OLLSCOIL NA hÉIREANN
THE NATIONAL UNIVERSITY OF IRELAND, CORK

COLÁISTE NA hOLLSCOILE, CORCAIGH
UNIVERSITY COLLEGE, CORK

SUMMER EXAMINATION 2008

Fourth Year Computer Science

CS4253: Computer Security

Professor S. Craw,
Professor J. Bowen,
Dr. S.N. Foley

Answer *Four* questions
Questions carry equal marks

Three Hours

1. a) With respect to symmetric-key cryptography, explain the following terms: *known-plaintext attack, brute-force attack, dictionary attack,* and *pre-computation attack.* (*15 marks*)

   b) A secure email program uses (single) DES-CBC to encrypt messages sent over a public network. An eight-character user-password provides the secret key and a block of null values is used as initialization vector. Prior to encryption, a block of null values is appended to the *end* of the email message. This block is intended to act as a recognizer: if it is not present after decryption then the message has been corrupted.

   Discuss the security vulnerabilities in this application. (*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

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

   should be stored on this magnetic strip. This gives the $AccountID$ and a 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. (*15 marks*)

2. a) 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*)

   b) Suppose that we devise a very simple form of public-key certificate as follows. A certificate denoted $cert(A, keyA, keyB)$ is a statement by the owner of public key $keyB$ that the public key $keyA$ is owned by A.

      i. Outline how RSA could be used to implement this type of certificate. (*5 marks*)

      ii. Suppose that Alice owns the public key $keyA$. Alice holds certificates: $cert(B, keyB, keyA)$, $cert(C, keyC, keyA)$, $cert(D, keyD, keyE)$, $cert(E, keyE, keyB)$ and $cert(D, keyD, keyF)$. Can Alice trust key $keyD$? Explain your answer. (*5 marks*)

      iii. Suppose Alice also holds $cert(F, keyF, keyC)$, in addition to the certificates above, but she only marginally trusts (in a PGP-sense) $cert(B, keyB, keyA)$ and $cert(C, keyC, keyA)$. Can she still trust key $keyD$? Explain your answer. (*5 marks*)

   c) A server(A) uses the following protocol to secure client (B) connections.

$$\begin{array}{lll} \text{Msg1} & B \rightarrow A & Cert_B \\ \text{Msg2} & A \rightarrow B : & \{K_{AB}\}_{K_B} \\ \text{Msg3} & B \rightarrow A : & \{N_B\}_{K_{AB}} \\ \text{Msg4} & A \rightarrow B : & \{Cert_A, \{N_B\}_{K_A^{-1}}\}_{K_{AB}} \end{array}$$

   where $Cert_A$ is the X509 certificate (issued by a well known Certification Authority) for public key K_A (private key K_A^{-1}) owned by A, and similarly, $Cert_B$ is the certificate for B's public key. N_B a 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) 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*)

   b) Describe the Type Enforcement protection model. Using the Tetris program above as an example, explain how and why Type Enforcement can provide stronger protection than a SUID based mechanism. (*15 marks*)

   c) The SUID root Tetris program described Part (a) 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) 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*)

   b) Write a note on computer viruses, considering their operation and infection. Discuss the effectiveness the following techniques in defending against viruses: virus checkers, code-signing, security-kernels. (*15 marks*)

   c) An organization plans to deploy a Kerberos authentication server and a public web server on the same host system. They are considering using a multilevel secure system as host *or* implementing the deployment in terms of the Clark-Wilson model. Advise the organization and discuss the suitability, pros and cons of these approaches. (*15 marks*)

[over...]

5. a) 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*)

b) It has been suggested that the JAAS framework should be used to provide authentication for the exams office server. The Exam Server `ExSvr.jar` includes the following code fragment.

```
LoginContext lc = new LoginContext("ExamOffice", new TextCallbackHandler());
lc.login();
subject s= lc.getSubject();
PrivilegedAction post= new PostPaper();
subject.doAs(s,post);
lc.logout();
```

where `PostPaper` is a class that inserts (using `executeUpdate()` from `java.sql.*`) the paper into the exam paper database. Explain the operation of each line of the above code. (*15 marks*)

c) Instead of using JAAS, it has been suggested that it might be better to use Java SSL to secure the connection between the exam office server and lecturer workstations. Sketch how SSL should be used in this case and compare the advantages and disadvantages of your solution with the JAAS solution. (*15 marks*)