OLLSCOIL NA hÉIREANN
THE NATIONAL UNIVERSITY OF IRELAND, CORK

COLÁISTE NA hOLLSCOILE, CORCAIGH
UNIVERSITY COLLEGE, CORK

SUMMER EXAMINATION 2001

Fourth Year Computer Science

CS 4253: Computer Security

Professor J. G. Hughes,
Professor C. J. Sreenan,
Dr. S.N. Foley

Answer *Four* questions

Three Hours

1. (a) Explain the desirable properties of a *one way hash* function. Describe how such a function is used to protect passwords in the Unix system, and discuss the benefits of taking this approach. (*8 marks*)

(b) 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. (*8 marks*)

(c) The following protocol is used to authenticate a client C to a server S. Both principles share secret *pass*, R is a random challenge, and $h()$ is a one-way hash function.

$$\begin{aligned} \text{Msg1}: &\quad S \rightarrow C: \quad R \\ \text{Msg2}: &\quad C \rightarrow S: \quad h(R, pass) \end{aligned}$$

The following Java code fragment from the server-side of this protocol reflects a number of (poor) implementation decisions. You may assume that the client-side uses similar implementation decisions.

```
MessageDigest md= MessageDigest.getInstance("MD5");
DataOutputStream out = ...   // stream to connecting client
DataInputStream in = ...   // stream from connecting client
byte[] passwd = ...                        // 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(R);                               // send to client

byte[] hashR = new byte[16]; in.readFully(hashR);
byte[] hashpass = new byte[16]; in.readFully(hashpass);
if (MessageDigest.isEqual(hashR,md.digest(R))
   && MessageDigest.isEqual(hashpass,md.digest(pass)))
    ...                                 // client authenticated
```

Identify and explain the security vulnerabilities in this implementation. Outline how the code should be repaired. (*9 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.

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

(a) What is the difference between long term and session keys? Describe how pass-phrase encryption might be used to provide long-term keys. How can salt be used to make such encryption more robust against attack? (*8 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, authorization and revocation. (*9 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. (*8 marks*)

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

i. Anybody may read and write files in `/tmp/`. (*2 marks*)

ii. Any code signed by the public key `simon` may have read and write access to files under `/usr/home/simon/`. (*2 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`. (*2 marks*)

(b) Suppose that we devise a very simple form of public-key certificate as follows. A certificate denoted $cert(A, keyA, keyB)$ states that the public key $keyA$ is owned by A and has been signed by (the private key corresponding to public key) $keyB$.

i. Suppose that Alice owns the public key $keyA$ (she owns private $keyA^{-1}$). 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. (*4 marks*)

ii. 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. (*4 marks*)

(c) Alice and Bob use a Diffie-Hellman key exchange protocol to establish a shared key K:

$$\begin{aligned} \text{MsgA}: &\quad A \to B: \quad g^x \bmod n \\ \text{MsgB}: &\quad B \to A: \quad g^y \bmod n \end{aligned}$$

where x and y are secrets known only to A and B, respectively, and suitable generator g and modulus n are publicly known.

i. How is K derived? Why is it known only to A and B? (*3 marks*)

ii. Why does this protocol not provide authentication? Propose an extension to the protocol that uses public key certificates to provide authentication. (*4 marks*)

iii. Propose an extension to the protocol that supports a key exchange between three principles. (*4 marks*)

4. (a) Describe the access-control mechanism that is used in Unix, paying particular attention to the permissions that are provided and their properties. (*7 marks*)

(b) Explain how a potential buffer overflow can result a Unix security vulnerability. Which of the following C programs have this vulnerability. Explain your answer. (*8 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 authorization 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? (*2 marks*)

ii. Describe how access control in standard Unix should be configured to support this policy. Note any potential security weaknesses in this implementation. (*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 could be supported (*3 marks*)

5. (a) 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. (*7 marks*)

(b) Briefly describe the Type Enforcement mandatory access control model. Use the problem of safeguarding against malicious mobile code down-loaded by your browser to illustrate your answer. Your answer should include a suitable Domain Definition Table. (*8 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. (*5 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. (*5 marks*)