OLLSCOIL NA hÉIREANN
THE NATIONAL UNIVERSITY OF IRELAND, CORK

COLÁISTE NA hOLLSCOILE, CORCAIGH
UNIVERSITY COLLEGE, CORK

Summer Examination 2010

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

   b) A document editor provides an option to store documents in encrypted form based on a user provided passphrase. The standard C library pseudo-random number generator `rand()` is used as a stream cipher to encrypt a document P as $C = P \oplus \texttt{rand}(k)$, where the seed k is a one-way hash of the passphrase. Comment on the effectiveness of this mechanism and discuss how a stream cipher might be properly used. (*15 marks*)

   c) A programmer modifies the document editor and uses DES in ECB mode for encryption. For added security, each block of plaintext is encrypted twice using an eight character user password as the key. Prior to encryption, a block of null values is appended to the end of the plaintext document. When the document is loaded/decrypted, the block is used to confirm the integrity of the document. Comment on the effectiveness of this design and suggest how it might be improved. (*15 marks*)

---

2. The back-end DBMS of a retail web-site `www.amadan.com` stores customer order details in a database table `CUST` which includes attributes `OrderID`, `UserID`, `NameAddress`, `CreditCard`.

   a) Prior to placing an order a customer logs in by providing their `userID` and password. If successful, they are directed to a URL that includes a simple authenticator, for example,

   ```
   http://www.amadan.com/order.asp?p1=simon&p2=12345
   ```

   whereby the user `simon` need not re-authenticate so long as he includes `p2=12345` in any URL. The authenticator is a simple global sequence number, incremented on each login. Describe an attack on this scheme whereby an attacker can masquerade as another user. Outline how the attack can be avoided by using authenticator cookies. (*15 marks*)

   b) Following a successful login, a user (`$userID`) can view payment details for any past order by providing an `$orderID` value, resulting in the following back-end query:

   ```
   SELECT CreditCard,NameAddress
   FROM CUST
   WHERE UserID = '$userid' AND OrderID='$orderID'
   ```

   Describe how an SQL-injection attack on this web-page could enable an attacker to discover the credit card details of other users. How might this attack be avoided? (*15 marks*)

   c) The website owners have a choice of deploying the web-server plus DBMS on either a standard Linux server or on an SELinux server that provides Type Enforcement based access control. Advise the website owners on the choice and illustrate your answer by comparing a Linux user-group policy versus a Domain Definition Table. (*15 marks*)

3. Alice (A) wishes to communicate securely with Bob (B) and proposes a symmetric key K_{AB}, a copy of which she intends to give to Bob. Trent is a trusted third party who shares secret (symmetric) key K_{AT} with Alice and secret (symmetric) key K_{BT} with Bob. The following protocol is used to pass the key K_{AB} to Bob.

$$\begin{aligned} \text{Msg 1:} \quad & A \rightarrow T : (\{B\}_{K_{AT}}, \{K_{AB}\}_{K_{AT}}) \\ \text{Msg 2:} \quad & T \rightarrow B : (\{A\}_{K_{BT}}, \{K_{AB}\}_{K_{BT}}) \end{aligned}$$

a) Discuss how the above protocol might be used to secure services provided over a distributed system. Your answer should consider the issues of authentication, secrecy, integrity and revocation. (*15 marks*)

b) Illustrate how third user, Eve (who shares a valid secret key K_{ET} with Trent) can subvert the protocol and get a copy of a key K_{AB} that Alice gives to Bob using this protocol. (*15 marks*)

c) Suggest a revision to the protocol that avoids this flaw and extend your protocol so that it supports mutual authentication between A and B. (*15 marks*)

---

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

b) A multilevel secure system has only one printer which is used to print jobs at all security levels. It is in a secured area and printouts are carefully labelled. A multilevel secure (trusted) print queue manager accepts requests from subjects at any security level. Its operations are:

i. `lpr <filename>`. Assign job number and add file to print queue. Returns `job#` to requester.

ii. `lprm <job#>`. Remove specified print job. Returns `success` or `failure`.

Sketch suitable algorithms that describe the behaviour of the above operations taking care to ensure that multilevel security is preserved. For the sake of simplicity it is not necessary to consider printer controls/scheduling. (*15 marks*)

c) Given public generator g and modulus n, principals A and B generate secrets x and y, respectively, and engage in the following variation of a Diffie-Hellman (DH) Key exchange:

$$\begin{aligned} \text{Msg1:} \quad & A \rightarrow B : \quad \{g^x \bmod n\}_{sK_A} \\ \text{Msg2:} \quad & B \rightarrow A : \quad g^y \bmod n \end{aligned}$$

A owns public, private keys (K_A, K_A^{-1}) and $\{...\}_{sK_A}$ denotes message signing (using K_A^{-1}).

i. How do A and B determine their shared key K? (*5 marks*)

ii. How can B be sure that only A *could* know the key K? (*5 marks*)

iii. Revise the protocol so that A is sure that B (and only B) *does* know the key K. (*5 marks*)

5. Bob provides a tax-returns service at `http://www.bob.com` and Alice uses the following Java code to *securely* send her salary and tax details (`byte[] msg`) to Bob over a socket-based connection (encapsulated as `DataOutputStream out`). Note that Alice's Java `KeyStore keystore` stores her public DSA key, alias `"alicePK"`.

```
Random rangen = new Random(0);
byte[] keySession = new byte[2];
rangen.nextBytes(keySession);
SecretKeyFactory desF = SecretKeyFactory.getInstance ("DES");
KeySpec ks = new DESKeySpec(keySession);
SecretKey key = desF.generateSecret(ks)
Cipher cipher = Cipher.getInstance("DES/ECB/PKCS5Padding");
cipher.init(Cipher.ENCRYPT_MODE,key);
byte[] cBytes= cipher.doFinal(msg)
out.write(cBytes);

String alice= "alicePassword".toCharArray();
PrivateKey priv = (PrivateKey) keystore.getKey("alicePK",alice);
Signature signature = Signature.getInstance ("DSA");
signature.initSign(priv);
byte[] sig = signature.sign(keySession);
out.write(sig);
```

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

b) It has been suggested that it would be better to use Java SSL to secure the connection between Alice and Bob. Outline how Java SSL should be used in this case and include an explanation of how the use of public key certificates in the protocol can help Bob to discover Alice's public key. (*15 marks*)

c) Suppose that Bob provides a Java tax-returns applet `tax` that Alice runs (instead of sending her tax details to Bob's server).

i. Write a Java security policy entry for Alice that grants Bob's applet read and write access to files in directory `file:/usr/home/alice/tax`. (*5 marks*)

ii. Explain why Bob's applet should be signed and by whom. (*5 marks*)

iii. Suppose that Alice may run a tax application `taxConsult.jar` hosted on Bob's server. Bob uses JAAS to control access. Write a Java security policy entry for Bob that permits the application access Alice's tax files in directory `file:/usr/home/tax/alice` (on Bob's file system) when executed by Alice. (*5 marks*)