Exam 2010 Answers (Joshua Nguyen)

1a) i. The information security goal related to this phishing scenario is the confidentiality of the victim’s personal information. Confidentiality deals with preventing the unauthorised disclosure of information.

ii) Vulnerabilities are weaknesses in a system that can be exploited to compromise the information security goals. An example of vulnerability is the people who are uneducated in phishing schemes and thus are vulnerable to these types of email phishing attacks. A threat is a set of circumstances with the potential to compromise the information security goals. An example of a threat is the actual phishing emails which provide links that compromise confidentiality.

iii) The nature of phishing emails is to send thousands of emails which means that even though there is a low response rate, it will still result in many compromised accounts. Therefore the phishing email is still considered a major information security problem.

b) The purpose of the Do phase of the Plan-Do-Check-Act process model is to implement the information security management system. This is done by implementing the selected control methods and by promoting the actions that manage the identified risks.

c)

i) Risk identification is identifying the risks involved with the system. This is done by identifying any plausible threats and vulnerabilities in the system, and combining these to identify any threatening events and their potential consequences.

Extra bits added for review (not asked in the question):

Risk analysis is the analysis of the identified risks in order to determine the magnitude of each risk. The magnitude of each risk is based on several factors including the severity of the consequences and the rate at which the event can occur.

Risk evaluation is the ordering of the risks to determine which risks must be prioritised in risk treatment. This can be done by comparing the magnitude of each risk identified in risk analysis and ordering them appropriately.

ii) The phishing email statistics can be used to identify the magnitude of the risk of phishing emails in order to compare it to the magnitude of others risks. This will aid in the risk treatment process.

iii) Qualitative analysis uses descriptive words to describe the likelihood of the risk occurring (rare, unlikely, possible, likely, almost certain). Quantitative analysis uses actual numbers or values to describe the likelihood of the risk occurring (0%, 25%, 50%, 75, 100%).

2. a)

The one time pad is restricted in that its key is truly random and is the same length of the message. As it is a symmetric cipher, both parties need to have the same key. As the key needs to be private, there are problems with the transferring of the key to the two parties and thus key management is the main restriction. If the key could be transferred securely than the message should be able to be transferred securely and thus no encryption is required.

b)

DIAGRAM NEEDED

In ECB mode each block of plaintext (P1,P2,P3 etc) is combined with the key in the encryption algorithm to create the encrypted block of text (C1, C2,C3 etc). To decrypt, the encrypted block is combined with the key in the decryption algorithm to create the original block of text. These blocks of text are concatenated to obtain the original plaintext message.

c) If H(M’) = H(M) than Bob can be confident that the message has not been altered in anyway (integrity of message preserved). This does not prevent MITM attacks from altering the message during transfer though.

e) Asymmetric ciphers utilise a public and private key pair for each member. As encryption is done using the public key which is public, secure key distribution is not an issue which is a major advantage over symmetric ciphers.

f) Symmetric ciphers cannot provide non-repudiation because the key used is associated with two or more parties. Due to the lack of a private key, a digital signature which uniquely identifies a party cannot be created and thus symmetric ciphers do not provide non-repudiation.

3.

c)

i) Authentication is required because the system needs to be assured that attackers are not masquerading as legitimate users.

ii) Single factor authentication is authentication using one factor. These factors can be knowledge based, object based, ID based or location based. It is weaker than two-factor authentication which combines two of these factors.

iii) Monitoring access should be performed to detect unauthorized activities such as security incidents and access control loopholes. It is also important for providing evidence of security incidents and providing a model of normal system behaviour.

d)  
Disadvantages of user selected passwords:

* Many users do not have training about selecting strong passwords. This means that the user selected passwords are often weak and thus easy to guess.
* Majority of user selected passwords are a concatenation of common words/slang. This makes it easy for attackers to guess.
* The password can be written down or stored in plaintext on the computer. This allows potential attackers to have full access to the password protected information/resource.

4.

a)

i) Spoofing may result in a failure of confidentiality because when the attacker can read the encrypted message using their private key. This means that the message is disclosed to an unauthorised user and thus confidentiality is breached.

ii) Digital certificates verify a person’s identity and associate their public key with them. This combats the spoofing problem because the message sender can be reassured that the public key is legitimate if the certificate authority is trusted.

iii) In order to trust the contents of the certificate, the certificate authority who issued the certificate must be trusted. If the certificate authority is untrusted than it can be verified by checking the public keys of each of the members of the trust pathway until a trusted certificate authority is found. The user must also trust that the method that the certificate authority uses to verify the entity is thorough and thus can be trusted.

b) The list of trusted certificates is controlled by the user and thus the user may begin to trust every certificate they come across, including malicious/untrusted certificates. Certification path processing is limited as they are only based on the currently available trusted certificates.

d)

i) The privacy amendment act (2000) is applicable in this situation because the airline is a large private organization that generates more than $3 million annually. This act provides guidelines in which the organization must adhere to in terms of personal information and its management.

ii) If the criminal gains access to the exposed records they can masquerade as the recorded person. This allows them to gain access to the private resources of the person whose identity was stolen.

5.

a)

i) The major problem associated with Basic HTTP Authentication is that it sends base64 encoded usernames and passwords. This is essentially sending plaintext usernames and passwords over an insecure channel which makes it very easy for attackers to gain access to these usernames and passwords.

ii) Digest HTTP authentication uses a challenge response system where the server sends a challenge and the client responds. The client response contains a hashed value of a combination of the username/password, the HTTP method, the nonce challenge value, and the requested URI. This means that the username and password are no longer sent as plaintext and thus eliminates the major issue found in HTTP basic authentication.

b)

i) TLS is performed in the transmission layer in the OSI model or the host-to-host transmission layer in the TCP/IP model.

ii) The client uses the server’s certificate to verify the server’s identity and ensure that the server’s public key is certified and thus trustworthy. It does this by comparing the certificate signer with a list of predefined trusted certificate authorities. This is required in order to provide confidentiality through a symmetric cipher and to provide integrity by establishing a shared secret key used to generate a message authentication code (MAC).

c)

i) A simple packet filter operates at the network layer and examines each packet independently of other packets. It decides whether to drop or pass the packet based on the information in packet headers and the predefined filtering rule table.

ii) Stateful packet filters operate in the same way simple packet filters do except they are able to examine the state of each packet. This allows the filter to examine the packets in the context of the conversation. If header values contradict the expected state, the packet is dropped.

iii) ???