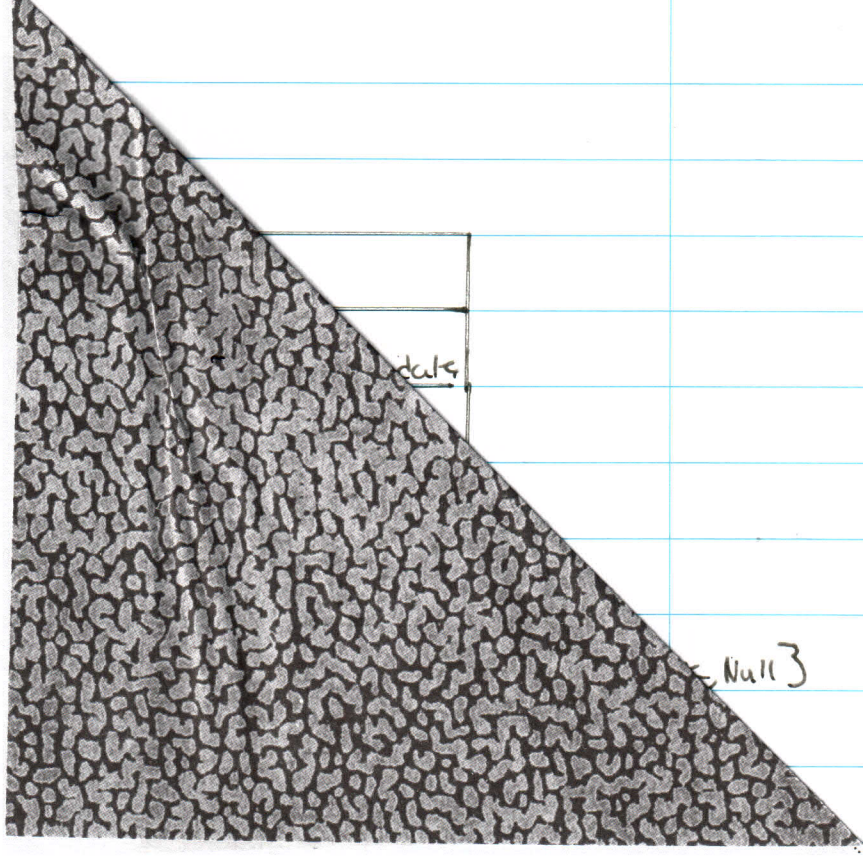
375

Coláiste na hOllscoile
Corcaigh
University College Cork



Uimhir Scrúdaithe
Examination Number 9 1 7 1 6 3

Do na Scrúdaitheóirí amháin **For Examiner's use only**	
1	
2	
3	
4	
5	
6	
7	
8	
9	
10	
11	
12	
13	
14	
Iomlán **Total**	

Module Code CS4615

Paper No. _____

Mír
Section _____

Calculator, Please state:	No. of Books submitted
Name Casio	2
Model Fx9lec4	

Note: If there are different sections on this paper, a separate Answer Book MUST be used for each section.

Q3

A

Database_table:

ID	Level	Client	Data
0	bank	Simon	Simons bank data
1	stock	Simon	Simons stock data
2	bank	Bob	bobs bank dat

Query Rule: Allowed combinations = {bank, stock, Null}

```
query (id, employee) :
    Entry = get (id)
    IF (employee.class U entry.level) is in Allowed_combinations
        employee.class = employee.class U entry.level
        return entry
    else
        return Null

insertion (Entry, employee)
    IF (employee.class = entry.level)
        return set (entry)
    else
        return False
```

5

set (entry) attemps to add entry to database. returns True if entry was added and False if entry could not be added because id already exists. it locks the table to atomically check if entry id exists. and subsequently add it if it does not

Q3

B Trojan horse running as stock classification would do the following:

First the trojan horse and the receipient would agree on an ID range to use eg 200 000 +, something not in use by normal data

To signal 2 bits of info the trojan would create IDs 200,000 and 200, 001 if it wanted to send a 0 bit it would not add an entry if it wanted to send a 1 bit it will.
To send for example the bitstring 01 it would leave id 200 000 unset and add an entry with id 200 001

The receipient will wait a pre determined amount of time before attempting to check to ensure the trojan has finished it will attempt to add an entry with ids 200,000 and 200001 if the write fails it received a 1 if it succeeds it recevied a 0

Closing the channel can be done in a number of ways

This includes splitting the tables into tables of different classifications of making (id, level) a composite key instead of a primary key

5

Q3
C

Risk assessment

$Risk_{conventional} = 0.01$ | $Cost_{conventional} = 250+250$

$Risk_{MLS} = 0.001$ | $Cost_{MLS} = 5000 + 250$

$Loss_{conventional} = €5000$

$Loss_{MLS} = €500$

Conventional

In Year 1 the cost for setting up a conventional system is €500 and a Potenial loss of €5000 costing In Year 1: €5500, Subsequent years: €5000

MLS

In Year 1 the cost for seting up the MLS system is €5250 with a potential loss of €500 costing In Year 1 €5750, subsequent years €500

It can be seen that the high upfront cost of of the MLS system is more than that of the conventional system

€5750 > €5500

but in Year 2 we have a saving of €4250 on the MLS system

Advise to go for MLS system for

Insurance cost €500
covers €200 000
Assumed loss € 300, 000

Cost OF conventional system with insurance

Year 1

€300,000 * 0.01 = 3000

+

€500 ← insurance cost

+

€ 250 +250 ← system cost

Conventional cost Year 1 = €4000
conventional cost Subsequent = €3500

10

Cost OF MLS system with insurance

€300,000 * 0.001 = 3000

+

€ 500

+

€5000 + € 250

Year 1 = 8750

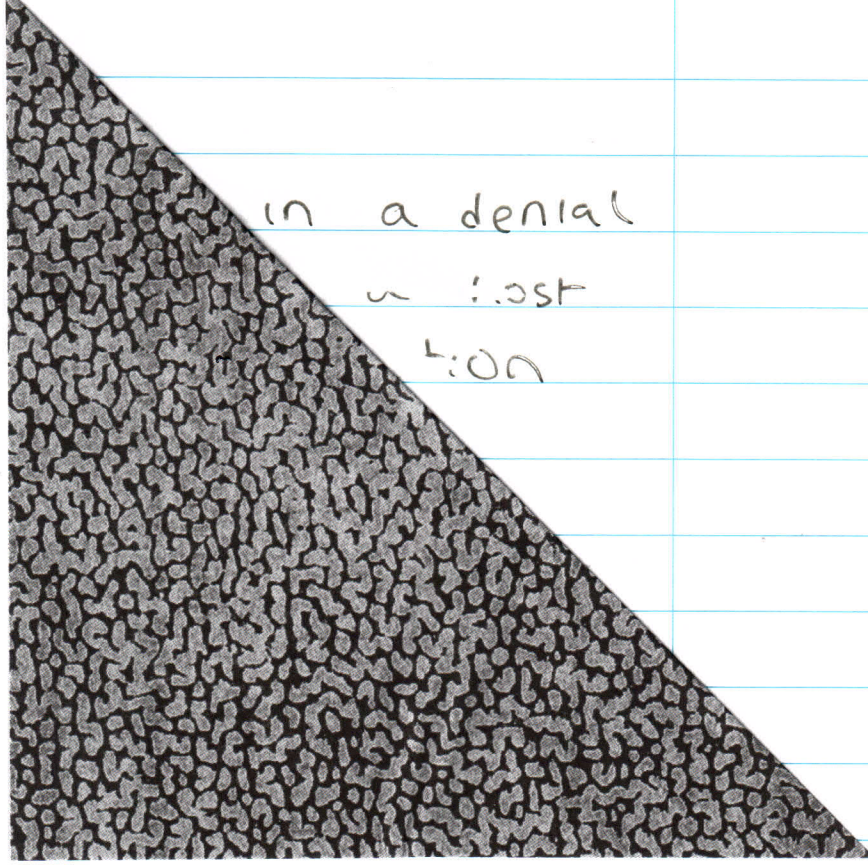
Subsequen Years = 3500

20

go insurance IF can afford MLS

375

Coláiste na hOllscoile
Corcaigh
University College Cork



Uimhir Scrúdaithe
Examination Number 9 1 7 1 6 3

Module Code CS4615

Paper No. _____

Mír
Section _____

Do na Scrúdaitheóirí amháin **For Examiner's use only**	
1	29
2	24
3	20
4	
5	
6	
7	
8	
9	
10	
11	
12	
13	
14	
Iomlán **Total**	73

Calculator, Please state:	No. of Books submitted
Name Casio	
Model Fx911es	

Note: If there are different sections on this paper, a separate Answer Book MUST be used for each section.

Q1

A A Syn Flood can result in a denial of service attack because a host must maintain state information for each connection (half open). A host is able to maintain a limited number of these half open connections and once this limit is reached further connection attempts will be ignored until previous connections are timed out or established and the host has more room to maintain the new connections

Normal 3 way handshake

1	S -> D	SYN(x)	
2	D -> S	ACK(x+1) SYN(y)	
3	S -> D	ACK(y+1)	

6

After msg 2 D must maintain who it sent SYN(y) to

An attack			Mitigation SYNcache
1	S -> D	SYN(x)	SYNKill, SYNcookies
1	S' -> D	SYN(x')	Tough to block as attacker
1	S'' -> D	SYN(x'')	may spoof IPs
1	S''' -> D	SYN(x''')	← D must now maintain

Q1 b

Example Program

```
int main(argc, argv) {
    char[6] buffer = alloc(6, char)
    strcpy(buffer, argv[0]);
}
```

This Program is vulnerable to attack as it copies the contents of argv[0] a user argument into a fixed size buffer. of len 6. If a user constructs a value for argv that is bigger that 6 chars it will overflow and overwrite other items on the stack one of these items includes the FRAME Pointer which instructs the program where to start executing after a function returns. If this can be changed to place where we have executable code we can get this program to run code that was not part of it using the same access rights it has. Particullary dangerous if this program is setuid root

Mitigation: Canary words. NX bit (no execute bit if supported) and bounds checking

6

Q1

c By including the current directory in your path variable if you type the name of any executable file in the current directory it will execute it.

Example

/shared_area/

contents

- a program called "ls" placed by attacker
- some other files

As alice has . in her path at the start the shell will start looking in the current directory when she types an program name

if alice did

ls

while in /shared_area

The executable the attacker placed would be run instead of the ls in /usr/bin

6

Q1

D

Shadowing

Rule no.	src IP	src prt	dst IP	dst prt	action
1	192.168.1.1	*	*	*	Allow
2	192.168.1.1	*	*	80	Deny

These rules are meant to allow all traffic from 192.168.1.1 to all ports but port 80 however rule 2 is shadowed by rule 1 as it (rule 1) matches all of rule 2

6

Q1

E A botnet is a collection of compromised hosts controlled by a malacious entity. They can be used for a number of reasons including DDOS, Proxying, and information gathering These hosts take commands from their controller and execute them

Yes and NO. botnets require network access to acquire commands and communicate with their controller IF a Firewall was able to block these commands the host in the botnet would not receive any further instructions and may lay dormant. however blocking the network traffic from a botnet is difficult as it can be made to look like normal traffic using tunnelling.

5

Q2

A

grant codebase "http://stockbroker.com/sMgmt.jar" {

Java.IO.FilePremission READ WRITE /portfol

3

grant codebase "Summary.Jar"

5

signed-by "stockbrocker-com" {

Java.IO.FilePremission READ WRITE /portfol

3

3

Q2

B Advice.Jar would have the Followins Security policy

```
grant codebase "http://rastag.com/Aduke.Jar" {
    Com.stockbroker.SummaryPermission
};
```

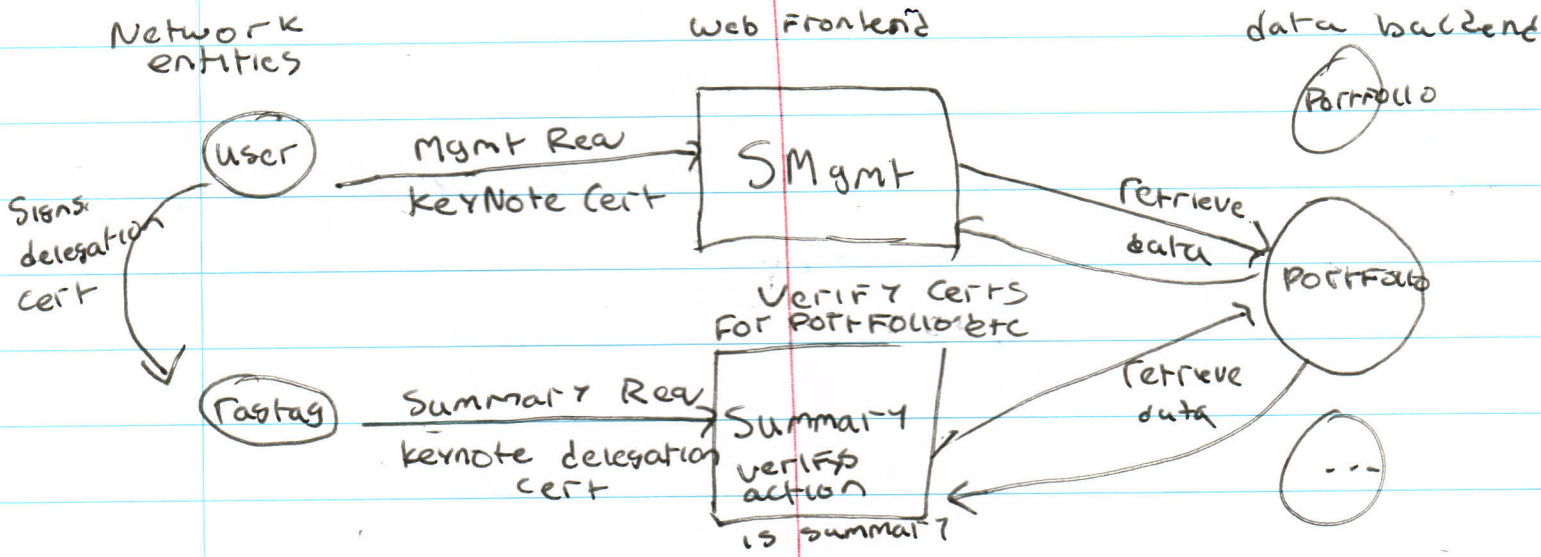
Summary.Jar would do the Followins in the Following example method getSummary

```
String getSummary() {
    SecurityManager sm = System.getSecurityManaser()
    IF (sm == Null) {
        Raise newException("SecurityManager not
                            Present, Exitins...")
    }
    sm.checkPermission(new SummaryPermission());
    Checks if caller has Summary Permission,
    Exception if not
    AccessController.doPrivilidged(
        //Method to read PORTFOLIO File is alle
    )
    do Privilidged is needed as we
    want to stop the AccessController From
    looking for the FilePermission For PORTFOLIO
    return Data From the caller of getSummary()
    as it might not have it
}
```

10

Q2

C A trust management system could be used to control access as follows



Stockbroker would issue the followins cert to user

Licensee : user_key

APPdomain : stockbroker

conditions : Portfolio = user_portfolio_ID

Signed by: stockbroker_key

local-constants : keys of entitys above

User would decegate summary permissions to rastas as follows

9

Licensee : rastas_key

Conditions : Action = Summary

Signed by: User_key

24

Policy at SMgmt and summary will accept all certs by stockbroker key