OLLSCOIL NA hÉIREANN
THE NATIONAL UNIVERSITY OF IRELAND, CORK

COLÁISTE NA hOLLSCOILE, CORCAIGH
UNIVERSITY COLLEGE, CORK

Summer Examination 2013

CS4615: Computer Systems Security

Professor I. Gent,
Professor B. O'Sullivan,
Dr. S.N. Foley

Answer *all* questions

1.5 Hours

1. a) Give an example of an *Attack Tree* and outline its use. (*6 marks*)

b) Write a Java security policy rule that permits Bob's applet read and write access to files in `file:/usr/home/alice/data`. Note any assumptions you make. (*6 marks*)

c) Using a simple example of a policy rule, illustrate how the *Java Authentication and Authorization Service* (JAAS) extends Java's code-centric security policy model. (*6 marks*)

d) Discuss security compliance audit. Use the PCI-DSS Requirement 3.4 *"Render Primary Account Number unreadable anywhere it is stored [...]"* to illustrate your answer. (*6 marks*)

e) If security state matrix $M[s, o]$ defines the access that subject s has on object o then define the Bell and LaPadula axioms for multilevel security. (*6 marks*)

(*Total 30 marks*)

---

2. A programmer implements *Terry's Game* in C on Unix. Player high-scores are stored in the file `/etc/highscores`. The game is SUID root and is executable by all, the highscores file is owned by root and is readable and writable only by its owner.

a) Why is the game SUID root? What are the dangers of running the game as SUID root? Using a sample Domain Definition Table, explain why Type Enforcement (used in SELinux) can provide better protection. (*15 marks*)

b) The SUID root program described Part (a) above may take as parameter a path to a scores file (to override default `/etc/highscores` path). The program has behaviour:

```
void main (int argc, char* argv[]){    // the terryG program
     // argv[0] gives path to scores file
   ...// Step 0. play Terry's game and on completion,
   ...// Step 1. open scores file to obtain this player's last score;
   ...// Step 2. create/open temporary file stmp in same directory as scores;
   ...// Step 3. open scores file, copy contents to stmp and current score;
   ...// Step 4. close files and rename stmp as score file;
}
```

Explain how a player can carry out a race/TOCTOU attack on this program. (*10 marks*)

(*Total 25 marks*)

---

3. a) In order to defend against Denial of Service, the server hosting Terry's Game runs a modified three-way handshake: a connection request results in a response containing SYN cookie $h(ip_s, ip_d)$, given source IP ip_s, destination IP ip_d and one-way hash function $h()$.

Explain how a SYN cookie mechanism operates, outline its advantages and note any vulnerabilities in the design of the mechanism above. (*15 marks*)

b) Suppose that Terry's Game is hosted at IP 192.168.1.1 on Port 666 and a firewall is used to provide host access control. The firewall is configured with policy:

index	SrcIP	DstIP	SrcPort	DstPort	Action
1	192.168.2.*	192.168.1.1	*	666	drop
2	192.168.*.*	192.168.1.1	*	666	drop
3	192.*.*.*	192.168.1.1	*	666	allow
4	192.168.2.20	192.168.1.1	*	666	allow
5	*.*.*.*	192.168.1.*	*	666	drop

Identify any anomalies in the policy and discuss how they might be eliminated. (*10 marks*)

(*Total 25 marks*)
