Computer Security 1, COMPGA01, 2011-12 **ANSWERS PAPER, CONFIDENTIAL**

Answer ALL questions. 2.5 hours.

Correct answers should be short, straightforward and clear, rather than long and obscure.

Marks for each part of each question are indicated in square brackets

Calculators are NOT permitted

Question 1. Questions about theory and mathematical models.

1. What is an order relation? Is a relation over integers where each element is related only to itself an order relation? Is it also a lattice?

   [5 marks]

   It should satisfy the three axioms which start with RAT: Reflexive, Antisymmetric, Transitive. Yes, it is a partial order relation. Not a lattice, because $GLB(1,2)$ is not defined.

2. Given a poset $A, \leq$ give an exact **mathematical** definition of LUB (defined as a certain element of a certain set satisfying certain properties). Explain the acronym LUB.

   [5 marks]

   LUB = Least Upper Bound. $LUB(a,b) = Min_{\leq}\{x \in A | x \geq a \text{ AND } x \geq B\}$

3. Let $\mathbb{N}, |$ be a poset where $|$ is the division relation. Show that $|$ is not a total order. Compute $LUB(5,12)$ and $GLB(4,6)$.

   [5 marks]

   $LUB(5,12) = 60$ and if it was a total order it would be either 5 or 12. We have $GLB(4,6) = 2$.

THIS IS THE ANSWERS PAPER, NOT TO BE PRINTED, CONFIDENTIAL

4. Given a lattice of type $C = P(Cat)$, and a totally ordered set of classifications H write a definition of the Bell-LaPadula product lattice.

[5 marks]

Let H be a set of classifications with a total ordering $\leq_H$, and let Cat be a set of categories, and let $C = P(Cat)$ be a set of compartments, being arbitrary subsets of Cat. The Bell LaPadula product lattice is defined as a poset $H \times C, \leq$ where $\leq$ is defined by:

$$(l_1, c_1) \leq (l_2, c_2) \iff l_1 \leq_H l_2 \ \wedge \ c_1 \subseteq c_2$$

5. Can one make a program that always says Y when a file contains a virus?

[5 marks]

Yes for example a program which always says Y for any file.

[Question 1.6 is on the next page]

6. In Biba's integrity model we have three integrity levels

   $L = \{Untrusted(UN) < UserSpace(US) < SystemHigh(SH)\}$. Imagine that files on a USB stick are at the $Untrusted(UN)$ level, user files and third-party software such as Adobe Acrobat on a PC are at the $UserSpace(US)$ level, and the OS runs at the highest integrity level. Consider the following set of categories

   $$Cat = \{SensitiveWorkFiles(S), PersonalData(P)\}.$$

   Let Bob be a subject with $\lambda(Bob) = (SH, \{S\})$ and let $\lambda(document1) = (UN, \{P\})$. Imagine that Bob runs Adobe Acrobat and tries to open document1 to read it.

   Is this operation allowed with the strict Biba model?

   Is this operation allowed with LWM = Low Water Mark policy for subjects?

   What happens with the Integrity Audit policy?

   [5 marks]

   In strict Biba policy it is not allowed (no read down, read only up). With LWM = Low Water Mark policy for subjects the operation is allowed and the integrity level of Bob will change to $\lambda(Bob) = (UN, \{\})$ to mark the fact the software currently running may have been contaminated by low-integrity data. With the Integrity Audit policy all operations are permitted and only changes in λ need to be recorded, and $\lambda(Bob)$ will change in the same way as above.

   [Total 30 marks]

Question 2. Small questions about OS and computer security.

1. What is the meaning of the exe permission for directories in Unix?

   [5 marks]

   Allows to CD to that directory which makes it the current working directory, and traverse the directory to explore sub-directories. In order to read a file it is necessary to have an 'x' permit to all directories on its path.

2. Explain what sticky bit is. When does it apply?

   [5 marks]

   Directories only, letter t or T if x absent. Last group. Even if the directory is writable by all, for example /tmp, still only the owner of the file, or owner of the directory, or root [frequently also a superuser] can remove or rename files contained in /tmp

3. In Unix, when an ordinary process is run by a user, does it have the access rights of the user, or the rights of its owner? Give one example of an executable which has additional privileges and behaves differently.

   [5 marks]

   By default, programs run with the permissions of their caller. Notable exceptions are setuid programs and setgid programs which are allowed to use the permissions of the owner or the group owner, and also to change the euid or guid at runtime.

   [Questions 2.4-2.8 are on the following pages]

4. Consider the following Unix file listing:

```
bash> ls -l /etc/shadow
-rw-r-----  1 root shadow  680 Dec  16 22:02 shadow
```

Is it possible to be able to run a dictionary attack on the passwords of all users, this without obtaining root access? Explain why.

[5 marks]

A program run by a person who is not root, but is a member of the group 'shadow' can read this file, but cannot write it. So he can run a dictionary attack against it.

5. Give just one example how the hard drive file system affects the security in a multi-user setting.

[5 marks]

If the file systems is FAT32, Windows XP will not encrypt files, and will not allow one to block access to files based on user permissions, because FAT32 does not implement user permissions at all.

6. In Windows implementation of Access Control Lists (ACL's), each object (example file) has a security descriptor, which contains a list of Access Control Elements (ACE) objects. What kind of data does one ACE contain? Are these ACE objects stored in the object's directory of the hard drive, in system directories, user data files, in RAM, or in the registry?

[5 marks]

One ACE will contain, for one user, group or another type of SID = Security Identifier, (for example SID="local system") an encoding for the set of rights which is allowed for this SID. They are stored in the object's directory, together with the file, as file attributes accessible and visible in totality only to the system.

7. Explain how in compiled C code, a program will call a sub-routine, and store some pointers on the stack using PUSH and PULL instructions, and how this can be exploited to run arbitrary code.

[10 marks]

When a program will call a sub-routine, it will write on the top of the stack the parameters of the routine, then the return address, (then a saved pointer to a bottom of the stack; which is not so important) and then in the space above, local variables will be created and used when running this "C" language routine. If we overwrite these local buffers with longer data downwards, we can overwrite the return address of the sub-routine to make it jump, after it finishes, to a memory location chosen by the attacker. If in addition this location contains machine code injected by the attacker into the same buffer, this code will be executed.

8. State the main objective of Memory Protection in modern PCs. Explain in which cases data in some parts of the memory can be prevented from being executed. Is Internet Explorer 8 run under windows Vista likely to be protected against execution of assembly code injected in a buffer allocated on the stack?

[5 marks]

One process should not be able to access memory of other processes. By extension it shouldn't be able to access kernel/system memory. Achieved by segmentation and paging and made possible by Intel CPUs starting from 386. For decades the execution prevention existed only in high-end Intel CPUs and professional OS's but in commercial PCs such as using Windows XP the protection existed only at segment level, not at the page level.This has been fixed with Data Execution Prevention (DEP) in late versions of Windows XP which works however only if the OSs, the motherboards and the exe itself are compatible and enable DEP. If Internet Explorer 8 is run under windows Vista or better, and if this is run on a recent PC, it should in most cases run with DEP.

[Total 45 marks]

Question 3. Consider the network illustrated in the Figure on the next page. We want to configure a simple stateless firewall with 3 zones. It should be a simple packet filter which inspects the IP and TCP headers and has no memory of previous packets. It should be able to prevent connections from being initiated from the 'wrong' side by checking if a certain appropriate flag in the header of packets is set. It should enforce the following policies:

1. any external client is allowed to connect to the Web server via the https protocol (tcp/443);
2. subnet1 is allowed to connect to the FTP server via the ftp protocol (protocol=tcp/port=21 for commands; tcp/20 for data);
3. any internal machine is allowed to connect to the Web server with ssh (tcp/22);
4. packets coming from the Internet showing a source IP included in the Internal IP addresses must be explicitly denied;
5. any other connection (both directions) not explicitly authorized by the rules must be blocked (for example telnet, mail http and many other types of insecure traffic are banned).

Implement this policy by filling a table with a certain number of firewall rules such as the example given. The correct answer expected contains a total of 10 rules.

Direction	IP Source	IP Dest	Protocol	Port Source	Port Dest	Flag ACK	Action Taken
Internet →DMZ	any	34.123.145.6	TCP	$\geq$1024	443	any	permit
Intranet →DMZ							

[The figure appears on the next page]

[Total 25 marks]

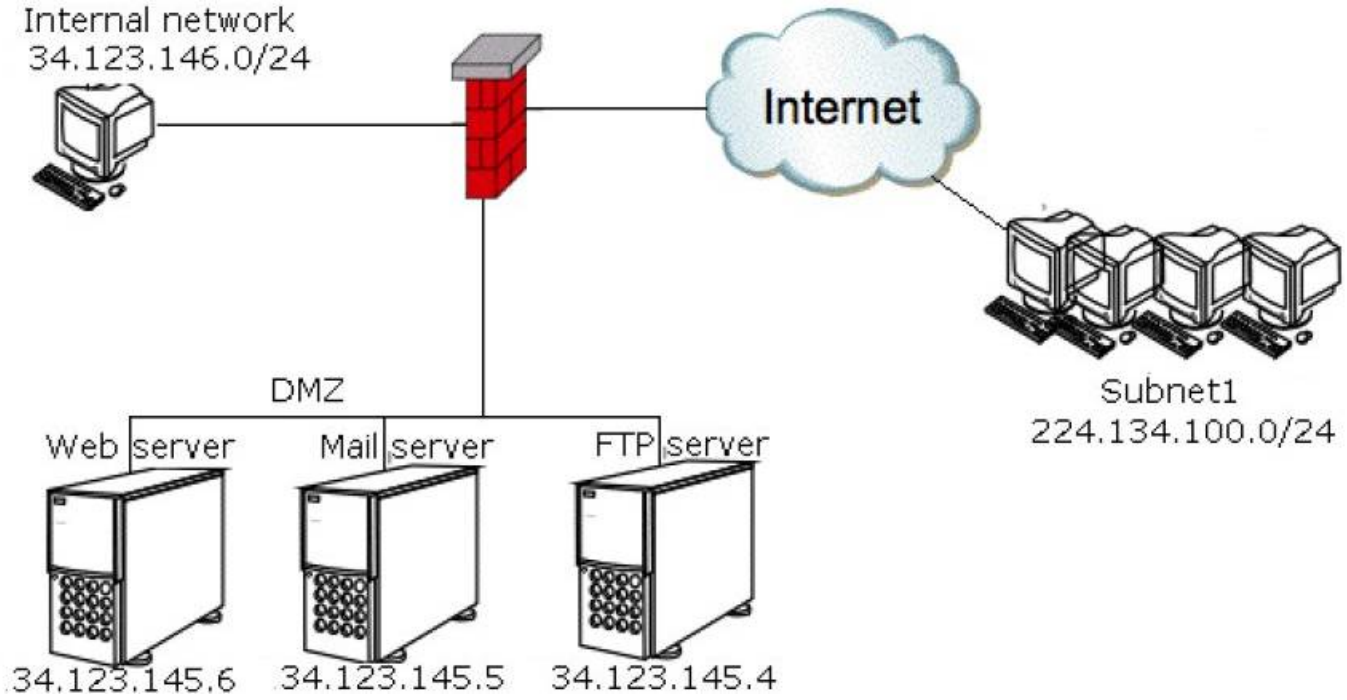

Figure 1: The network for Question 3.

[Total For The Whole Exam 100 marks]

Solution to Question 3.

Direction	IP Source	IP Dest	Protocol	Port Source	Port Dest	Flag ACK	Action Taken

Any external client is allowed to connect to the Web server via https (443):

The flag ACK in the second rule (and similar elsewhere) will drop out packets without ACK.

Here below: it is NOT necessary to initiate HTTPS connections (SYN=1 ACK=0) by the server.

Here and elsewhere, whatever is unnecessary should be blocked.

Internet →DMZ	any	34.123.145.6	TCP	≥1024	443	any	permit
DMZ→ Internet	34.123.145.6	any	TCP	443	≥1024	ACK=1	permit

Only subnet1 is allowed to connect to the FTP server, ports 21 and 20:

Internet →DMZ	224.134.100.0/24	34.123.145.4	TCP	≥ 1024	21	any	permit
DMZ→ Internet	34.123.145.4	224.134.100.0/24	TCP	21	≥1024	ACK=1	permit
DMZ→ Internet	34.123.145.4	224.134.100.0/24	TCP	20	≥1024	any	permit
Internet →DMZ	224.134.100.0/24	34.123.145.4	TCP	≥1024	20	ACK=1	permit

Any internal machine is allowed to connect to the Web server with ssh (tcp/22):

Intranet →DMZ	34.123.146.0/24	34.123.145.6	TCP	≥1024	22	any	permit
DMZ→ Intranet	34.123.145.6	34.123.146.0/24	TCP	22	≥1024	ACK=1	permit

Packets coming from the Internet showing an internal source IP must be denied:

Internet →any	34.123.146.0/24	any	any	any	any	any	deny

Email, http and any other connection not explicitly permitted is blocked:

any	any	any	any	any	any	any	deny

THIS IS THE ANSWERS PAPER, NOT TO BE PRINTED, CONFIDENTIAL

END OF PAPER