OLLSCOIL NA hÉIREANN
THE NATIONAL UNIVERSITY OF IRELAND, CORK

COLÁISTE NA hOLLSCOILE, CORCAIGH
UNIVERSITY COLLEGE, CORK

Summer Examination 2005

Fourth Year Computer Science

CS4253: Computer Security

Professor M. Calder,
Professor G Provan,
Dr. S.N. Foley

Answer *Four* questions
Questions carry equal marks

Three Hours

1. a) A programmer wants to use DES Cipher Block Chaining to support both integrity and confidentiality. He implements the following scheme. He appends a block of nulls at the end of the plaintext message prior to encryption. If the block of nulls is not present after decryption then message has been corrupted. Outline an attack on this scheme, whereby an attacker can corrupt the ciphertext blocks without being detected. Describe how message integrity and confidentiality should be implemented. (*15 marks*)

   b) A secure webserver uses the standard C library random number generator `rand()`, seeded with a passphrase, as a stream cipher in order to provide simple group-based web-page security. Each group of users share a common passphrase k that is used to create and view shared web-pages, encrypted as $C = P \oplus \texttt{rand}(k)$. Comment on the effectiveness of this mechanism and discuss how a stream cipher might be properly used. (*15 marks*)

   c) A Bank's ATM cards have a magnetic strip on one side. This strip holds details about the account number and PIN (Personal Identification Number) of the customer. The Bank's IT department has decided that the fields

$$\{AccountID, PIN\}_{K_B}$$

   should be stored on this magnetic strip. This gives the $AccountID$ (an 8 byte value) and four-digit PIN, encrypted using DES-ECB by K_B, where K_B is a key known only to the Bank (and it's ATM machines). An ATM uses key K_B to validate the PIN, entered by the customer, against that on the ATM card before allowing any activity on the account.

   Outline a simple attack on this scheme, whereby a criminal can gain access to another customer's account and does not need to know the customer's PIN. Propose a improved scheme for ATM cards and briefly explain why your proposal is secure. (*15 marks*)

2. a) Explain the properties of a one-way cryptographic hash function. Collisions were recently constructed within the MD5 hash function; discuss the impact of this result. (*15 marks*)

   b) Explain the desirable properties for a digital signature scheme. Alice A (owner of public key K_A) sends a message to Bob B (owner of public key K_B) using message exchange,

$$A \rightarrow B : \{M, h(M)\}_{K_{ab}}, \{\{A, B, K_{ab}\}_{K_a^{-1}}\}_{K_B}$$

   where, $h()$ is a one-way hash function, $\{\ldots\}_K$ represents encryption using the key K, and K_{ab} is a session key generated by A. Comment on the effectiveness of this protocol. (*15 marks*)

   c) The web site `www.amadan.com` (A) uses the following protocol to secure the connection between customers (B) and its shop front.

$$\begin{array}{lll} \text{Msg1} & A \rightarrow B : & \{K_{AB}\}_{K_B} \\ \text{Msg2} & B \rightarrow A : & \{N_B\}_{K_{AB}} \\ \text{Msg3} & A \rightarrow B : & \{Cert_A, \{N_B\}_{K_A^{-1}}\}_{K_{AB}} \end{array}$$

   where K_B is B's public key, $Cert_A$ is an X509 certificate for A's public key K_A (private key K_A^{-1}) that is issued by a well known Certification Authority, and N_B a random nonce. K_{AB} is the proposed session key. Outline an attack on this protocol. Suggest how the protocol might be repaired. (*15 marks*)

3. a) If I was not too worried about Trojan Horses and covert channels how could I use the user-group policy mechanism in Unix to implement a rather crude form of multilevel security? Explain your answer and discuss its effectiveness. (*15 marks*)

   b) A Unix based implementation of the Tetris game maintains information on player scores in the file `/etc/scores`. The game is SUID root and is executable by all, the scores file is owned by root and is readable and writable only by its owner.

      i. Why is the game SUID root? Explain how the SUID permission operates. (*7 marks*)

      ii. Discuss the dangers of using SUID root and suggest a safer way of securing the program and file. (*8 marks*)

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

```
void main (int argc, char* argv[]){
  char scores[12];
  strcpy(scores, argv[0]);            // argv[0] gives path to scores file
  ...// Step 0. play game;
  ...// Step 1. open scores file to obtain user'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;
}
```

   Identify and explain potential security vulnerabilities in this design. (*15 marks*)

4. a) Sketch the operation of *TCP/IP wrappers*. Discuss the difference between this security mechanism and a conventional security kernel. (*15 marks*)

   b) Explain, using an example, how the low-water-mark mechanism provides flexibility, yet preserves integrity in the Biba model. Do you think a comparable mechanism providing a similar degree of flexibility (and security) could be introduced into the Bell LaPadula model? Explain your answer. (*15 marks*)

   c) A multilevel secure system that implements the Bell LaPadula model is configured with a partial ordering based on compartments `sales`, `admin` and `stock`. Most applications run as untrusted, except for a special trusted program `Stats` that is used to generate statistics from `sales` data and copy it to personnel files in the `admin` compartment.

      i. Give a diagram that specifies the partial order based on these compartments. (*4 marks*)

      ii. What is the difference between a *trusted* and *untrusted* subject? Why is it necessary to treat `Stats` as trusted? (*4 marks*)

      iii. Outline how a Type Enforcement mechanism can enforce the above multilevel security requirement. Explain why the Type Enforcement approach provides better support for the Principle of Least Privilege than the Bell LaPadula model. (*7 marks*)

5. a) A network printer P prints jobs from authorised users (U) submitted using the protocol:

$$U \rightarrow P: \quad [file, R, h(R, passwd)];$$

where $file$ is the file to be printed, R is a nonce, and $h(\ldots)$ a one-way hash function. Each authorised user shares a secret *passwd* with the printer. The following Java fragment gives the client-side of the protocol.

```
DataOutputStream out = ...      // stream to printer server
MessageDigest md= MessageDigest.getInstance("MD5");
byte[] passwd = "mypasswd";              // shared password
Random rangen = new Random(0);//java.util.Random generator-
byte[] R = new byte[1];            //-random seed used is 0
rangen.nextBytes(R);        // generate 1 byte random value
out.write(file);
out.write(R);                              // send to server
out.write(md.digest(passwd));
```

Identify and explain the security vulnerabilities in this protocol and implementation. (*15 marks*)

b) It is decided that it would be better to implement the Printer Server using the JAAS framework. The Printer Server `PrSvr.jar` includes the following code fragment.

```
LoginContext lc = new LoginContext("CS4253", new TextCallbackHandler());
lc.login();
subject s= lc.getSubject();
PrivilegedAction lpr= new PrintAction();
subject.doAs(s,lpr);
lc.logout();
```

where a `PrintAction` is a class that implements basic printing using the `getPrintJob()` method in the `java.awt.Toolkit` class Explain the operation of each line of the above code. (*15 marks*)

c) It is decided that the permission `PrintActionPermission` should be required to execute the `PrintAction`. Kerberos users `Alice@cs.ucc.ie` and `Bob@ee.ucc.ie` are permitted to use this printing service. Sketch how this should be implemented and how the Java security policy should be configured. (*15 marks*)