Course code/ kurskod	Course name / kursnamn			
EDA 263	Computer Security			
Anonymous code Anonym kod		Examination date Tentamensdatum	Number of pages Antal blad	Grade Betyg
EDA263 - 41		2014-08-27	14	5

Solved task Behandlade uppgifter No / nr		Points per task Poäng på uppgiften.	Observe: Areas with bold contour are to be completed by the teacher. Anmärkning: Rutor inom bred kontur ifylles av lärare.
1	✓	8-	
2	✓	+	
3	✓	7+	
4	✓		
5	✓	6—	
6	✓	10	
7	✓	12	
8			
9			
10			
11			
12			
13			
14			
15			
16			
17			
18			
Total examination points Summa poäng		57	

(a). Relational database is a database management technique where ~~enti~~ different entities involved in a particular concerned
2 scenario are connected through relations. The structure of a relational database is defined by the schema. In this schema it contains non-sensitive data ~~with~~, sensitive data and metadata.
~~Nor~~ A normal database user have access only to the non-sensitive data and meta-data. This meta-data describes ~~about~~ information about the structure of the database. Sensitive data is accessible only to the database administrator.
In a relation database the threat of inference means getting accessing to ~~non~~ sensitive data by means of the non-sensitive data and metadata. ~~A~~this means although a normal user does not have access to sensitive data he can execute legitimate queries on non-sensitive data and get legitimate responses. ~~By Combining~~ Depending on the situation by combining this results with meta-data an attacker can derive sensitive information. Also when data items appear invidually it may not make any sense, but if they are combined together they may help to infer or derive sensitive data.

(b). Query size restriction is a technique that can be
2 use to protect a statistical database against an inference attack. In query size restriction, when a characteristic formula C is executed over a database and if the size of resultant set of ~~queries~~ ~~is~~ ~~set~~ charact eristic formula is a small value then the answer to the query is rejected. If we consider the letter k to be a small number chosen by a database administrator then we can define the restriction as follows, with an upper bound and lower bound.

$$k \leq |X(C)| \leq N-k$$

This k has to be chosen ~~larger~~ of enough size so that it will thwarts the inference attacks. When there are less number of overlaps between ~~queri~~ results of queries k can be chosen to be smaller, where as if the overlap is high k has to be large value. If the value $|X(C)|$ is not between the above limits it is rejected.

(c). Tracker attack is an attack that can be used to
2 derive information about an individual data item or a few data items, when the query size restriction is imposed upon a database. Using tracker attack information such as number of records can be derived. When the tracker is combined with an attribute in the database one can derive the exact value for that item.

12.

For example let us consider two ~~query~~ characteristic formulas called C1 and C2, where $x(C_1)$ & $x(C_2)$ have an overlap of size 1. as follows.

$count(C) = count(C_1) - count(T)$.

In this case since there is query size restriction, if we execute C_2 after ~~C2~~ C_1, then the query C_2 will be rejected But using a tracker T where $T = C_1$ and (not C_2), we can get answers for C_1 and T. Then by reducing count of T by count of C_1 we can get the count of the overlap.

(d).

When determining the exact salary of the professor Dod first using a tracker we can build a count such that the value of count to be 1.

let us consider the following characteristic formulas

C1 ⇒ sex = female $2 \le |x(C_1)| - 6 \le 11$ $N = 13 \quad k = 2$, $2 \le x(C1 \le 11$

C2 ⇒ dept = CS AND position = Prof

Now we can build the tracker T as follows.

T ⇒ C1 AND NOT C_2. $2 \le |x(T)| = 5 \le 11$

⇒ (sex = female) AND {NOT (dept = CS AND position = prof).

then we have count $(C_1) = 6$ and count $(T) = 5$

therefore count $(C) = count(C_1) - count(T)$
$= 6 - 5$
$= 1$.

then if we combine the attribute salary with C we should get the salary of the professor Dod. But in order to combine the salary ~~of Dod~~, we need to get some idea about the salary. ~~Then we~~ By executing some extra queries we can get some idea about salary.

if we execute C_3 ⇒ dept = CS AND position = prof

count $(C_3) = 2$ $2 \le |x(C_3)| = 2 \le 11$

then we can get the values of salaries as follows)

max (C3, Salary) = 80

min (C3, Salary) = 60

Ex. 1.

Now we can select the salary value 80 or 60 and combine it with C. as follows. Let us choose 80

D ⇒ salary = 80

count (C AND D) - count (T OR (C, AND D)) - count (T).

= ~~6 - 5~~ 5 - 5

= 0 ↑

This means we do not have any body with ~~salary~~ salary value 80 in the query set count (C AND D).

So definitely the salary of Dod is 60.

2.

Rule set A

In this rule set
- all the incoming traffic for mail server at port 25 is denied
- all the traffic coming to web server at port 80 is allowed.
- all the other types of traffic is also allowed.

So this rule set defines a default permit policy for all the incoming traffic other than mail traffic. The advantages of this stance or policy is that any body who wants to start a new service ~~in the~~ inside company network can easily do it without getting the specific permission from the system administrator. So anybody who wants to run a new service for testing purposes or commercial purposes can do it easily. ~~This will reduce~~ However if there are vulnerabilities in these new services an attacker can exploit those vulnerabilities and attack a system, because firewall rules are base only on static packet filtering. Also any employee who want to access a machine inside the network remotely can do it without getting explicit permissions this is another advantage. This may also improves the productivity of workers in the company.

Rule set B.

- In this rule set
  - all the incoming traffic to mail server at port 25 is denied
  - all the incoming traffic to web server at port 80 is allowed.
  - all the other types of incoming traffic is denied.

So this rule set defines a default deny policy or a stance. The major advantage of this method is other than the specifically allowed applications or incoming traffic no other traffic is allowed. therefore any malicious traffic which tries to enter the system is denied. So this provides a better security than rule set A. But on the other hand if some body wants to start a new service for testing or commercial purposes he has to explicitly obtain the permission from the System administrator. this may also involves ~~the~~ testing that application for known vulnerabilities. Therefore this policy may cause inconvenience to most of the uses. This an disadvantage. This may affects the employee satisfaction in the organization.

7+ 3

(a). $E_K(c)$.

2 Here the AS is ~~authenticatin~~ encrypting the reply to the client C. In Kerberos user passwords are never transmitted over the network.

So ~~the~~ ~~ene~~ when AS is encrypting the reply, the encryption is totally based on the password of the client C. Therefore this reply can be only decrypted by the client C. Any other user or attacker cannot decrypt this message and get the Ticket granting ticket ~~of~~ in cases if they capture this reply. So only client C can get the Ticket TGS.

(b). $K(C, TGS)$.

This is a session key generated by AS and distuted
2 to both C and TGS, so that in future communications that happen between C and TGS they can use this session key as a symmetric key to encrypt and decrypt the communication. Since this is a symmetric key it take less time in encryption and decryption. Also this session key is valid only to that session until the client C logout from the session. If the session timeouts after the lifetime, they may have to obtain a new session key.

(c). Lifetime2.

This specify the time period which a user can
2 use a ticket after it is issued that is ~~after~~ until lifetime 2 time units after the timestamp of the message, the message can be used. This thwarts the effects of an attacker using a ticket forever, if he gets hold of a ticket. This lifetime should be chosen to be not so small or not so big so that ~~soffi~~ an attacker does not have enough time to decrypt a message and get hold of a ticket or use a ticket.

(d). $TS_5 + 1$

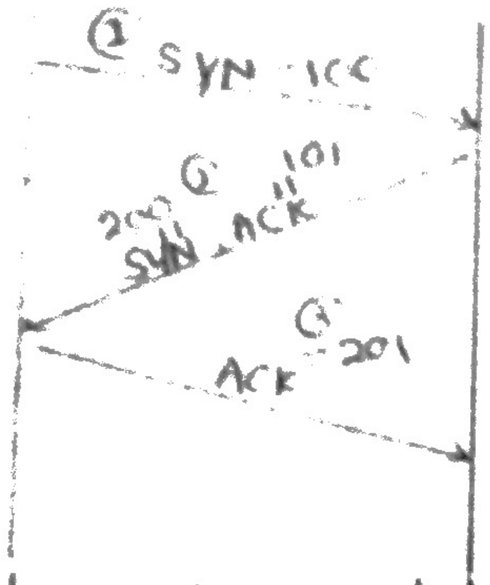
In kerneros other than client authenticating to the server, the server should also be authenticated to the client. This kind of ~~mutual~~ ~~au~~ mutual
1+ authentication is required in kerberos so that the client knows that he is communicating to the correct server. By sending $TS5+1$ ~~the~~ with encryption base on $E_{K(C,V)}$ this is guaranted.

prevent reply attack

4

SYN spoofing attack

(a) client server



In a client server architecture, when a client wants to establish a TCP connection with a server first it performs the TCP threeway handshake. Here, first the client sends the server a connection request with a sequence number for that request packet. When the server receives this request, it open an entry in its TCP connection ~~req~~ table and sends a reply to the (server) with an acknowledgement to the request packet and also a sequence number for the server replies. The idea of ~~the~~ two connection request table is to keep state about the tcp connections requests that are not completed yet. When the client receives this reply it sends back a reply by the acknowledging the servers reply. This threeway handshake is depicted in the figure above. (When the servers receives this, it remove the entry from its connection table for that request.)

~~(b) In a ty~~

2

(b). In a typical TCP SYN spoofing attack an attacker first sends a TCP connection request and wait until it receives a reply from the server. When the client receives the reply from ~~the~~ server, the client does not respond to that server reply. So that the ~~client~~ connection request table at the ~~s~~ server site get filled with uncompleted connection requests. ✓ When the server table is full with this kind of ~~con~~ uncompleted connection requests it can not longer responds to the new connections requests, so a denial of service ~~attacks is executed~~ happens at the server site. When compared to the figure from a ~~the~~, in a SYN spoofing attack the steps 1 and 2 are completed but not step 3. In a syn spoofing attack the requests actually ~~com~~ goes with a spoofed address, ~~not the~~ as the source address, not with the original source address ✓

2 - -

5 4

(c). Attacker is targeting the connection request table at the server machine. ✓ In a typical server this table is designed with the assumption that within less amount of time all the connection requests are completed by the requesting clients. Therefore this table is kept ~~small~~ with small number of entries.

(d). ~~In order to this attack to be succesful~~
In this attack since we use a spoofed address as a source address the connection reply 2 from server goes to the spoofed address. ~~The~~ when reply 2 is received by a user system ~~with~~ which has the spoofed address since it did not requested for the connection it may reply with an RST packet then the sever will drop this connection request and the attack will not be successful ✓ ~~In~~ Therefore in order to this attack to be successful when selecting the spoof address, an attack should select an address where there is no host available on that address or select a busy system which cannot responds to reply 2 messages from server ✓ the latter case may be achieved by making a DOS attack to the host wit the spoofed address.

2

(e). In a message flooding attack, the attacker needs a large bandwidth ✓ in order to fill the targeted system with requests. Because in message flooding all the steps of threeway handshake are completed and we keep the targeting system busy with flooded messages so that it cannot answer the legithmate user.
But in ~~Syn~~ contrast, in a SYN spoof attack an attacker does not need to have access to a high bandwidth, but a bandwidth small enough to keep the targeting systems connection request table busy. ✓
That is why an attacker may choose this attack over a message flood attack.

not very precise, but in general 2- correct

(a). The function readInput() is vulnerable to a buffer overflow attack. Because when it get the user input at line

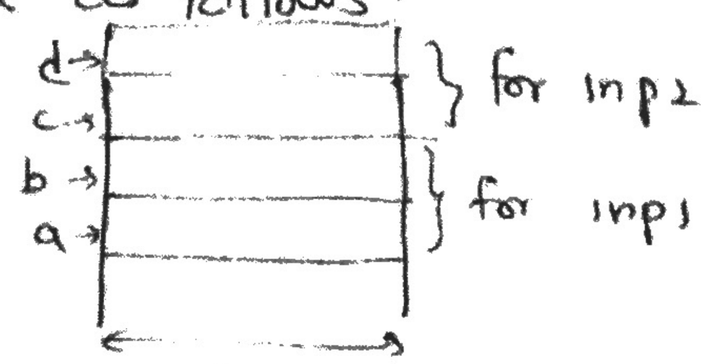
"gets(inp);"

the program does not check the size of input. The ~~the~~ size of the char array 'inp' is defined to be 16 bytes and the user inpet is stored in-to this array by gets. By the definition of gets it does not check the size of the input - ~~so~~ Because of this reason if the user input a string which is greater than 16 a buffer overflow attack occurs. In order to check fix this, the function readInput() should ~~read~~ the size of the input before assigning it to 'inp' variable. Then if it is less than or equal to 16 it can store it there. Otherwise ~~it~~ the program can discard the rest of the bytes ~~or~~ and store the result or reject user inpet and ask ~~for~~ ~~the~~ a input less than 16. What the problem? 2--

(b). A buffer is a continguous block of memory, allocated to store a variable or some data. When a program tries to store more data than allocated amount a buffer overflow occurs. When a buffer overflow occurs the rest of the data which is larger than the specified amount may flow into other memory areas. For example let us consider two variables inp1 and inp2 as follows which are defined consecutively in a program.

```
inp1[5];
inp2[6];
```

if the memory is allocated in stack for those variables it ~~be~~ will be as follows.



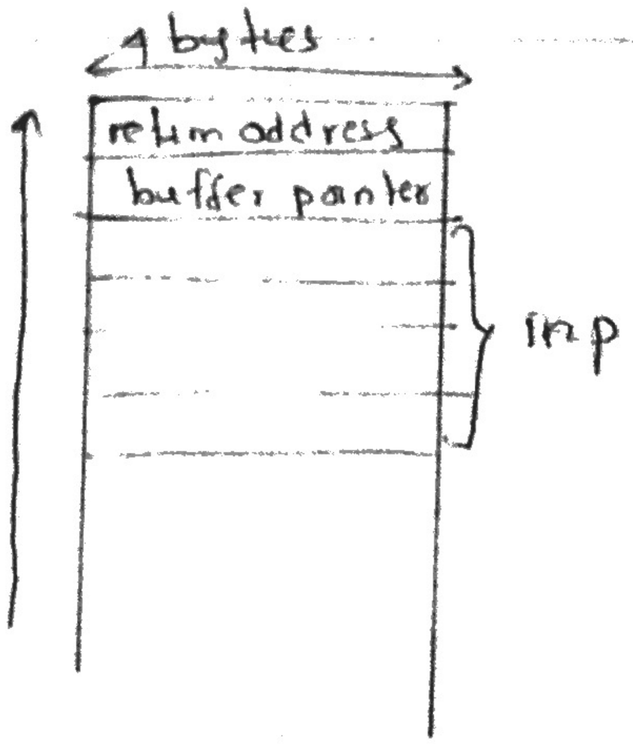
but if a user enters data for inp1 of size lets say 12 then addresses a and b can store 8 bytes, but the rest will ~~can~~ flow into address c, which actually belong to inp2. This is a buffer overflow.

How can you exploit this, what is the problem? 2--

5

5

(c).

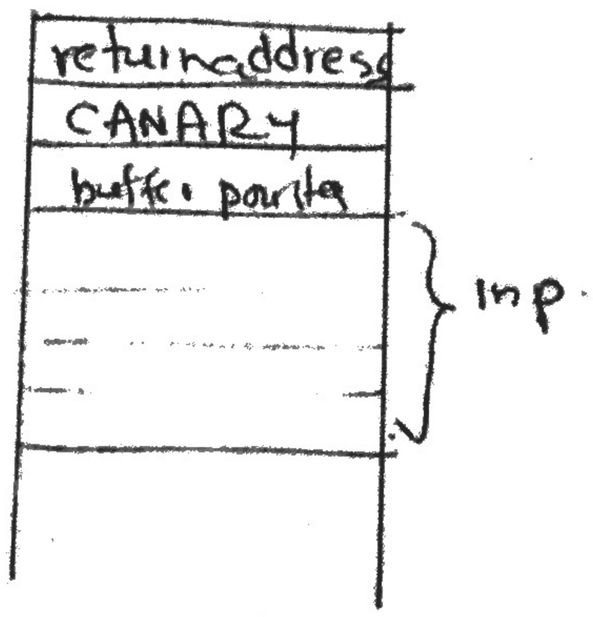


Lets consider a stack with 4 bytes ~~of~~ word size. When this function is called inside another function, on top of the stack for that ~~but~~ function will be the return address to the calling program. then there is the buffer pointer. then there is the 4 blocks of memory for inp variable.

not exact enough, SP!

(d). Canary is a software mechanism use as a protection against a buffer overflow. ~~Where the~~ The canary is a known value placed between the return address and the rest of the data in the stack so that if a buffer overflow occurs the canary is corrupted. By reading the canary value they can be detected and ~~stop~~ then one can stop a buffer overflow

The stack should change as follows.

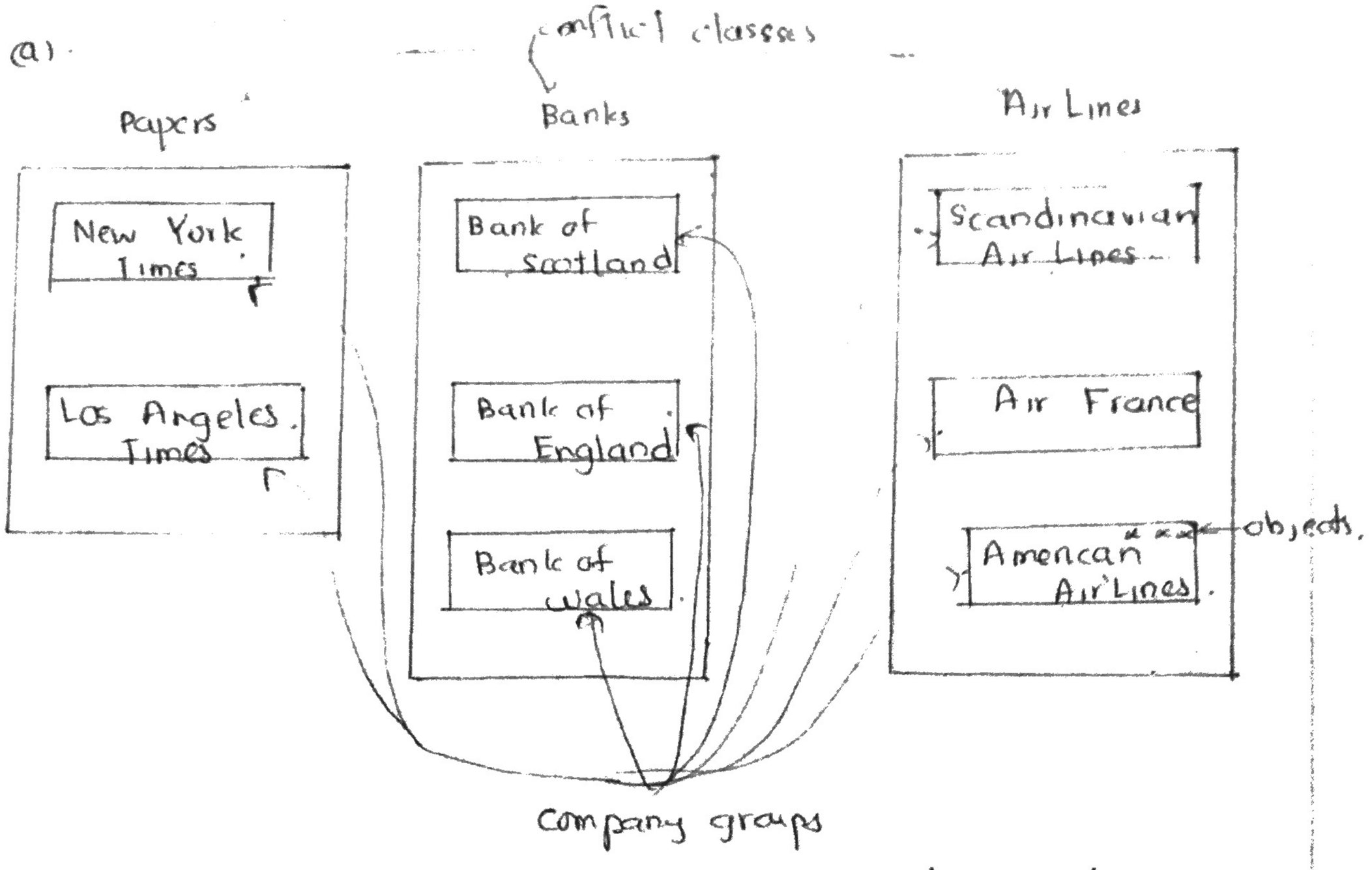


2

5

6

@1)



~~In this exam~~ In Chinese wall model ~~,~~ there are three levels of information. They are conflict classes, Data sets company ~~groups~~ and objects.

According to this example we have three different conflict classes. They are papers, Banks and AirLines. A conflict class contains a set of company groups which includes a set of different companies with conflicting Interests.

For example if we consider the paper conflict class we have two diffexent company graps. One is New york times and the other is Los Angles Times. Each of these company group contains objects that is specific to that organization. An object may be a file, a document or any other valuable critical resource.

For example ~~Eac~~ in the paper conflict class the New York Times company groups may contains objects, such as the document describing the purchases made by the company, the salaries of employees.

Very good 3/3

6.

(b). Simple Security Rule:

A subject S can read object O only if

- S has accessed an object from the same company group ~~that it~~ as O

  or

- S has not accessed any object from the conflict class where O belongs to.

1/1

(c).

(1). allowed.
This is the first time Alice access an object from ~~Bo~~ Banks conflicting class.

(2). denied
Alice has already accessed ~~delete fro~~ objects from another bank.

(3). allowed
This is the first time Alice accessing an object from Air Lines conflict class.

(4). allowed
This is the first time Bob accessing an object from Air Lines conflict class.

(5). denied.
Alice has already accessed objects from another bank.

(6). allowed
This is the first time Bob accessing the papers conflict class.

(7). allowed
Alice has already accessed objects from Bank of wales.

6

(8) · allowed.
Alice has already accessed objects from Bank of wales.

(9) · allowed
This is the first time Bob accessing an object from this conflict class.

(10) · allowed
Alice has already accessed objects from Air France.

(11) · allowed
Bob has already accessed objects from Air France.

(12) allowed.
Alice has already accessed objects from Bank of wales..

6/6

12 7

(a).
Side-channel attack is an attack that can be ~~used by~~ caused based on the side channel information. For example if an attacker has access to ~~th~~ an encryption device, without having access to encrypted or decrypted text, he can use side channel information to derive the plain text. For example, timing attacks ~~are~~ ~~to~~ is such a side channel attack, where attacker can record the time the device using to encrypt ~~or decrypt a~~ plaintext or decrypt a ciphertext or part of it. 2—

Good

(b). Trojan horse is a malware programme that appears to have a useful function but also has a unsuspected ~~an~~ hidden activity. Trojan horses are exploiting social engineering aspects for its spr~~ea~~ eading. For example an attacker can distribute a personnel management tracking software for free but also it secretly collects information about the system such as passwords. Often these kind of Trojan Horses are used to collect financial and secret information. If the compiler on a system is a Trojan horse, while compiling a source code into a binary it will also include the Trojan Horse program into the original source code. Therefore we need other methods to verify the correctness of a compiled program. This is ~~called the~~ technique is also known as the Thompson's compiller trick. 2+

(c). Protection profile is a system ~~in~~-independent set of requirements specified for particular category of products with some common features. This is usually specified by the system users.
Security target is a system-dependent set of requirments specified by a product. This product is a specific product produced by a vendor and the requirements are the functional and assurance requirements offered and evaluated for that product. The main difference between PP and ST is that PP specifies what is demanded by a product category where a ST defines what is actually offered by a specific profile. One or more PPs can be used by a ST to define its requirments. There are two concepts used in common criteria process.

2

(d). SQL injection is an attack launched against a database while making SQL queries into the database. Usually when there is a program that takes inputs from a user and passes them ~~to a q~~ to a query as part of ~~the~~ query without properly validating them a SQL injection can occur. In order to protect against these attacks when passing user arguments as parts of a query one should validate them using a parameter -ised API or other valid validation method. By SQL injection depending on the severity of the attack an attacker can ~~atter~~, add records, delete records or modify records in a database. Also in extreme cases he can drop a table or entire database. This techniques are applied in defensive programming.

2

(e). RSA is a public key cryptography mechanism whereas AES is a symmetric key cryptography mechanism. Both of them supports 256 bit keys. In order to protect the confidentiality of a very sensitive document, one can use AES over RSA, because RSA is proven to be broken with a 256 bit key by practice, although there is the general norm that public key cryptography is secure which is not true. Using AES is possible in this case because it addresses the issue of confidentiality in a symmetric key system.

2

(f). It is not possible to use one key as a primary key and other key as a backup key. Because in public key cryptography, the two different keys have another purpose. One can be used as a public key and distributed by one party to the rest of the parties. ~~to whom~~ Then those parties can encrypt any communication to the public key owner using the public key. The other key ~~is~~ which is known as the private key is retained by the key owner so that he can use it to decrypt any encrypted communication to him. Therefore for succesful communication we need both of the keys and one key cannot be considered as a backup for another.

2