1. a) Give the typical requirements of a secure distributed system.

[3 marks]

b) Describe the meaning of a system in the context of security engineering.

[6 marks]

c) In security engineering define what is meant by a principal and explain the meaning of identity.

[5 marks]

e) Explain why challenge response identification systems are used.

[2 marks]

f) Explain how public key cryptography may be used for identification.

[4 marks]

Solution 1

a) Typical requirements of a secure distributed computing system are:

- User authentication
- Message integrity with respect to origin and content
- Message confidentiality
- Fault-tolerance

[3 marks]

b) In the context of security engineering a system is taken to mean:
One or more applications, for example, payroll

Together with the collection of components, operating system, communications, and other parts of an organization's infrastructure that they are dependent upon

Together with all users of the applications both internal and external to the organization, the management of the organization, its customers and surrounding environment including competitors and regulators

[6 marks]

c) A ***principal*** is an element of the system.
An element can be

- a person
- a role
- an item of equipment
- a piece of software
- an encryption key

Identity means a correspondence between the names of two principals signifying that they refer to the same person, item of equipment, or piece of software.

- This is best understood in terms of one person taking on several roles.

[5 marks]

d) The use of one-time passwords does not rule out the possibility that an attacker can learn the password before the identification takes place. To get around this problem ***challenge response identification systems*** are used.

[2 marks]

e) Public-key cryptography may be used for identification as follows:

- If Bob wants to identify himself to Alice he asks Alice for a random number
- Bob encrypts this random number with his private key and sends the cipher text to Alice
- Alice decrypts the cipher text using Bob's public key and compares the result with the number she sent.
- If there is a match then she accepts this as proof of identity.

For this challenge response system to work Alice must be sure that she has the authentic public key of Bob.

[4 marks]

2. a) Explain what a nonce is and the reason for using a nonce.

[2 marks]

b) Describe how a man-in-the-middle attack may be performed on a Wi-Fi network and the consequences of such an attack.

[10 marks]

c) Explain how a man-in-the-middle attack on a Wi-Fi network can be defeated.

[4 marks]

d) Outline the scope of key management.

[4 marks]

Solutions 2

a) In principle, a nonce is a number that is used only once.

- o A nonce is used to guarantee a message is fresh and not a replay of an old message.

[2 marks]

b) Wi-Fi is a wireless technology that provides simple broadband access using a laptop and an access point to which the laptop has authenticated itself.

Suppose an attacker has a modified Wi-Fi card designed to intercept data. All information coming from the access points within wireless range can be read.

Suppose an attacker wishes to authenticate to a corporate access point they should not be able to use. In a man-in-the-middle attack the attacker sets up a bogus access point:

- o The bogus access point identifies a real corporate access point in advance.
- o When a corporate laptop sees the bogus access point and tries to associate to it the bogus access point copies all the messages it receives to the valid corporate access point, substituting its own Medium Access Control (MAC) address for the source address.
- o The bogus access point copies all the messages received from the valid access point back to the mobile device again substituting its own Medium Access Control (MAC) address for the source address. This intervention is possible even when the data is encrypted and without the enemy knowing the secret keys.

If the message content is encrypted very little can be achieved without some knowledge of the contents of the messages before they were encrypted.

More can be achieved if the attacker is allowed to replay captured messages.

In particular, if a simple challenge response scheme were used for authentication by replaying captured messages the bogus access point could associate itself to the corporate access point.

[10 marks]

c) A man-in-the-middle attack on a Wi-Fi network can be defeated by requiring mutual authentication between the corporate user and the access point and providing protection against replay attacks. The security methods for Wi-Fi called Wireless Protected Access (WPA) and Robust Security Network (RSN/WPA2) do this.

[4 marks]

d) Key management includes all aspects of the keying relationships:

- o User initialisation
- o Generation and distribution of keying material
- o Controlling key material use
- o Backing up
- o Archiving and updating keying material.

[4 marks]

3. a) In general, there are three types of identity authentication tasks. List these tasks.

[4 marks]

b) Explain the role of the logic of authentication.

[4 marks]

Solutions 3

a) In general, there are three types of identity authentication tasks which are:

- Identity authentication for something known, such as a password;
- Identity authentication for something possessed, such as a smart card;
- Identity authentication for some personal characteristics, such as fingerprints.

[4 marks]

b) The logic of authentication formally describes the operation of an authentication protocol. It does this by formally describing the knowledge and the beliefs of the legitimate parties involved in authentication, and while analyzing the authentication protocol step by step, describes how their knowledge and beliefs change at each step. After the analysis, all the final states of the protocol are set out.

[4 marks]

5. a) An ideal password authentication scheme has to withstand a number of attacks. Describe five of these attacks.

[10 marks]

b) Describe the goals an ideal password authentication scheme should achieve.

[10 marks]

Solutions 5

a) Any five of the following:

SR1. Denial of Service Attacks
An attacker can update false verification information of a legal user for the next login phase. Afterwards, the legal user will not be able to login successfully anymore.

SR2. Forgery Attacks (Impersonation Attacks)
An attacker attempts to modify intercepted communications to masquerade the legal user and login to the system.

SR3. Forward Secrecy
It has to be ensured that the previously generated passwords in the system are secure even if the system's secret key has been revealed in public by accident or is stolen.

SR4. Server spoofing attacks
Mutual authentication can help withstand the server spoofing attack where an attacker pretends to be the server to manipulate sensitive data of the legal users. Mutual authentication means the user and the server can authenticate each other. Not only can the server verify the legal users, but the users can also verify the legal server.

SR5. Parallel Session Attacks
Without knowing a user's password, an attacker can masquerade as the legal user by creating a valid login message out of some eavesdropped communication between the user and the server.

SR6. Password Guessing Attacks
Most passwords have such low entropy that they are vulnerable to password guessing attacks, where an attacker intercepts authentication messages and stores them locally and then uses a guessed password and seeks verify the correctness of their guess using these authentication messages.

SR7. Replay Attacks
Having intercepted previous communications, an attacker can replay the intercepted messages to impersonate the legal user to login to the system.

SR8. Smart Card Loss Attacks
When the smart card is lost or stolen, unauthorized

[10 marks]

b) An ideal password authentication scheme should achieve the following goals:

1 The passwords or verification tables are not stored in the system.
2 The passwords can be chosen and changed freely by the users.
3 The passwords cannot be revealed by the administrator of the server.
4 The passwords are not transmitted in plain text over the network.
5 The length of a password must be appropriate for memorization.
6 The scheme must be efficient and practical.
7 Any unauthorized login can be quickly detected when a user inputs a wrong password.
8 A session key is established during the password authentication process to provide confidentiality of communication.
9 The ID should be dynamically changed for each login session to avoid partial information leakage about the user's login message.
10 The proposed scheme is still secure even if the secret key of the authentication server is leaked out or stolen.

[10 marks]

6. a) Describe the three main concerns with the use of passwords for authentication. Explain what is meant by a social engineering attack on a password.

[4 marks]

b) Explain how attacks on passwords are broadly classified.

[4 marks]

c) Explain how access control lists are use to represent access control matrices. Describe the environments in which they are widely used and their advantages and disadvantages.

[6 marks]

d) Suppose the following groups are defined to shorten a system's access control lists:

- Group1: Alice, Bob, Cynthia, David, Eve
- Group2: Alice, Bob, Cynthia
- Group3: Bob, Cynthia

Suppose the access control list for File 1 is:

- File 1: Group 1, R; Group 2, RW

If Alice wants to write to File 1 giving your reasoning state whether Alice will be allowed to do so if:

i) The first relevant entry policy is applied
ii) The any permission in list policy is applied

Suppose the access control list for File 2 is:

- File 2: Group 3, RWE

iii) Show how the need for a Group 3 for File 2 can be removed using access none.

[6 marks]

Solutions 6

a) There are three main concerns with the use of passwords for authentication:

- Will the user disclose the password to another person intentionally, accidentally, or because they were deceived?
- Will the user be able to regularly enter the password correctly?
- Will users be able to remember their passwords or will they have to record them somewhere or choose easily guessed passwords?

When an attacker obtains a password directly from its user by deceit the attack is known as social engineering.

[4 marks]

b) Attacks on passwords can be broadly classified as:

- A targeted attack on one account: The attacker tries to obtain a particular user's password.
- Attempt to penetrate any account on a system: The attacker tries to steal any password for the system, for example, by a dictionary attack.
- Attempt to penetrate any account on any system: This is when an attacker is seeking access to any system within a given domain.
- Service denial attack: An attacker may want to prevent a specific user from using the system.

[4 marks]

c) Access control lists are used to simplify access rights management by storing the access control matrix a column at a time along with the resource to which the column refers.

ACLs are widely used in environments where the users manage the security of their own files such as Unix systems.

Their advantages are:

- Easy to understand
- Easily answer the question "who has what kind of access to this resource"
- Work well in distributed systems; Rights stored together with resources

Their main disadvantage is:

- May be inefficient. Determining rights may require searching a long list

[6 marks]

d) The first relevant entry is Group 1 because Alice is a member of Group 1. Group 1 has read only access to File 1 son Alice has read only access to File 1.

Alice is a member of Group 1 and Group 2. As Group 2 has read and write access to File 1, Alice has write access to File 1.

The access control list for File 2 may be written:

– File 2: Alice, None; Group 2, RWE

[6 marks]

7. a) Explain the principle of least privilege.

[5 marks]

b) Explain how capability lists are used to represent access control matrices. Discuss the main problem associated with the use of capability lists and its consequences.

[6 marks]

c) Explain how capability lists are now commonly implemented in the form of attribute certificates to get around the main problem associated with the use of capability lists for access control.

[3 marks]

d) The permission bits associated with a program call Prog1 and a dataset called Data1 are as follows:

Prog1: 1 1 1 1 0 1 1 0 0

Data1: 1 1 1 1 0 0 0 0 0

State the permissions these bits give.
Describe the advantages and disadvantages of using permission bits for access control.

[6 marks]

Solutions 7

a) The principle of least privilege requires that a user be given no more privilege than necessary to perform a job. Ensuring least privilege requires identifying what the user's job is, determining the minimum set of privileges required to perform that job, and restricting the user to a domain with those privileges and nothing more. By denying to subjects transactions that are not necessary for the performance of their duties, those denied privileges cannot be used to circumvent the organizational security policy.

[5 marks]

b) Capability lists register per principal what rights the principal has to the listed resources. The main problem with capability lists is that changing the status of a resource which can be difficult because it can be hard to find out which users have permission to access the resource. For example, changing a program's status so that no user may execute it can be difficult because it can be hard to find out which users have permission to execute the program. This equally applies to changing a files status and can be a problem when investigating an incident or preparing evidence of a crime.

[6 marks]

c) Attribute certificates are closely related to public key certificates. Attribute certification in essence is a way of extending authentication-oriented use of Public Key Infrastructure (PKI) to support tasks related to authorization. Attribute Certificates provide a solution to certify binding of attributes to a given subject.

[3 marks]

d)

File	Owner	Group	Others
	r w e	r w e	r w e
Prog1	1 1 1	1 0 1	1 0 0

Prog1 can be read, written, and executed by its owner, read and executed by its group, other users can read it

Data1	1 1 1	1 0 0	0 0 0

Data1 can be read, written, and executed by its owner, and read by its group, other users can do nothing with it.

The advantages and disadvantages of using permission bits for access control are:

- They are very simple
- They provide a fixed set of rights for a fixed set of subjects sand are therefore very inflexible
- They are efficient because the are no lists to search; Access rights are registered directly with the objects to which they relate

[6 marks]

8. a) Shannon proposed two measures of security: *unicity distance* and *cover time*.

Explain how each of these concepts seeks to provide an indication of the security of a cipher system and outline the theoretical concept which has now superseded the notion of cover time.

[8 marks]

Solutions 8

(*a*) If we assume that a cryptanalyst knows everything about a cipher system but the key, the unicity distance is the average number of ciphertext characters which must be received before he can in principle identify the key. It is defined as H(K)/(H(Σ)-H(X)) where

(i) H(K) is the entropy of the key, and for equally likely keys is log(|K|)

H(Σ) is the maximum entropy for a source with |Σ| symbols = log(|Σ|).

H(X) is the actual entropy of the source.

(ii) The cover time was defined as the computation time required to determine the key, given sufficient plain text and cipher text, assuming that a cryptanalyst had access to a powerful computer.

(iii) The concept of computational complexity is the modern counterpart of cover time. Generally one designs a cipher system so that encryption and decryption are computationally feasible, whereas identification of the key by a cryptanalyst is infeasible. Feasible generally means polynomial time, whereas infeasible generally means super-polynomial. By choosing a sufficiently "large" instance of his cipher system, the cryptographer can ensure that the cryptanalyst cannot afford sufficient computer power to attack it.

[8 marks]

9. a) Explain briefly the concepts: one-way function, one-way hash function, trapdoor one-way function.

[5 Marks]

b) Explain why a stream cipher fails to protect message integrity.

[5 Marks]

c) Describe how a one-way hash function may be used for message authentication.

[5 Marks]

d) The concept of computational complexity has superseded the notion of covertime as a measure of the security of a cryptosystem. Explain how computational complexity theory provides the theoretical basis for the design of modern scalable cryptosystems.

[5 Marks]

Solution 9

a) A one-way function is a function that is easy to compute but which is extremely difficult to invert.

A hash function is a function that takes a big number, or a piece of text, or some other data and computes from it a smaller number or bit vector. A one-way hash function is similar. A one-way hash function is a function for which it is extremely difficult to find two distinct arguments that give the same result. Also, given the result of a one-way hash function, it should be extremely hard to find any argument that gives that result.

A **trapdoor one-way function** is a one-way function together with a certain piece of additional information. It is extremely difficult to invert without the additional information, but easy to invert using the additional information.

[5 marks]

b) A stream cipher cannot protect message integrity because it is vulnerable to attacks in depth. For example, fund transfer messages are very highly structured. Suppose an attacker knew bytes 37-42 of such a message contained the amount to be transferred. They could request a modest sum (500 euro) to be sent to an accomplice. If by wiretapping the attacker can obtain the corresponding ciphertext for the message C = M XOR K they know M for bytes 37-42 so know K for bytes 37-42. They take the ciphertext and change bytes 37-42 to read 500,000 euro XORed with K for bytes 37-42 then send it on.

[5 marks]

c) In a symmetric key system, a one-way hash function is used as the fundamental component of a key dependent Hash-Based Message Authentication Code that takes as its input the whole message and outputs a message authentication code that is appended to the message. Only those with knowledge of the key may generate or check the message authentication code. In a public key system the message is input into a one way hash function the output of which is a message digest. A private key is used to encrypt the message digest to give digital signature which is attached to the message. The corresponding public key may be used to check the signature. An adversary will be unable to create a valid signature.

[5 marks]

d) A modern scalable cryptosystem is designed so that encryption and decryption are computationally feasible but identification of the key by a cryptanalyst is infeasible. A problem is considered feasible if it is in class P and infeasible if it is not. It follows that cryptosystems are designed so that encryption and decryption are in P and cryptanalysis is not. By choosing a sufficiently large key the cryptographer can ensure that the cryptanalyst cannot afford sufficient computer power to attack it.

[5 marks]

11. a) A Feistel cipher is used in the DES algorithm. Describe the operation of a Feistel cipher.

[5 marks]

b) Briefly describe three modes of operation of DES.

[7 marks]

c) Discuss the security of AES.

[12 marks]

Solutions 11

a) A Feistel cipher is given an arbitrary set of functions over Boolean vectors of length n. The plaintext and ciphertext are both pairs of n bit words (w_1, w_2). One of the given functions f is chosen and the pair of words $(w_2, f(w_1) \oplus w_2)$ is formed, where $\oplus$ is bitwise addition modulo 2. This step is repeated as many times as required, choosing a different f each time. To recover the key from a plaintext-ciphertext pair requires the solution of a set of polynomial equations modulo 2.

[5 marks]

b) Any three of the following would be acceptable:

On July 1, 2009, Bruce Schneier blogged about related-key attacks published in December 2009 on the 192-bit and 256-bit versions of AES, which exploit AES's somewhat simple key schedule. A related-key attack can break 256-bit AES with a complexity of 299.5 which while faster than brute force is still infeasible. In a similar manner, 192-bit AES can be broken by an attack with a complexity of 2176. 128-bit AES is not affected by these attacks.

In ECB mode, a 64 bit plaintext is encrypted directly. This mode is generally used only for key encryption. A potentially powerful technique for improving the security of DES is triple encryption. That is encrypting each message block under three different DES keys in succession. Triple encryption is thought to be equivalent to doubling the key size of DES, to 112 bits, and should prevent decryption by an enemy capable of single-key exhaustive search.

In CBC mode, a random initialisation vector is XORed with the first block of plaintext. The result is then encrypted with DES and transmitted. The result is also XORed with the next data block and the process repeated.

DES may also be used in cipher feedback mode (CFB). This is a variant of CBC which does not require that a full 64 bit block is received before encryption can begin. It is useful when the text is character based and in some network applications where data blocks are smaller the 64 bits. The process is started by encrypting a random initialisation vector stored in a 64 bit shift register and taking the first k of the 64 bits of the output of the DES algorithm. These k bits are XOR'ed with the first k bits of plaintext to give k bits of ciphertext. The k ciphertext bits are input to the shift register. The contents of the register form the input to the DES algorithm at the second step. At each step the plaintext is enciphered in blocks of k bits at a time and each ciphertext block of k bits is fed into the 64 bit shift register. The shift register is the input to DES for generating k bits for XORing with the next block of plaintext to give the next k bits of ciphertext.

OFB mode is the stream cipher version of DES. An initialisation vector is chosen randomly and stored in a shift register as an initial input to DES. This is encrypted and *k* bits of the result form *k* bits of a keysteam and are also shifted into a shift register ready for the next cycle. The resulting keystream is XORed with the data just as with a linear feedback shift register.

[7 marks]

c) Side-channel attacks do not attack the underlying cryptographic algorithm, and so have nothing to do with its security, but attack implementations of the cipher on systems which inadvertently leak data. There are several such known attacks on certain implementations of AES:

- In October 2005 a paper was presented that demonstrated several cache-timing attacks against AES. One attack was able to obtain an entire AES key after only 800 operations triggering encryption, in a total of 65 milliseconds. This attack requires the attacker to be able to run programs on the same system or platform that is performing AES.
- In December 2009 an attack on some hardware implementations of AES was published that used Differential Fault Analysis and allows recovery of key with complexity of 2^{32}.

Although there is no proof of the security of the AES cryptographic algorithm it is the first publicly accessible and open cipher approved by the United States National Security Agency (NSA) for top secret information. In 2003 it stated:

“The design and strength of all key lengths of the AES algorithm (i.e., 128, 192 and 256) are sufficient to protect classified information up to the SECRET level. TOP SECRET information will require use of either the 192 or 256 key lengths. The implementation of AES in products intended to protect national security systems and/or information must be reviewed and certified by NSA prior to their acquisition and use.”

On July 1, 2009, Bruce Schneier blogged about related-key attacks published in December 2009 on the 192-bit and 256-bit versions of AES, which exploit AES's somewhat simple key schedule. A related-key attack can break 256-bit AES with a complexity of $2^{99.5}$ which while faster than brute force is still infeasible. In a similar manner, 192-bit AES can be broken by an attack with a complexity of 2^{176}. 128-bit AES is not affected by these attacks.

[12 marks]

12. a) Define a discrete memoryless source.

[2 marks]

b) What is Perfect Secrecy? Describe a system that achieves it.

[6 marks]

c) Explain how the unicity distance of the system, described in part b), justifies the claim that the system is unbreakable if keys are not reused.

[4 marks]

d) Explain why it is impractical to implement the system described in part b).

[2 marks]

Solutions 12

a) A discrete memoryless source (DMS) is a source that emits an endless stream of statistically independent, distinguishable symbols from its alphabet and is the simplest model of an information source.

[2 marks]

b) A cipher system has perfect secrecy if the ciphertext gives the cryptanalyst no information about the key. The one time pad achieves perfect secrecy. It comprises a sequence of random symbols drawn from the same alphabet as the message which is known to both the sender and the receiver. A message is encrypted by combining it with an initial segment of the sequence of the same length as the message. That segment is then discarded. The segment is the key and in the case of a message made up of bits the combining of the message and the key can be as simple as XORing the two sequences together

[6 marks]

c) Unicity distance $U = \dfrac{H(K)}{\lg|\Sigma| - H}$.

For a message of n symbols the one time pad requires n randomly generated symbols of the key. For a key of n symbols drawn from an alphabet Σ there are $|\Sigma|^n$ possible keys. If all keys are equally likely then the probability of a particular key is $1/|\Sigma|^n$ and $H(K) = n\lg|\Sigma|$. Since $H > 0$, $U = \dfrac{n\lg|\Sigma|}{\lg|\Sigma| - H} > n$ and we need more ciphertext characters than the n available to break the cipher.

[4 marks]

d) The one time pad is impractical because we cannot mathematically generate truly random sequences. A one time pad can be approximated by generating an extremely long psuedorandom sequence.

[2 marks]

13. a) Discuss the security of additive, multiplicative and affine ciphers against known plaintext attacks.

[5 Marks]

b) An affine cipher with modulus 26 encrypts 4 as 2 and 7 as 17. Determine the key.

[5 Marks]

c) Consider an encryption system in which the entropy of the plain text is 32 bits per 128 bit block and in which the AES algorithm is used with a single 128 bit key. Assuming that all keys are equally likely, calculate the unicity distance of this cipher system.

[4 marks]

d) Outline what it means for a cryptosystem to be scalable and how scalability is achieved.

[3 marks]

e) The computational complexity of a problem is generally stated as the number of primitive steps required by some model of computation to solve the problem. Define the class of polynomial time problems (P).

[3 marks]

Solutions 13

a) None are secure against known-plaintext attacks. This can be seen by considering the affine ciphers, of which the other two are special cases. An affine cipher comprises multiplication by one key, and then addition of a second key. Thus the key is given as a pair of integers $(k_\times, k_+)$, and we encrypt with

$$a \mapsto a \times_m k_\times +_m k_+ .$$

In order to attack an affine cipher, two different plaintext-ciphertext pairs are required. This gives two equations, and since there are two unknowns to be obtained, this is sufficient. We have

$$a_1 k_\times + k_+ \equiv_m b_1$$
$$a_2 k_\times + k_+ \equiv_m b_2$$

There is a unique solution to these equations if the difference between plaintexts is coprime with the modulus.

[5 marks]

b) We know $4k_\times + k_+ \equiv_m 2$ and $7k_\times + k_+ \equiv_m 17$. Subtracting these equations we obtain

$$(4-7)k_\times + (k_+ - k_+) \equiv_{26} 2-17 \Leftrightarrow$$
$$-3k_\times \equiv_{26} -15 \Leftrightarrow$$
$$k_\times \equiv_{26} 5$$

From $4k_\times + k_+ \equiv_m 2$ we get $4\times 5 + k_+ = 2 \Rightarrow k_+ = 2 - 20 = -18 = 8 \bmod 26$

[5 marks]

c) Unicity distance is defined as $U = \dfrac{H(K)}{\lg|\Sigma| - H(X)}$ where

H(K) is the entropy of the key, and for equally likely keys is *lg(|K|)*

$\lg|\Sigma|$ is the maximum entropy for a source with $|\Sigma|$ symbols

H(X) is the actual entropy of the source.

Unicity distance of the system = H(K)/(lg $|\Sigma|$-H(X)) = 128/(128-32) = 1.3333.

[4 marks]

d) A cryptosystem is scalable if it allows us to set the cryptanalyst a harder task whenever the time spent on encryption and decryption is increased, by using a longer key. To achieve scalability, it must be arranged that as the cryptosystem is scaled up, the time required for cryptanalysis increases much faster than the time spent on encryption and decryption.

[3 marks]

e) Problems whose computational complexity is no greater than $O(n^a)$, for some constant a, where n is the size of the problem are members of the class of polynomial time problems (P).

[3 marks]