OLLSCOIL NA hÉIREANN
THE NATIONAL UNIVERSITY OF IRELAND, CORK

COLÁISTE NA hOLLSCOILE, CORCAIGH
UNIVERSITY COLLEGE, CORK

SUMMER EXAMINATION 2012

CS4615: Computer Systems Security

Professor Ian Gent,
Professor J. Bowen,
Dr. S.N. Foley

Answer *all* questions

1.5 Hours

1. a) Discuss effectiveness of code-signing in preventing malicious software. *(6 marks)*

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

   c) Which of the following C programs are vulnerable to a stack smashing attack? Outline how the selected program enables the attack to be carried out. *(6 marks)*

```
void main1(int argc, char* argv[]){
   char buffer[6];
   strcpy(buffer,argv[0]);
}/*main1*/
```

```
void main2(int argc, char* argv[]){
   char buffer[6];
   strcpy(buffer,"long text");
}/*main2*/
```

   d) Give an example of how the Access Matrix Model can be interpreted in terms of *access control lists* and in terms of *capabilities*. *(6 marks)*

   e) Describe the operation of the Setuid (suid) permission in Unix. *(6 marks)*

(Total 30 marks)

---

2. a) The java class `CreditCard` is used to manage credit card details stored in a user's workstation file `~/.mycreditcard`. The `CreditCard` operation

```
public String details(){ ... }
```

checks (via pop-up dialog box) with the user whether credit card details (in `.mycreditcard`) should be returned; if not, a null string is returned. When the user shops at `www.buy.com`, she uses the `www.buy.com/Checkout.jar` to pay for items selected; this applet invokes `CreditCard.details()` to obtain customer credit card details.

Outline how the Java security manager is used to ensure that the downloaded `Checkout` applet cannot access the user's credit card details without the permission of the user. Your answer should include: a suitable Java security policy and an explanation of how a new Java permission is declared and used by `details`, and whether `details` should be treated as a privileged operation *(15 marks)*

   b) Suppose that `buy.com` also offers a `checkout` application that a customer can manually download and execute. This application invokes a local application `creditCardDetails`. While these applications are implemented in C, and run natively on the customer's SELinux workstation, their behavior is similar to their Java counterparts in Question 2a. Outline how the Domain and Type Enforcement policy for this workstation might be configured to protect the user's credit card details. Your answer should include sample domains, types and domain definition table. *(10 marks)*

(Total 25 marks)

---

3. a) A multilevel secure system offers a document indexing system with the operations:

- assign(n,p,s): give the document (file) located at path p the name n.
- view(n,s): view the contents of the document with name n.

where s is the subject requesting the operation. Note that document names are unique across the system and are in addition to the name (path) given to the file containing the document. A table is used to store the name-path relationship, for example:

Name	Path
ExamPaper	/home/store/a
Attendance	/home/store/b
LectureNotes	/home/store/c

i. Sketch suitable algorithms that describe the behavior of the above operations taking care to ensure that multilevel security is preserved. *(10 marks)*

ii. Given that document names are unique in a table, explain how a Trojan-Horse running at top-secret could establish a covert-channel and signal one bit of information to a subject operating at unclassified. *(5 marks)*

b) A conventional (non-MLS) linux server currently hosts an email-service plus a service that is similar to that in Question 3a but is used only for top-secret documents.

The owner is concerned about Trojan Horse attack and estimates that, in terms of lost of reputation, among other things, unauthorized leakage of top-secret document information would cost $500,000, while unauthorized access to email would cost $10,000. The probability of such an attack on a conventional linux system that hosts both services is estimated to be 0.1. If the services were to be hosted on an MLS system then the probability of attack would reduce to 0.0001. Assume that an MLS system costs $5,000, while a standard linux server costs $500 and that their operational costs are zero.

Use this information to carry out a *Risk Assessment* and advise the company on how best to configure the system(s) and mitigate the risk of Trojan Horse attack. *(10 marks)*

(Total 25 marks)