CS4615 – Summer 2014 Answers

1. a) Explain how a SYN-flood can result in a denial of service attack. *(6 marks)*

Answer

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

b) Give an example of a C program that contains a stack smashing attack. Assuming that you have available a suitable input string that can generate this attack in your program, explain how it might be used to compromise a system. *(6 marks)*

Answer

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

c) Alice includes the current directory "." in her shell path on the `cs1.ucc.ie` Unix server:

```
PATH = .:/usr/local/bin:/usr/bin:/bin:/usr/X11R6/bin:/usr/lib/java/bin
```

How might an attacker use this to compromise Alice's account? *(6 marks)*

Answer

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

d) Give an example of an iptables firewall policy that contains a shadowing anomaly. Explain your answer. *(6 marks)*

Answer

Q1 Shadowing

D

Rule no.	src IP	src Port	dst IP	dst Port	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

e) What is a *botnet*? Would a firewall prevent the operation of a botnet? Explain your answer. *(6 marks)*

(30 Total marks)

Answer

A botnet (also known as a zombie army) is a number of Internet computers that, although their owners are unaware of it, have been set up to forward transmissions (including spam or viruses) to other computers on the Internet. Any such computer is referred to as a zombie - in effect, a computer "robot" or "bot" that serves the wishes of some master spam or virus originator.

A properly configured Firewall may help protect against botnets, but attackers are evading firewall rules by using modified IRC server programs (as commonly used IRC ports are blocked) such as web-based control channels which are harder to filter, as the bots are mixed in with other legitimate connections.

c 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.

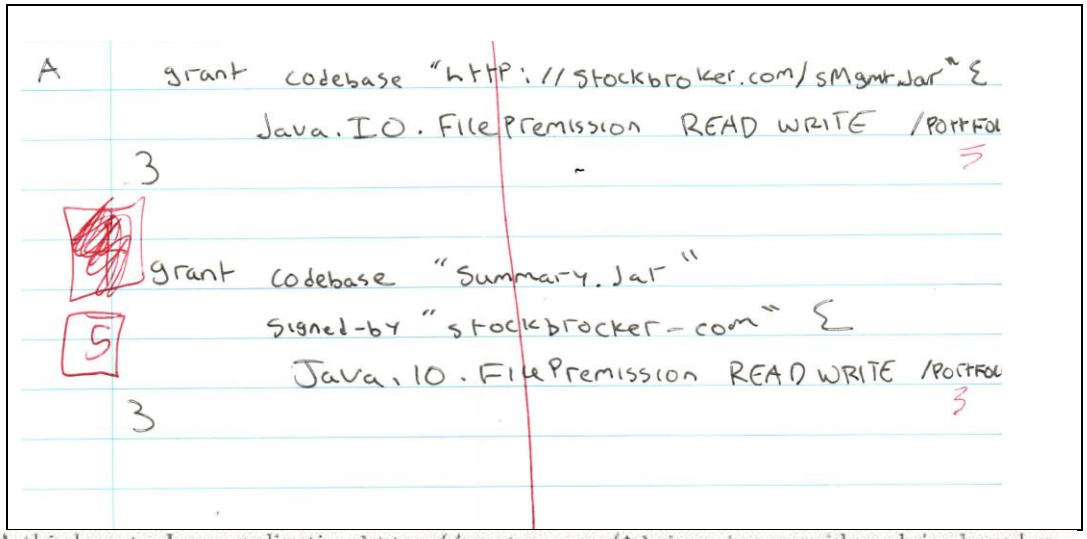
5

---

2. When a client visits `http://stockbroker.com/SMgmt.jar`, a stock management application is downloaded and executes in the client's Java VM. This application uses (`RW` access) a local file `portfolio` on the client's workstation to store data on the client's stocks. The stockbroker provides a further Java application `Summary.jar` that returns stock summary detail based on the data it reads from the local client `portfolio` file.

   a) Write Java security policy rule(s) that permit the stockbroker's applications to have the necessary access to the portfolio file. *(5 marks)*

Answer ???



b) A third party Java application `http://ragtag.com/Advice.jar` provides advice based on a stock portfolio summary. When executing in the client Java VM, it invokes `Summary.jar` (from stockbroker) and generates investment advice based on the summary data.

Outline how the Java security manager can be used to ensure that this advice application may not have direct access to the `portfolio` file, but may still generate its advice by invoking `Summary.jar`. Your answer should include: a suitable Java security policy; an outline of how a new Java permission is declared and used by `Summary.jar`, and whether `Summary.jar` should be treated as a privileged operation. *(10 marks)*

Answer

B Advice.Jar would have th Followins Security Policy

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

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

```
String getSummary() {
    SecurityManager sm = System.getSecurityMan
    IF (sm == Null) {
        Raise newException("SecurityManager no
                            Present, Exitins...")
    }
    sm.checkPermission(new SummaryPermission
    Checks if caller has Summary Permission,
    Exception if not
    AccessController.doPrivilidged(
        //Method to read PORTFOLIO File is alled
    )
    do Privilidged is needed as we
    want to stop the AccessController From
    looking for the FilePermission For PORTFOLIO
    Return Data From the caller Of getSumm
    as it migh not have it
}
```

B Advice.Jar would have the Followins Security Policy

```
grant codebase "http://ragtag.com/Advice.jar" {
    com.stockbroker.SummaryPermission
};
```

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

```
String getSummary() {
    SecurityManager sm = System.getSecurityManager()
    IF (sm == Null) {
        raise newException("SecurityManager not
                            present, Exiting...")
    }
    sm.checkPermission(new SummaryPermission());
    Checks if caller has Summary Permission,
    exception if not
    AccessController.doPrivileged(
        // Method to read PORTFOLIO File is called
    )
    do Privileged 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

c) The stockbroker decides that it will no longer use mobile code and, instead, hosts client data and application execution on its own servers. `SMgmt` and `Summary` become network services to which clients and ragtag may direct their requests.

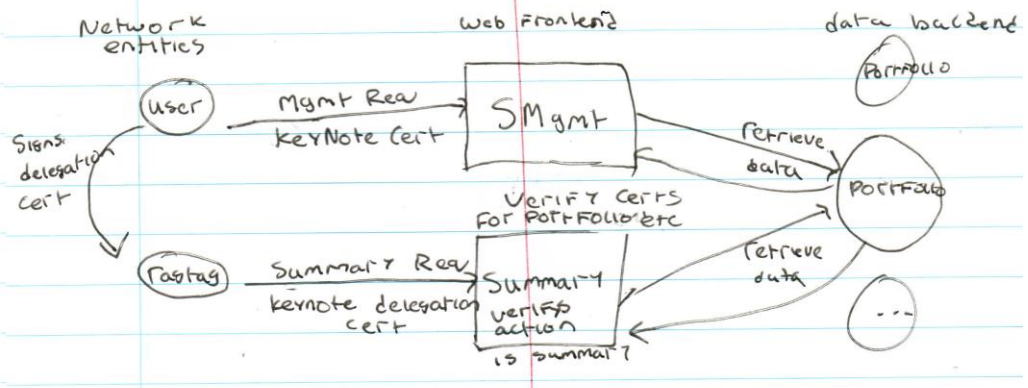
Outline how a Trust Management system could be used to control client access to these services. You answer should include examples of suitable KeyNote credentials. *(10 marks)*

(25 Total marks)

Answer

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

3. The stockbroker in Question 2 moves to offer banking services in addition to stockbroking services. For simplicity, all client data records are managed in database table $R(id, client, data)$ whereby each record of (bank or stock) *data* has a unique identifier *id* (primary key). Strict separation (no information flow) between banking and stock data is required. A Chinese Wall policy is applied to banking and stockbroking divisions: an employee may only access banking data or stock data, but not both.

   a) Describe how multilevel security (MLS) can provide a high-degree of assurance for this system. Your answer should include a revised database table (with sample tuples), rules that govern table querying and insertion, and sample employee clearances. *(10 marks)*

Answer

- With the use of Multi-Level Security (MLS), a DBMS can allow subjects with different security clearances to simultaneously access objects with different security levels.
- The Security clearances and security levels typically considered are: Top Secret (TS), Secret (S), Confidential (C) and Unclassified (U).
- MLS allows subjects with higher security clearance to easily allow access objects with equal or lower security level.

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
```

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

5

b) Give an example of a covert channel that permits a Trojan Horse to signal *two bits* of stock data to an employee in the banking division. Describe how the channel should be closed. *(5 marks)*

Answer

Trojan horse running as stock classification would do the following:

First the trojan horse and the recepient 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 recepient 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 received 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

c) A breach of the Chinese Wall/failure of the security mechanism in Question 3(a) would cost the stockbroker €500,000 in fines and loss of reputation. The stockbroker has a choice: either host both banking and stocks services on a single high-assurance MLS system (costing €5,000) following the design in Part (a), or host stocks on one conventional server and and banking on a separate conventional server (each costing €250). The probability of such an attack on the conventional systems configuration is 0.01; this is reduced to 0.001 if the MLS configuration is used instead. Use this information to carry out a *Risk Assessment* and advise the stockbroker on the best option.

Suppose that insurance could be purchased for €500 per annum (regardless of system) that covered €200,000 in the event of a security failure. How would you revise your advice?

(10 marks)

(25 Total marks)

Answer ???

Risk assessment

$Risk_{conventional} = 0.011$ | $Cost_{conventional} = 250+250$

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

$Loss_{conventional} = €5000$

$Loss_{MLS} = €500$

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 savins 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't afford MLS