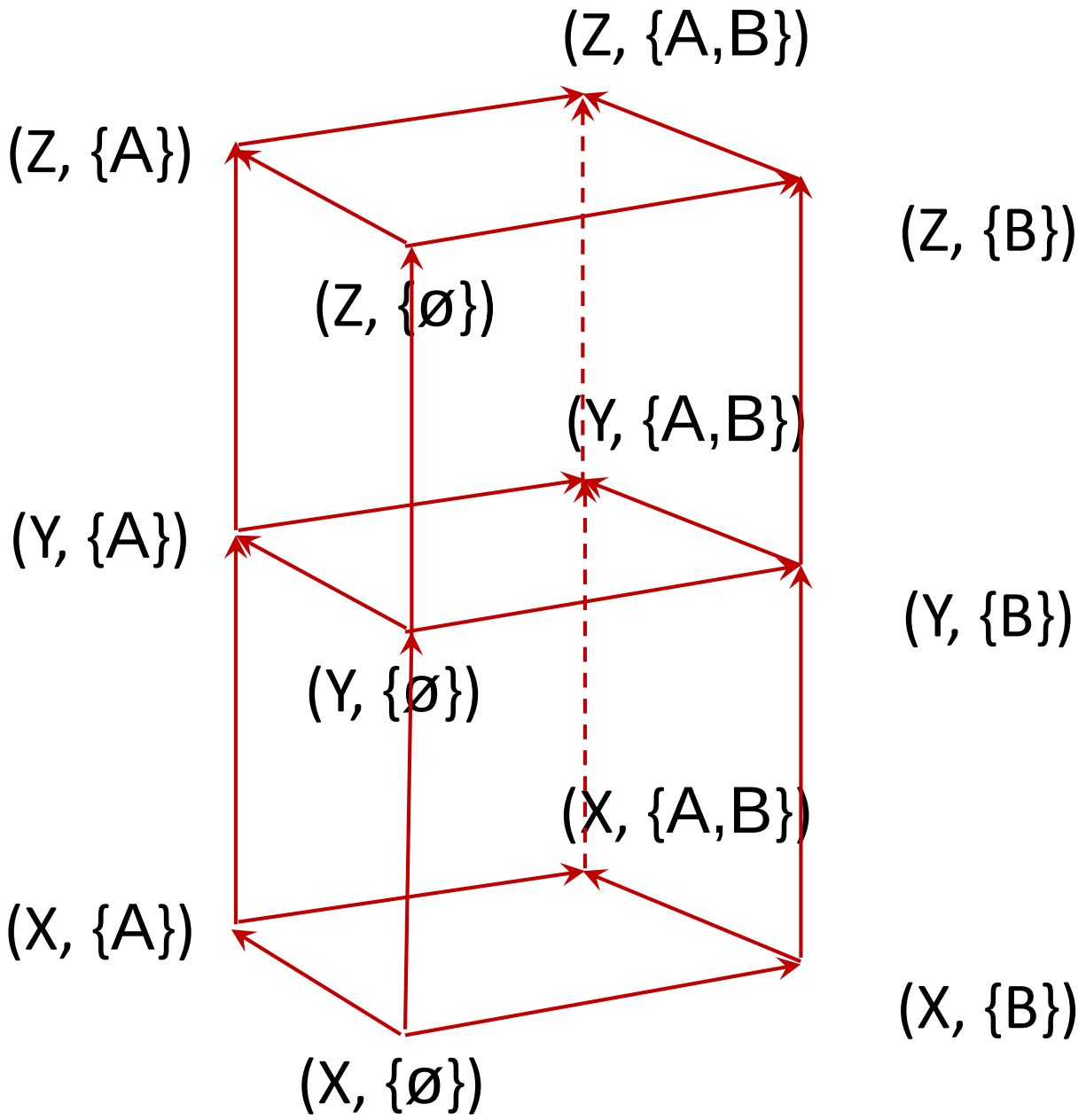
Part B – Question 5 …1

5) A company has two department, A and B and has determined that it is appropriate to have three levels of sensitivity, in increasing order X, Y and Z. Draw a BLP lattice system to represent this scenario. Using examples, explain the three BLP rules, 2 mandatory and 1 discretionary.

{A} {B}

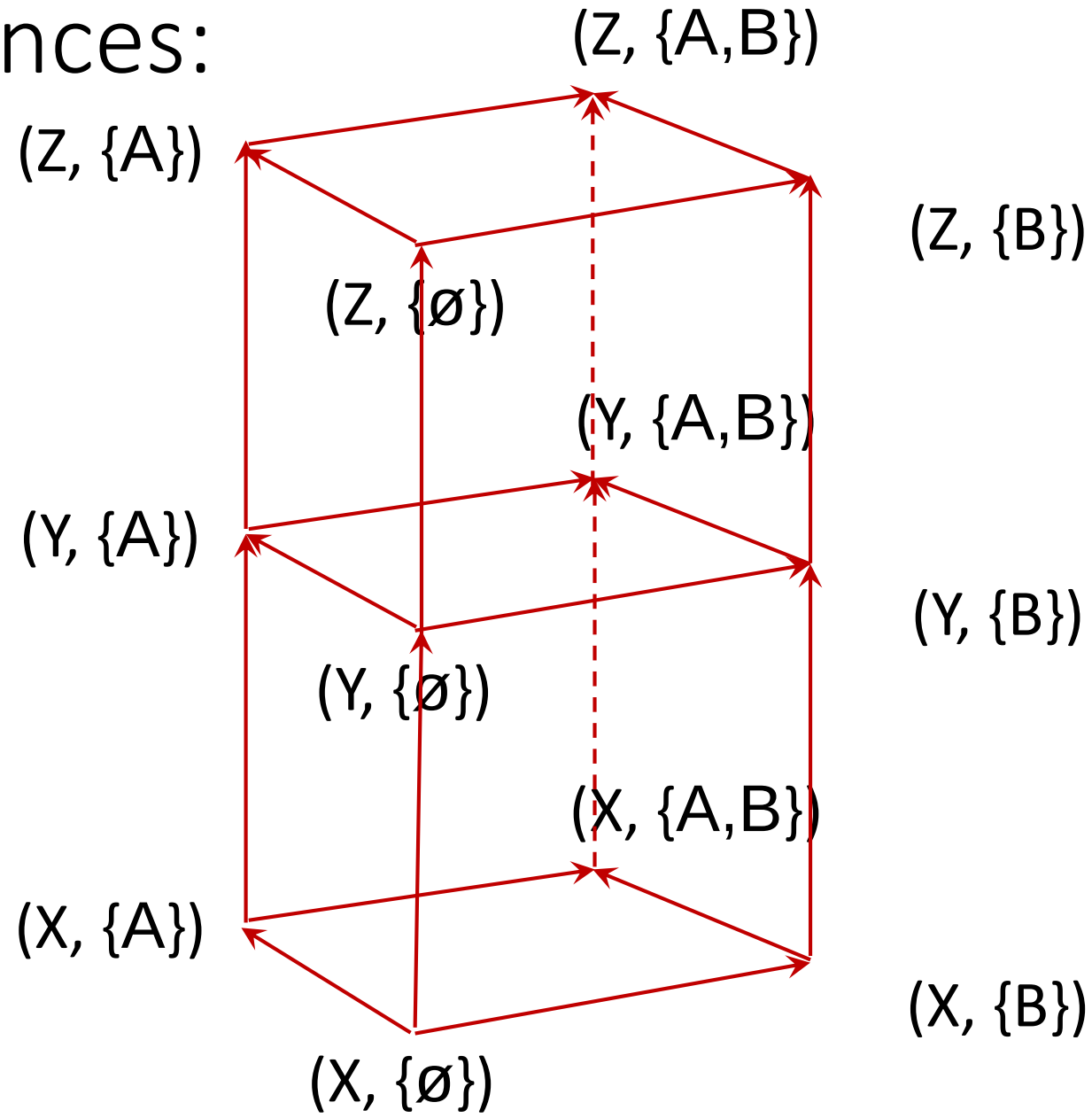





(Z, {A,B})
(Z, {A})
(Z, {B})
(Z, {ø})
(Y, {A,B})
(Y, {A})
(Y, {B})
(Y, {ø})
(X, {A,B})
(X, {A})
(X, {B})
(X, {ø})

Example of the dominances:

(Z,{ø}) ≥ (Y,{ø}) ≥ (X,{ø})
(Z,{A}) ≥ (Y,{A}) ≥ (X,{A})
(Z,{A}) ≥ (Z,{ø})
(Z,{B}) ≥ (Y,{B}) ≥ (X,{B})
(Z,{B}) ≥ (Z,{ø})
(Z,{A,B}) ≥ (Y,{A,B}) ≥ (X,{A,B})
(Z,{A,B}) ≥ (Z,{A})
(Z,{A,B}) ≥ (Z,{B})
(Y,{A}) ≥ (Y,{ø})
(Y,{B}) ≥ (Y,{ø})
(X,{A}) ≥ (X,{ø})
(X,{B}) ≥ (X,{ø})



BLP properties (Rules)

- Ss-property
  - Subject S(n) can WRITE object O(n) iff level of clearance of subject L(S) is less than or equal the level of clearance of the object L(O), that is, L(S) ≤ L(O), and the subject has permission to WRITE the object.

- *-property
  - Subject S(n) can READ object O(n) iff level of clearance of subject L(S) is greater than or equal (dominant) the level of object L(O), that is, L(S) ≥ L(O), and the subject has permission to READ the object.

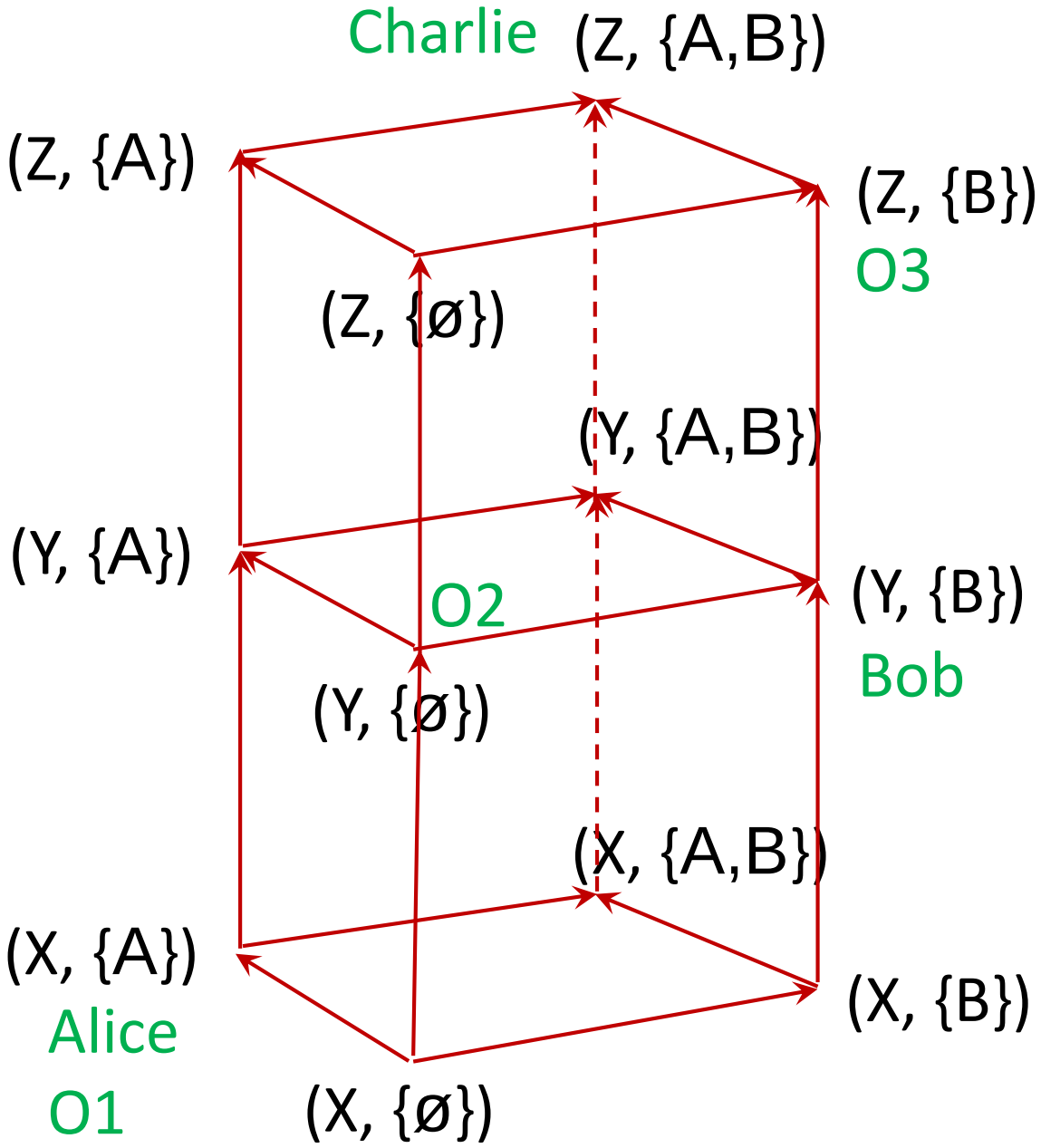
- Discretionary
  - Subject S(n) can discretionarily transfer his/her authorization to Subject at a different clearance level (subject to organization policy).

Subjects and Object at various level of clearance

- For example, we have three subjects Alice, Bob and Charlie and three objects O1, O2 and O3 with the following level of clearance defined:

Subject	Level
Alice	(X,{A})
Bob	(Y,{B})
Charlie	(Z,{A,B})

Object	Level
O1	(X,{A})
O2	(Y,{ø})
O3	(Z,{B})



Subject	Level
Alice	(X,{A})
Bob	(Y,{B})
Charlie	(Z,{A,B})

Object	Level
O1	(X,{A})
O2	(Y,{ø})
O3	(Z,{B})

Access Control Matrix:

	O1	**O2**	**O3**
Alice	R, W	-	-
Bob	-	R	W
Charlie	R	R	R

Part B – Question 6 …1

6) In the third assignment for this subject you looked at detecting intrusions in an event based scenario. An example of the information your program was to initially generate was as follows:

Event	Average	Stdev	Weight
Logins	4.50	1.25	2
Total time online	287.15	42.12	1
Emails sent	65.40	30.71	1
Orders processed	150.73	20.13	1
Pizza’s ordered online	2.03	1.06	0.5

Part B – Question 6 …2

Explain what each of these columns represent. How such values would be generated in practice, and how they are used in the detection of intrusions. You do not need to give numerical calculations but if it helps you to explain you can.

Part B – Question 6 …3

- The first column, “Event” contains the list of events being monitored.
- The second column, “Average” contains the average or mean that a particular event has under a normal situation.
- The third column, “Stdev” contains the standard deviation a particular events may be deviated from the mean. This can be the basis for specifying an anomaly, e.g., a measure as being more than a certain number of standard deviations away may be identified as anomaly.
- The fourth column, “weight” contains a factor to adjust the important or criticality of an event to the intrusions to be identified.

Part B – Question 6 …3

- In practice, the information such as the mean and standard deviation are generated based on specific user's daily activities value for the past one week, or one month, or a year or any other specific number of days. The daily activity are capture based on the definition of events defined in the description or definition file. The mean and standard deviation are then computed based on these activities values. Finally, a threshold value is computed as the sum of the weight multiplied by 2. The computed mean, standard deviation and then used to compute the live (actual) activities to determine the distance (deviation) from the computed values. If the sum of the daily event distances exceeded a threshold, an alarm is raised.

Part B – Question 7 …1

7) Explain what tailored attacks are. Give some specific examples in two different domains and explain how they perform relative to other attacks in those other domains.

Tailored phishing attack is where the attack is done on all people who are known to be customers to a particular banks etc. it is similar to tailored dictionary attack where we use what we know about the person to increase the likelihood of successful attack.

Part C – Question 1 …1

1) For each of the following CWE's, explain what the problem is and the potentials 'bad thing' that could happen
   a. CWE-307: "Improper restriction of excessive authentication attempts."
   b. CWE-759: "Use of a One-Way Hash without a salt."
   c. CWE-306: "Use of Hard-coded Credentials."
   d. CWE-131: "Incorrect Calculation of Buffer Size."

https://cwe.mitre.org/

Part C – Question 1 …2

a. CWE-307: “Improper restriction of excessive authentication attempts.”

   The problem is where there is not enough authentication restriction is being placed. If no restriction are placed then the attacker can use unlimited attempts to break the password.

Part C – Question 1 …3

b. CWE-759: “Use of a One-Way Hash without a salt.”

The problem is where salt is not used in hashing which makes the hash less secure. if salt is not used the adversary can just hash all the possible passwords and compare to break the password.

Part C – Question 1 …4

c. CWE-306: “Use of Hard-coded Credentials.”

The problem is where sensitive credential like passwords are hard coded into the software used for internal authentication. This creates a loophole for the adversary to bypass the authentication process.

Part C – Question 1 …5

d. CWE-131: “Incorrect Calculation of Buffer Size.”

The problem is where the buffer size of program is not computed properly the information is leaked out of bound of the buffer. This may cause buffer overflow where an adversary can place a malicious address in place of the return address to run the malicious code.

Part C – Question 2 …1

2) The following questions cover a range of topics:
   a. Sketch the process used within a state machine based security model to prove the security of an access control system.
   b. What is IDIP and what purpose does it serve? Explain briefly how it works.

Part C – Question 2 …2

c. Two versions of a loop are given below. One is an example of defensive programming. State which and explain why. You need to briefly explain what defensive programming is to answer this question completely.

A

```
size_T elements = strlen(container);
for (i = 0; i < elements; ++i)
    State = combine(state, container[i]);
```

B

```
size_T elements = strlen(container);
for (i = 0; i != elements; ++i)
    State = combine(state, container[i]);
```

Part C – Question 2 …3

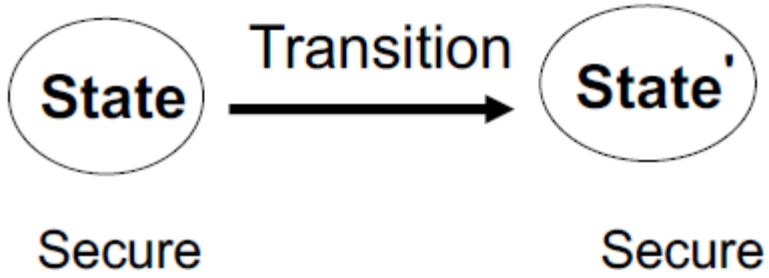
a. Sketch the process used within a state machine based security model to prove the security of an access control system.

Part C – Question 2 …4

1. Define appropriate state variables.
   - State relationships between them.
2. Define conditions for a secure state:
   - This includes the relationships between values of state variables that must be maintained during state transitions.
   - These are security constraints.
3. Define state transition functions:
   - Define the mechanisms by which state variables can change.

Part C – Question 2 …5

4. Prove each transition function maintains a secure state, when acting on a secure state.



4. Define an initial state.
5. Show the initial state is secure.
6. Apply induction to show evolution of the system must leave it secure, by 4 and 6.

Part C – Question 2 …6

b. What is IDIP and what purpose does it serve? Explain briefly how it works.

IDIP is known as Intrusion detection and isolation protocol is to stop an attack by blocking the connection. It works by detecting an attack and blocking the connection to the target from the source and inform the previous node about the attack which then blocks the connection and inform its previous node until which the connection is block from the source to the target.

Part C – Question 2 …7

c. Two versions of a loop are given below. One is an example of defensive programming. State which and explain why. You need to briefly explain what defensive programming is to answer this question completely.

A

```
size_T elements = strlen(container);
for (i = 0; i < elements; ++i)
    State = combine(state, container[i]);
```

B

```
size_T elements = strlen(container);
for (i = 0; i != elements; ++i)
    State = combine(state, container[i]);
```

Part C – Question 2 …8

Program A is defensive programming. Defensive programming is to guard against unexpected errors, but defensive programming is different from error handling. If a public variable is to accept and store integer, and you check if the value is integer is error handling as we know beforehand. If a private variable is to accept and store an integer and a program function is used to store the value and check are in place to make sure it is integer is defensive programming. Program A is defensive programming as the for loop is checking for I < elements, and as long as this condition is satisfied, the loop will run and eventually terminate, but program B has I != elements. There is a possibility that I is larger than elements outside the code hence it will lead to an indefinite loop.

Part C – Question 3 …1

3) The following questions relate to access control and authentication:
   a. What is the primary assumption we make about analysing the strength of a method of choosing a password? Why do we make this assumption?
   b. Based on your assumption from previous question, which of the following two methods of generating a password is better? Justify your answer. In every instance the choosing is uniformly random.
      A. Choosing a five digit number.
      B. Choosing a lower case letter, followed by a digit, following by an upper case letter, followed by two digits.

Part C – Question 3 …2

c. What does the “No write up” rule in the context of Biba imply? Give a simple example to illustrate your answer.
d. Should the password strength for an account be tied to the clearance level of a user? Justify your answer.

Part C – Question 4 …1

4) These questions relate to a variety of topics:
   a. What is honeypot?
   b. What role might a honeypot play in the detection and management of instructions?
   c. Give an example to illustrate how particular data within a real system might be considered to be a honeytoken.
   d. Explain why and when it is a bad idea to seed a random number generator with time only.
   e. What is XSS and what does it exploit?

Part C – Question 4 …2

a. What is honeypot?

A *honey pot* is a decoy that lures attackers away from production systems. It's usually a computer attached to the network that runs special software to emulate services, applications, protocols. A honey pot should not contain any data other than the information specifically created to trick the attacker. Nor should it be allowed to connect to any other system except other honey pots, to prevent the attacker from using the honey pot to launch an attack.

Part C – Question 4 …3

b. What role might a honeypot play in the detection and management of instructions?

We can use honeypots to rule the attacker to stay on the system long enough for the administrators to respond to the attack. In this case, the honeypots act as decoys in the intrusion detection and prevention system.

Part C – Question 4 ...4

c. Give an example to illustrate how particular data within a real system might be considered to be a honeytoken.

A honey token is a non-computer honeypot. Example fake data in database. This fake data are similar to the real data but to encourage the attacker to be in the system long enough to respond to the attack.

Part C – Question 4 …5

d. Explain why an when it is a bad idea to seed a random number generator with time only.

It is a bad idea if the random number generator is used to generate password. This is because if the adversary knows the approximate time the password was generated, then the adversary can execute the random number generator a period of time frame close to the actual time and may obtain the random password.

Part C – Question 4 …6

e. What is XSS and what does it exploit?

XSS is an abbreviation for cross site scripting. It exploits vulnerabilities in using dynamic web content, in particular, it involves the use of those vulnerabilities to gather data from a user that should not be gathered. XSS enables attackers to inject client-side scripts into web pages viewed by other users.

Part C – Question 5 …1

5) One of the client puzzles we considered contained the statement h(C, Ns, Nc, X) = 000…000Y.
   a. Describe each of the components in the expression above.
   b. How does the selection of Ns and Nc differ, and what significance does this have?
   c. How much work is required to “solve” the puzzle, in the context of this statement?
   d. Explain how the puzzle would differ if the right hand side of the statement was Y000…000 rather than 000…000Y?
   e. Describe how we could modify this to generate sub-puzzles.
   f. What does the term resource disparity refer to in the context of puzzles?

Part C – Question 5 …2

$$h(C, Ns, Nc, X) = 000 \ldots 000Y.$$

a) Describe each of the components in the expression above.

- h: a cryptographic hash function (e.g., MD5 or SHA)
- C: the client identity
- N_s: the server's nonce
- N_c: the client's nonce
- Y: the rest of the hash value; may be anything
- $000 \ldots 000$: the k first bits of the hash value; must be zero. The reasonable values of k lie between 0 and 64.
- X: the solution of the puzzle

Part C – Question 5 …3

b) How does the selection of Ns and Nc differ, and what significance does this have?

- Both Ns and Nc are randomly generated. There is no specific pattern that is associated to the generation of the nonce.
- To prevent attacker from precomputing solution, a server may periodically generates Ns.
- The size of Ns ranges between 0 and 64 bits while the size of Nc ranges between 0 and 24.
- The selection of the size of Ns and Nc affects the difficulty level of the puzzle, in other words, the efforts the client need to solve the puzzle.

Part C – Question 5 ...4

c) How much work is required to “solve” the puzzle, in the context of this statement?

The cost of solving the puzzle depends exponentially on the required number of k of zero bits in the beginning of the hash. If $k = 0$, no work is required. If $k = 64$, then in the worst case, it would be 2^k. In such a puzzle, the reasonable values of k lie between 0 and 64.

Part C – Question 5 …5

d) Explain how the puzzle would differ if the right hand side of the statement was Y000…000 rather than 000…000Y?

Part C – Question 5 …6

e) Describe how we could modify this to generate sub-puzzles.

Part C – Question 5 …7

f) What does the term resource disparity refer to in the context of puzzles?

4b_Abliz09

Part C – Question 6 …1

6) These questions relate to a variety of topics:
   a. Describe how virus and worm propagation differs.
   b. How does a stateful inspection firewall differ from the traditional packet filters?
   c. Describe a typical phishing process.
   d. Explain the role a sandbox might play in the detection and analysis of malware.

Part C – Question 6 …2

a. Describe how virus and worm propagation differs.

   Virus propagate by manual transferring of infected files while worm propagate using only network connection.

Part C – Question 6 …3

b. How does a stateful inspection firewall differ from the traditional packet filters?

   Stateful inspection firewall allows a more dynamic structure such as authentication is required before an “allow” entry for a particular connection while traditional packet only deal with individual packets.

Part C – Question 6 ...4

c. Describe a typical phishing process.

A typical phishing process involves deception where the user is fooled into believing that there are issue with his account and enter his account details to fix the issue but is actually stored and collected by the phisher to cause harm.

Part C – Question 6 ...5

d. Explain the role a sandbox might play in the detection and analysis of malware.

sandbox plays an import role as if a software is suspected that to be a malware and it is a malware, the vector of damage caused by the infection is limited to that vector and it cannot affect the main environment keeping the main environment safe.

Part C – Question 7 …1

7) These question relate to inference:
   a. Describe and give examples of two different types of disclosure we might want to avoid in the context of a statistical database.
   b. Explain the difference between direct and indirect attacks. Use an example to assist in your explanation.
   c. Name and describe two methods of protecting, at the query level, against inferential attacks in statistical interfaces. For each of those methods describe a potential problem.

Part C – Question 7 …2

a. Describe and give examples of two different types of disclosure we might want to avoid in the context of a statistical database.

The two types of disclosure are:

i. Disclosure of exact data, for example, Adam is 27 years old.
ii. Disclosure of bound, for example, Adam is younger than 30 years old.

Part C – Question 7 …3

b. Explain the difference between direct and indirect attacks. Use an example to assist in your explanation.

Direct attack is an attack where the aggregates are over small enough samples that information about individual elements of data can be obtained. Indirect attack is an attack where information external sources is combined with the results of aggregate queries.

Part C – Question 7 …4

An example of direct attack is an average salary of all employees older than 60 discloses an exact value of salary if exactly one employee older than 60 is employed.

An example of indirect attack is that we know, independent of the database, who lives in which suburb and who is a member of which department, the query …

```
SELECT SUM(SALARY), COUNT(*)
FROM EMPLOYEE
WHERE GROUP BY DEPTNAME, SUBURB;
```

… may then disclose the salaries of the employees who are the only people employed in a department and living in a particular suburb.

Part C – Question 7 …5

- One of the method of protecting inference attack is to design the database in such a way that inference is reduced. This approach removes an inference channel by altering the database structure or by changing the access control regime to prevent inference. One potential problem with this technique is the unnecessarily stricter access controls that may reduce availability.

Part C – Question 7 …6

c. Name and describe two methods of protecting, at the query level, against inferential attacks in statistical interfaces. For each of those methods describe a potential problem.

   i. Try to design a database in such a way that inferences is reduced.
   ii. Attempt to reject specific/sequence of queries which may lead to inference attack.