OLLSCOIL NA hÉIREANN
THE NATIONAL UNIVERSITY OF IRELAND, CORK

COLÁISTE NA hOLLSCOILE, CORCAIGH
UNIVERSITY COLLEGE, CORK

Summer Examination 2011

Fourth Year Computer Science

CS4253: Computer Security

Dr C. Shankland,
Professor J. Bowen,
Dr. S.N. Foley

Answer *Four* questions
Questions carry equal marks

Three Hours

1. A secure email client (Alice) encrypts an email message M as $\texttt{rand}(K) \oplus M$, where K is a secret shared with the intended recipient (Bob), `rand()` is the standard Unix pseudo-random number generator and $\oplus$ is a bitwise XOR operator.

   a) Comment on the effectiveness of this scheme and and suggest a more appropriate scheme for providing message secrecy *and* integrity. (*15 marks*)

   b) Suppose that Alice (owner of public key K_A) uses the following key-exchange protocol with Bob (owner of public key K_B) in order to share the secret K that is to be used to encrypt the email message.

   $$A \rightarrow B : \{\{A, K\}_{sK_a}\}_{K_B}$$

   where, $\{..\}_{sK_a}$ denotes message signing by the owner of public key K_a and $\{..\}_{K_b}$ denotes encryption using public key K_b. Comment on the effectiveness of this protocol. Does it provide a digital signature scheme for email messages? (*15 marks*)

   c) Suppose that we devise a very simple form of PGP-style 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 (an email address).

      i. Describe how public key cryptography can be used to implement this certificate. (*8 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. (*7 marks*)

---

2. a) Describe the Access Matrix Model of security. Illustrate, using an example, how Unix access control lists (ACLs) can be represented in this model. Why is it reasonable to use this model to represent an access control policy mechanism? (*15 marks*)

   b) A simple multilevel secure database management system is to be designed. Each row 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 Customer-information table (*custid* is primary key).

custid	*level*	Name	Company
0031	topsecret	Monty	Springfield Nuclear
1002	secret	Wolfcastle	Planet Springfield
1022	unclassified	Moe	Moe's Tavern

   Given the usual ordering between the specified security levels, a secret process may read the Moe and Wolfcastle entries but not the Monty entry, and so forth. You should assume that when a new tuple is inserted into the table it is assigned the security-level of the subject inserting it.

      i. Propose suitable multilevel security rules that govern how database operations `UPDATE` and `SELECT` should behave. (*8 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. (*7 marks*)

   c) Describe how the MLS DBMS mechanism in Part b) of this question could form part of a Chinese-Wall policy mechanism that ensured that a user cannot access customers records from competing companies. In answering the question be sure to explain *why* the Chinese Wall is enforced. (*15 marks*)

3. 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. Authentication Server Trent is a trusted third party who provides a message translation service. Trent shares symmetric key 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? (*5 marks*)

iii. Extend the protocol to provide mutual authentication for Alice and Bob. (*6 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. (*15 marks*)

---

4. An Internet facing server `gamer.com` hosts an online multiuser game service on Port 666.

a) A string containing client data received at this port on `gamer.com` is passed by the service, without checking, to the C function:

```
void play(char *str){
  char buff[60];
  strcpy(buff,str);
  // .....
  }
```

Describe how a buffer-overflow in this function could enable a remote attacker gain control of the `gamer.com` host. (*15 marks*)

b) There is a concern about SYN-flood based denial of service attacks on `gamer.com`. The administrator uses a (flawed) implementation of SYN-cache whereby the state associated with a half-open connection is stored in the hashtable bucket indexed as $h(i.p)$, where $h()$ is a one-way hash function, i is the IP address of `gamer.com` and p is the requested port on `gamer.com`. Describe how an attacker can still carry out a SYN flood on this host and outline how the SYN-cache scheme should have been implemented. (*15 marks*)

c) Suppose that the probability of a SYN-flood based denial of service attack on `gamer.com` during a calendar year is 0.01, with a resulting loss of earning of $100,000. Deploying a SYN-cache reduces this probability to 0.001, however, it is recommended that the server is upgraded (once off cost $900), in order to support the SYN-cache processing requirements. Suppose that SYN-cookies entirely eliminate the risk of SYN-flood based denial of service, however, their continual use impact connection performance with a yearly loss of earnings of $5,000.00.

Use this information to carry out a *Risk Assessment* and advise the owners of `gamer.com` on how best to mitigate the risk of denial of service. (*15 marks*)

5. a) Explain the properties of a one-way cryptographic hash function. It is possible to find collisions in the MD5 hash function: discuss the impact of this result. (*15 marks*)

b) 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);                              // send to server
out.write(md.digest(passwd));
```

Identify and explain the security vulnerabilities in this protocol and implementation. (*15 marks*)

c) 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 and purpose of each line of the above code. (*15 marks*)