OLLSCOIL NA hÉIREANN
THE NATIONAL UNIVERSITY OF IRELAND, CORK

COLÁISTE NA hOLLSCOILE, CORCAIGH
UNIVERSITY COLLEGE, CORK

AUTUMN 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) 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) 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)*

   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. 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.

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

   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)*

3. 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. *(15 marks)*

   b) Briefly describe the Type Enforcement mandatory access control model. Use the problem of safeguarding against malicious code in applications to illustrate your answer. Your answer should include a suitable Domain Definition Table. *(15 marks)*

   c) An organization plans to deploy a Kerberos authentication server and a public web server on the same host system. They are considering using either a standard Unix system or a multilevel secure system as host. Advise the organization and discuss the suitability, pros and cons of these approaches. *(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.

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

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

5. A publisher provides subscriber-only web access to its newspaper. Subscription is free and users log in via an SSL-protected web-page, providing a subscriber user-id and password.

a) Sketch the operation of the SSL protocol, what it is intended to achieve, and its suitability for this application. Note that it is not necessary to reproduce the exact SSL protocol messages. *(15 marks)*

b) The login form is implemented by passing user login data to a backend DBMS application that checks the information from 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 subscriber. How can this attack be avoided? *(15 marks)*

c) Once the user is authenticated the server sets an authentication cookie in the browser of the user. Suppose that the application developer coded the cookie using Unix `crypt(UserID^K)` which encrypts a a block of nulls using the DES key `UserID^K` (the catenation of the user-id and a secret key `K` known only to the webserver, truncated to 56 bits). Outline an attack whereby it is possible for a subscriber to discover secret key K. *(15 marks)*

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.

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

(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:

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

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)*

OLLSCOIL NA hÉIREANN
THE NATIONAL UNIVERSITY OF IRELAND, CORK

COLÁISTE NA hOLLSCOILE, CORCAIGH
UNIVERSITY COLLEGE, CORK

AUTUMN 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) Comment on the fundamental differences between the following approaches to security: Biba model of integrity; Clark-Wilson model of integrity; Software Wrappers (such as TCP/IP wrappers). *(8 marks)*

   (b) A vendor uses Message Authentication Codes (MACs) as signatures for orders from customers. A customer generating purchase order PO emails message $(PO, h_k(PO))$ to the vendor, where h_k is a keyed one-way-hash function and secret key k is known only to the vendor and the customer. To verify the signature the vendor simply recomputes the hash of the purchase order and compares it with the MAC provided. What is wrong with this signature scheme? *(8 marks)*

   (c) After a simple Diffie-Hellman 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. 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 $K = g^{xy} \bmod n$. *(9 marks)*

2. A discretionary access-control based protection mechanism is to be designed for a network file server.

   The protection mechanism allows the creator (owner) of a file to decide the access-rights (*read*, *write*) that all other users of the server may have for that file (world access-rights). The owner of a file may have any access to the file. Any user, other than the owner, may access a file if the world access-rights are appropriately set. This mechanism can be described in terms of three primitive operations which modify and/or test the protection state:

   - A user u creating a file f invokes operation *CreateFile(u,f)*. For simplicity, you may assume that file f does not already exist.
   - A user who owns a file f may add access-right a to the world access-rights of file f by invoking operation *AddRight(u,f,a)*.
   - If it does not violate the protection policy outline above, then invocation of *Open(u,f,a)* grants user u access-right a to file f.

   (a) Describe how this mechanism can be abstractly modeled using the the HRU access-matrix model. Your answer should clearly identify the access-rights required, along with descriptions of the three operations above in terms of the HRU model primitives. *(12 marks)*

   (b) A system designer decides to implement this protection mechanism by attaching an Access Control List(ACL) with each individual file. Comment on whether or not this is a sensible approach. *(6 marks)*

   (c) Briefly explain the safety-problem. Do you think the safety-problem might be decidable for this particular security mechanism? Explain your answer. *(7 marks)*

3. (a) Explain how an attacker can carry out a *TCP IP spoof* by interfering with the TCP three-way handshake. *(6 marks)*

(b) Describe how SYN Flooding can cause a denial of service attack. Suggest a possible defense to this attack and comment on its effectiveness. *(7 marks)*

(c) A programmer reads the S/KEY one-time-password scheme and (incorrectly) implements it as:

- For a given i, $h^i(s)$ denotes $h(h(\ldots h(s)))$, representing i applications of one-way hash function h to value s, where s represents an initial password (seed) chosen by the user.
- When a user picks her (initial) password s, the system stores $(1, h(s))$ in the password file.
- If a user has logged-in $i-1$ times since choosing initial password s, then the system stores $(i, h^i(s))$ in the password file.
- When a user attempts to log-in for the i^{th} time the system presents i as a challenge. The user (knowing s) provides response $r = h^{i-1}(s)$. The system compares $h(r)$ with the hash value stored in the password file and, if equal, updates this password entry to $(i+1, h(h(r)))$.

Outline an attack on this scheme and describe how it should be fixed. *(12 marks)*

4. (a) A Java application inputs an DES-CBC encrypted file, decrypts it, and outputs the result to another file. Sketch its implementation. *(7 marks)*

(b) What is the difference between code-centric and user-centric security? Sketch how one might augment their web browser so that Java applets may access the local file system only during working hours. *(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. *(10 marks)*

5. (a) 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

$$(\{PIN\}_{K_B}, \{AccountID\}_{K_B})$$

should be stored on this magnetic strip. $\{PIN\}_{K_B}$ gives the PIN encrypted under a symmetric key 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)*

(b) 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.

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

i. Illustrate how third user, Eve (who shares a valid secret key K_{ET} with Trent) can subvert the protocol to get a copy of a key K_{AB} that Alice gives to Bob using this protocol. *(6 marks)*

ii. Propose a revised version of this protocol that is resilient against this attack. Briefly explain why you think your solution is more secure. *(5 marks)*

(c) Explain why the Needham Schroeder and the Kerberos key exchange protocols are more *practical* than the Wide-Mouth Frog protocol. *(6 marks)*

OLLSCOIL NA hÉIREANN
THE NATIONAL UNIVERSITY OF IRELAND, CORK

COLÁISTE NA hOLLSCOILE, CORCAIGH
UNIVERSITY COLLEGE, CORK

AUTUMN EXAMINATION 2004

Fourth Year Computer Science

CS4253: Computer Security

Professor M. Calder,
Professor C. J. Sreenan,
Dr. S.N. Foley

Answer *Four* questions
Questions carry equal marks

Three Hours

1. 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 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)*

2. a) Describe how the RSA scheme is used to implement digital signatures. *(8 marks)*

A vendor uses Message Authentication Codes (MACs) as signatures for orders from customers. A customer generating purchase order PO emails message $(PO, h_k(PO))$ to the vendor, where h_k is a keyed one-way-hash function and secret key k is known only to the vendor and the customer. To verify the signature the vendor simply recomputes the hash of the purchase order and compares it with the MAC provided. What is wrong with this digital signature scheme? *(7 marks)*

b) A bank provides one-time password key-fobs to customers who wish to do their banking over the Internet. Each customer is given a unique key-fob which generates fresh time-based pass-codes at 30 second intervals. Each key-fob is tamper-resistant and stores a master secret key K (known only to the bank) and its owner's *userid*. A key-fob calculates the pass-code as $(\{time\}_K, \{userid\}_K)$. When a customer attempts to login, she provides $(userid, passcode)$; the remote bank system decrypts the pass-code fields, matches the use-rid and checks that the time is current.

Outline an attack on this scheme that would allow an eavesdropper gain access to a another customer's account (without having to steal the victim's key-fob). *(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) Develop suitable Java security policy *grant* entries for the following requirements.

i. Anybody may read and write files in `/tmp/`. *(5 marks)*

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

b) The following Java fragment establishes an SSL connection to a server.

```
char[] storepass= "spasswd".toCharArray();
KeyStore keystore= KeyStore.getInstance("JCEKS");
keystore.load(new FileInputStream("keystore"),storepass);

TrustManagerFactory tmfactory= TrustManagerFactory.getInstance("SunX509");
tmfactory.init(keystore);
TrustManager[] clienttm= tmfactory.getTrustManagers();

SSLContext sslcontext= SSLContext.getInstance("SSL");
sslcontext.init(null, clienttm, null);

SocketFactory  sfactory = sslcontext.getSocketFactory();
/* open an SSL socket on host port 5999 */
SSLSocket s= (SSLSocket) sfactory.createSocket("serverhost",5999);
DataOutputStream out = new DataOutputStream(s.getOutputStream());
```

Explain the purpose of the keystore, trust manager and socket factory in this code. Outline how they contribute to the authentication of, and the secure connection to, the server. *(15 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.

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

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. *(15 marks)*

4. a) Briefly describe the Type Enforcement mandatory access control model. Use the problem of safeguarding against possible buffer overflows in applications such as web-servers to illustrate your answer. Your answer should include a suitable Domain Definition Table. *(15 marks)*

b) Briefly describe the Biba model of Integrity and explain how it differs to the Type Enforcement model. *(15 marks)*

c) 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)*

5. 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.

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

a) What is the difference between long term and session keys? Describe how pass-phrase encryption might be used to provide long-term keys. What defences can be used to make it harder to carry out a dictionary attack on pass-phrases? *(15 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. 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. *(15 marks)*