OLLSCOIL NA hÉIREANN
THE NATIONAL UNIVERSITY OF IRELAND, CORK

COLÁISTE NA hOLLSCOILE, CORCAIGH
UNIVERSITY COLLEGE, CORK

AUTUMN EXAMINATION 2009

Fourth Year Computer Science

CS4253: Computer Security

Professor Alan F. Smeaton
Professor J. Bowen
Dr. S.N. Foley

Answer *Four* questions
Questions carry equal marks

Three Hours

1. a) Explain the properties of a one-way cryptographic hash function. Explain how a one-way cryptographic hash function can be used to implement message integrity. *(15 marks)*

   b) 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 plain-text 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 cipher-text blocks without being detected. *(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. 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.

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

   a) What is the difference between long term keys and session keys? Describe how pass-phrase encryption might be used to provide long-term keys. *(15 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) Explain how a potential buffer overflow can result a Unix security vulnerability. Which of the following C programs have this vulnerability. Explain your answer. (*15 marks*)

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

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

   b) Describe how SYN flooding can cause a TCP/IP denial of service attack. Outline how SYN-cookies can provide a defense and comment on their effectiveness. (*15 marks*)

   c) A server S accepts exam papers from lecturers (L) when submitted using protocol:

$$L \rightarrow S: \quad [file, R, h(R, passwd)];$$

   where $file$ contains the exam paper, R is a nonce, and $h(\ldots)$ a one-way hash function. Each lecturer shares a secret $passwd$ with the exams office server S. The following Java fragment gives the client-side of the protocol.

```
DataOutputStream out = ...       // stream to exams 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 security vulnerabilities in this protocol/implementation. (*15 marks*)

5. a) Write a note on computer viruses, considering their operation and infection. Discuss the effectiveness of virus scanners and code-signing in defending against viruses. *(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 simple multilevel secure database management system is to be designed. Each tuple in a database table is assigned a separate security-level, and subjects at any security-level may access the table (but not necessarily every record in the table). For example, consider the following employee relation table (*emp-id* is primary key).

emp-id	*level*	Name
0031	topsecret	Mulder
0200	secret	Scully
1002	secret	Jones

Given the usual ordering between the specified security levels, a secret process may read the Scully and Jones' entries but not the Mulder entry, and so forth.

i. Propose suitable multilevel security rules that govern read/write access by subjects to table rows. You should assume that when a new tuple is inserted into the table it is assigned the security-level of the subject inserting it. *(7 marks)*

ii. Given that primary key values 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 secret. Suggest how the covert channel might be closed. *(8 marks)*