OLLSCOIL NA hÉIREANN
THE NATIONAL UNIVERSITY OF IRELAND, CORK

COLÁISTE NA hOLLSCOILE, CORCAIGH
UNIVERSITY COLLEGE, CORK

Summer Examination 2009

Fourth Year Computer Science

CS4253: Computer Security

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

Answer *Four* questions
Questions carry equal marks

Three Hours

1. a) Explain the properties of a one-way cryptographic hash function. What is the impact of the birthday paradox on the effectiveness of a hash function that generates a 160-bit hash value? (*15 marks*)

   b) A secure USB memory stick uses onboard AES hardware to encrypt data files to be stored. The AES key is computed as an MD5 hash of a password provided by the user. The device requires the user to change their password at least once every three months and, in order to prevent the user re-using old passwords, the device stores a list of the hash of every previous password. A proactive password checker also requires that passwords be comprised of at least 4 uppercase alphabetic and 3 numeric characters. Discuss any vulnerabilities that this implementation may have. (*15 marks*)

   c) One-time password key-fobs are issued to all employees for access to the company systems. Each key-fob generates fresh time-based pass-codes at 30 second intervals, is tamper-resistant and stores a master secret key K (known only to the authentication server). A key-fob calculates the pass-code as $(\{time\}_K, \{userid\}_K)$, for its owner *userid*. Outline an attack on this scheme that would allow an attacker gain access to another user account (without having to steal the victim's key-fob). (*15 marks*)

2. A networked server hosts a Kerberos Authentication Service and an Apache web-server that uses a MySQL back-end database server.

   a) The web and database server host an application system requiring user login which is implemented by passing user login data to the backend DBMS application that checks the table `UserTable(UserID,Email,Passwd)`. If the user enters just `userid` and selects the `ForgottenPassword` button then the application emails the corresponding password to the user. The backend query for this action is:

```
SELECT Email, Passwd
FROM   UserTable
WHERE  UserID = '$userid';
```

   Describe how an SQL-injection attack on this web-page could enable an attacker to login as another user. How might this attack be avoided? (*15 marks*)

   b) On discovery of the injection attack, a full application code review was ordered and another web-form was discovered that passes data to the following C program.

```
void main1(int argc, char* argv[]){
  char buff[6];
  strcpy(buffer,argv[0]);
  .....
  }/*main1*/
```

   Describe how a buffer-overflow attack on this application could enable an attacker to gain control of the host. (*15 marks*)

   c) In light of the above attacks, it has been decided to replace the existing server host by a high-assurance system that enforces mandatory Multilevel security (MLS). Describe the (Bell LaPadula) access-rules for MLS and give a suitable compartmentalization policy for the server host that would provide better system protection. Discuss any limitations of this approach. (*15 marks*)

3. Consider the following fragment from a Kerberos-like authentication protocol, whereby initiator A requests, and is granted, a ticket from Authentication Server S to be used with service B.

$$\begin{aligned} \text{Msg 1}: &\quad A \rightarrow S: \quad A, B, N_a \\ \text{Msg 2}: &\quad S \rightarrow A: \quad T_{ab}, \{N_a, K_{ab}\}_{K_{as}} \end{aligned}$$

Principals A and B share long-term secret keys K_{as} and K_{bs} with server S, respectively; N_a is a nonce; $\{\ldots\}_K$ represents symmetric key encryption with secret key K. The server issues a ticket $T_{ab} = \{L, K_{ab}\}_{K_{bs}}$ for the session key K_{ab}, valid for time period specified by L.

a) Suppose that B above is a ticket granting service and, thus, T_{ab} is a ticket granting ticket. Propose and explain a suitable protocol exchange between A and B that will result in A obtaining a ticket for a file server C. (*10 marks*)

b) Describe the subsequent protocol exchange that A should execute in order to establish a secure and authenticated connection to the service C. (*10 marks*)

c) Discuss how the long-term secrets in the protocol (K_{as} and K_{bs}) are protected by the system. Why is it preferable for A to use a ticket granting service? (*10 marks*)

d) Describe an attack on the protocol whereby Eve can masquerade as A. (*15 marks*)

4. a) Let $cert_{K_A}^{K_T}$ be a public key certificate issued by Trent, the owner of public key K_T, and concerning the public key K_A owned by Alice. Describe the typical contents of this certificate, how it is implemented (signed) and how it is used in practice. (*15 marks*)

b) A Certification Authority owns public key K_T and issues certificate $cert_{K_A}^{K_T}$ for Alice's public key K_A. Alice A sends a message M to Bob B using the following protocol:

$$A \rightarrow B : cert_{K_A}^{K_T}, \{M, h(M)\}_K, \{A, B, K\}_{sK_A}$$

where, K is a secret session-key, $k()$ is a cryptographic one-way hash function and $\{\ldots\}_{sK_a}$ denotes signing by the owner of public key K_a. The goal of the protocol is to *securely* send a *digitally signed* message to B. Identify and discuss weaknesses in the protocol and suggest an improved protocol.

c) Given suitable public generator g and modulus n, principals A an B generate suitable secrets x and y, respectively, and engage in the Diffie-Hellman (DH) Key exchange.

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

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

ii. Explain why K cannot be determined by a third party observing the exchange. (*5 marks*)

iii. Suppose that A has RSA public key K_A. Revise the DH Key exchange in order to provide authentication of A. (*5 marks*)

5. a) Describe the access-control mechanism that is used in unix, paying particular attention to the file system access controls. (*15 marks*)

   b) An order processing system is implemented in terms of programs `prop` and `appr`, which are executed when proposing a new order and order approval, respectively. Both programs are permitted access to the `order` file. Clerk Clare is permitted to propose orders, which may be approved by Manager Mike. The data in the order file is periodically checked for entries that don't match the company's goods-received log.

      i. Outline how security of the application system should be represented and interpreted in terms of the Clark-Wilson model. (*7 marks*)

      ii. Sketch how the Unix protection mechanism can be used to support the Clark-Wilson model of this application. (*8 marks*)

   c) Develop suitable Java security policy *grant* entries for the following requirements.

      i. Any code signed by the public key `simon` may have read and write access to files under `/usr/home/simon/`. (*5 marks*)

      ii. *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`. (*5 marks*)

      iii. The principal simon, authenticated in Kerberos domain `CSDOMAIN`, may read and write files in `/tmp/`. (*5 marks*)