OLLSCOIL NA hÉIREANN
THE NATIONAL UNIVERSITY OF IRELAND, CORK

COLÁISTE NA hOLLSCOILE, CORCAIGH
UNIVERSITY COLLEGE, CORK

Summer Examination 2006

Fourth Year Computer Science

CS4253: Computer Security

Professor S. Craw,
Professor G Provan,
Dr. S.N. Foley

Answer *Four* questions
Questions carry equal marks

Three Hours

1. A server maintains details of users and their passwords in a file that is composed of a sequence of 16-byte records. Each record contains an eight byte user-id and an eight byte password, and is sorted by user-id. Client systems maintain their own copy of this file for local user authentication. Clients periodically obtain an encrypted copy of the password file across a public network. The file is encrypted with a secret `key` (known to server and all clients) using the following Java code.

```
Cipher cipher = Cipher.getInstance("DES/ECB/PKCS5Padding");
cipher.init(Cipher.ENCRYPT_MODE,key);
FileInputStream fin = new FileInputStream(passwdplain);
FileOutputStream fout = new FileOutputStream(passwdenc);
CipherOutputStream out = new CipherOutputStream(fout, cipher);

byte[] buffin new byte[1024]; int length;
while ((length = fin.read(buffin))!=-1)
  out.write(buffer,0,length);
fin.close; fout.close;
```

   a) Describe how a passphrase could be used to generate the key `key`. What is a dictionary attack on a passphrase? What defences should be used to make it harder to carry out a dictionary attack on pass-phrases? Explain your answer. (*15 marks*)

   b) Provide Java code that a client system could use to extract a plaintext copy of the encrypted password file. Explain its operation. (*15 marks*)

   c) Describe an attack on the above scheme whereby a user of a client system, who controls the network, can log in as another user. How can this attack be avoided? (*15 marks*)

2. Alice (A) wishes to communicate securely with Bob (B) and proposes a symmetric session key K_{AB}, a copy of which she intends to give to Bob. Trent is a trusted third party who provides a message translation service. Trent shares symmetric K_{AT} with Alice, and symmetric key K_{BT} with Bob. The following protocol is used to pass the key K_{AB} to Bob.

$$\begin{aligned} \text{Msg1}: &\quad A \rightarrow T: \quad B, N_A, \{K_{AB}\}_{K_{AT}} \\ \text{Msg2}: &\quad T \rightarrow A: \quad \{A, K_{AB}\}_{K_{BT}}, \{N_A\}_{K_{AT}} \\ \text{Msg3}: &\quad A \rightarrow B: \quad \{A, K_{AB}\}_{K_{BT}} \end{aligned}$$

   a) i. What is the difference between long term and session keys? (*4 marks*)

   ii. What is the intended purpose of the Nonce N_A in this protocol? (*4 marks*)

   iii. Extend the protocol to provide mutual authentication for Alice and Bob. (*7 marks*)

   b) Describe how the above protocol might be used to secure services provided over a distributed system. Your answer should consider the issues of authentication, authorisation and revocation. (*15 marks*)

   c) Illustrate how a third principle Eve (who shares a valid secret key K_{ET} with Trent) can subvert the protocol to get a copy of the key K_{AB} that Alice gives to Bob using this protocol. In addition, illustrate how Eve can subvert the protocol and masquerade as Alice to Bob, even when Alice does not initiate a key exchange with Bob. (*15 marks*)

3. A publisher provides subscriber-only web access to its newspaper. Subscription is free and users log in via an SSL-protected web-page, providing a subscriber user-id and password.

   a) Sketch the operation of the SSL protocol, what it is intended to achieve, and its suitability for this application. Note that it is not necessary to reproduce the exact SSL protocol messages. (*15 marks*)

   b) The login form is implemented by passing user login data to a backend DBMS application that checks the information from the table `UserTable(UserID,Email,Passwd)`. If the user enters just `userid` and selects the `ForgottenPassword` button then the application emails the corresponding password to the user. The backend query for this action is:

```
SELECT Email, Passwd
FROM   UserTable
WHERE  UserID = "$userid";
```

   Describe how an SQL-injection attack on this web-page could enable an attacker to login as another subscriber. How can this attack be avoided? (*15 marks*)

   c) Once the user is authenticated the server sets an authentication cookie in the browser of the user. Suppose that the application developer coded the cookie using Unix `crypt(UserID^K)` which encrypts a a block of nulls using the DES key `UserID^K` (the catenation of the user-id and a secret key `K` known only to the webserver, truncated to 56 bits). Outline an attack whereby it is possible for a subscriber to discover secret key K. (*15 marks*)

4. a) Briefly describe the Type Enforcement mandatory access control model. Use the problem of safeguarding against possible buffer overflows in applications such as web-browsers to illustrate your answer. Your answer should include a suitable Domain Definition Table. (*15 marks*)

   b) A multilevel secure system has only one printer which is used to print jobs at all security levels. It is in a secured area and printouts are carefully labelled. A multilevel secure (trusted) print queue manager accepts requests from subjects at any security level. Its operations are:

      i. `lpr <filename>`. Assign job number and add file to print queue. Returns `job#` to requester.

      ii. `lprm <job#>`. Remove specified print job. Returns `success` or `failure`.

   Sketch suitable algorithms that describe the behaviour of the above operations taking care to ensure that multilevel security is preserved. For the sake of simplicity it is not necessary to consider printer controls/scheduling. (*15 marks*)

   c) An application system has users A and B, Transform Procedures (TPs) $T1$ and $T2$, and Constrained Data Items (CDIs) X, Y and Z. It has authorisation triples $(A, T1, (X))$ and $(B, T2, (Y, Z))$ which must be preserved according to rule E2 of the Clark Wilson model.

      i. What application certification should be done given the above triples? (*5 marks*)

      ii. Describe how a Type Enforcement policy is configured to support this policy. (*5 marks*)

      iii. Suppose that a third user C may choose to always use either $T1$ *or* $T2$, but not both; once made, the choice cannot be reversed. Outline how this additional requirement might be supported. (*5 marks*)

5. a) Develop suitable Java security policy *grant* entries for the following requirements.

   i. Anybody may read and write files in `/tmp/`. (*5 marks*)

   ii. Any code signed by the public key `simon` may have read and write access to files under `/usr/home/simon/`. (*5 marks*)

   iii. *Any* jar files or classes from source `http://cs.ucc.ie` may have read access to any file in the directory `/usr/home/simon/cs`. (*5 marks*)

   b) 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. [Hint: treat `details()` as a privileged operation]. (*15 marks*)

   c) Given suitable public generator g and modulus n, principals A an B generate suitable secrets x and y, respectively, and engage in the Diffie-Hellman Key exchange.

$$\begin{array}{lll} \text{Msg1:} & A \rightarrow B & g^x \bmod n \\ \text{Msg2:} & B \rightarrow A & g^y \bmod n \end{array}$$

   i. How do A and B determine their shared key? (*4 marks*)

   ii. Explain why this shared key cannot be determined by some third party. (*4 marks*)

   iii. Extend the protocol to provide mutual authentication between A and B. (*7 marks*)