OLLSCOIL NA hÉIREANN
THE NATIONAL UNIVERSITY OF IRELAND, CORK
COLÁISTE NA hOLLSCOILE, CORCAIGH
UNIVERSITY COLLEGE, CORK

AUTUMN 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) 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. *(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) Explain why, after a simple Diffie-Hellman (DH) key exchange neither party knows who they are talking to and must authenticate each other in some way.

   What is wrong with the following protocol that uses a DH-exchange followed by a mutual authentication, where N_a and N_b are nonces generated by A and B, respectively and $K = g^{xy} \bmod n$. Propose a scheme to fix this weakness. Explain your answer.

$$\begin{array}{lll} \text{Msg1} & A \rightarrow B : & g^x \bmod n, N_A \\ \text{Msg2} & B \rightarrow A : & g^y \bmod n, N_B \\ \text{Msg3} & A \rightarrow B : & \{Alice, N_A + 1\}_K \\ \text{Msg3} & B \rightarrow A : & \{Bob, N_B + 1\}_K \end{array}$$

   where N_A and N_B are challenges and $K = g^{xy} \bmod n$. *(15 marks)*

3. a) Outline how password based login authentication works in Unix. Your answer should include an explanation of how *salt* helps defend against a dictionary attack. *(15 marks)*

b) Explain how a potential buffer overflow can result in 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*/
```

c) A particular 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 the E2 rule of the Clark Wilson model.

i. What application certification should be done given the above triples? *(3 marks)*

ii. Describe how access control in standard Unix should be configured to support this policy. Note any potential security weaknesses in this implementation. *(7 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 could be supported *(5 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 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 two bits of information to a subject operating at secret. (Hint: recall the multilevel file-system discussed in lectures). Suggest how the covert channel might be closed. *(8 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);
out.write(md.digest(passwd));                  // send to server
```

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)*

We need to declare a new permission object

```
public final class PrintActionPermission extends BasicPermission{
super(); }
```

and in the PrintAction class we need to check for this permission before submitting the job.

```
SecurityManager sm = System.getSecurityManager();
if (sm!=null) {
  sm.CheckPermission(new PrintActionPermission())
}
[...] submit the job;
```

The security policy configuration file will include:

```
grant codebase "file:./PrSvr.jar"
 Principal javax.security.auth.kerberos.KerberosPrincipal "Alice@cs.ucc.ie"
 permission PrintActionPermission();
grant codebase "file:./PrSvr.jar"
 Principal javax.security.auth.KerberosPrincipal "Bob@ee.ucc.ie"
 permission PrintActionPermission();
grant codebase "file:./PrintAction.class"
 permission java.lang.RuntimePermission ''queuePrintJob'';
```

Note I'm looking for a *sketch* and explanation here: I do not expect syntax/name -perfect answers.