# ITS335 – Quiz 3

IT Security, Semester 2, 2015

Prepared by Steven Gordon on 16 February 2016
its335y15s2q03, Steve/Courses/2015/s2/its335/assessment/quiz3/quiz3.tex, r4481

## Question 1 [3 marks]

There are 4 users in a public-key cryptosystem: *Preecha*, *Peeranont*, *Kamolchanok* and *Vasana*. Assume all relevant keys, e.g. ($PU_{Meerit}$,$PR_{Meerit}$), have been generated and distributed. The public key encryption/decryption algorithms are denoted as E(key,message) and D(key,message), a hash algorithm is H(message) and concatenation is ||.

(a) [ Preecha | Vasana | Peeranont | Peeranont ] has a message $M$ to send to [ Kamolchanok | Peeranont | Preecha | Kamolchanok ]. Write an equation that shows what is sent across the network to ensure the message will be confidential. [1.5 marks]

**Answer.** *The sender uses the receivers public key to encrypt the message to obtain ciphertext:* $E(PU_{receiver}, M)$.

(b) [ Peeranont | Preecha | Vasana | Preecha ] has a message $M$ to send to [ Vasana | Kamolchanok | Kamolchanok | Vasana ]. Write an equation that shows what is sent across the network to ensure the receiver will be able to authenticate the message (confidentiality is not required). [1.5 marks]

**Answer.** *The sender uses their private key to sign the message, by encrypting the hash of the message to encrypt the message to obtain a signature which is sent with the message:* $M||E(PR_{sender}, H(M))$. *Alternatively:* $E(PR_{sender}, M)$

## Question 2 [3 marks]

(a) The process of converting a coded message back to the original message is called *decryption*.

(b) *Data integrity* is a security service that assures data received are exactly as sent.

(c) In a *masquerade* attack, a malicious user pretends to be someone they are not.

(d) *Access control* is a security service that controls who can have access to a resource.

(e) The process of converting a coded message back to the original message is called *decryption*.

(f) In a *traffic analysis* attack, a malicious user observes patterns of communications, without having to read the message contents.

(g) *Authentication* is a security service that assures the received data originated from the claimed sender.

(h) In a *replay* attack, a malicious user sends an identical copy of a previous message they have intercepted.

(i) The information known only to sender and receiver in a cipher is called a*key*.

(j) In a *modification* attack, a malicious user changes the contents of an intercepted message.

(k) The process of converting an original message into a coded, apparently random message is called *encryption*.

(l) *Availability* is a security service that assures a system is always accessible to authorised users.

## Question 3 [2 marks]

Explain the difference between the three common malicious software propagation methods: worm, virus and social engineering.

**Answer.** *A virus attaches to another program, while a worm is a standalone program. Social engineering involves tricking a user to run malicious software.*

Explain the difference between a normal virus, a metamorphic virus and a polymorphic virus, including discussing how easy they are to detect by anti-virus software.

**Answer.** *A normal virus simply copies itself, as is, to other files. When a poly- morphic virus copies the original virus to create a new virus, the new virus appears different than the original, but functions the same. For a metamorphic virus, the new virus both appears different and functions differently.*

## Question 4 [2 marks]

Select all of the true statements from the list below by selecting the letter (a), (b), (c) or (d). Zero (0) or more statements may be true. [penalty for incorrect or missing selections]

(a) **A countermeasure is a way to deal with an attack**

(b) In the context of computer security objectives, CIA is refers to Central Intelligence Agency

(c) Symmetric key cryptography is used to provide confidentiality; it cannot provide authentication

(d) **RSA is public key cipher that is considered secure**

(e) In the context of computer security objectives, CIA is refers to Confidentiality, Insurance and Attackers

(f) **Threats are potential violations of security policy that exploit vulnerabilities**

(g) **Triple DES (3DES) is more secure than DES, but is slower**

(h) In computer security, assets consist of vulnerabilities, threats and attacks

(i) **AES is symmetric block cipher that is considered secure**

(j) All block ciphers use a 64-bit key

(k) In the context of computer security objectives, CIA is refers to Confidentiality, Integrity and Authentication

(l) RSA is symmetric block cipher that is considered secure

(m) Symmetric key cryptography is used to provide confidentiality; it cannot provide authentication

(n) **It is normally assumed the attacker knows the ciphers (algorithms)**

(o) AES is public key cipher that is considered secure

(p) **A countermeasure is a way to deal with an attack**

## Question 5 [2 marks]

You have the task of implementing a login system. Explain an advantage and disadvantage of the following mechanism with respect to password usage. Be specific about the advantage (e.g. what attacker it can prevent) and disadvantage (e.g. what is a problem if used).

*Generate random passwords for users.*

**Answer.** *Advantage: Lower chance of attacker guessing password. Disadvantage: Difficult for user to remember.*

*Require users to have passwords that contain a mixture of uppercase, lowercase, digits and punctuation characters.*

**Answer.** *Advantage: Lower chance of attacker guessing password. Disadvantage: Difficult for user to remember, difficult to type.*

*Restrict the number of failed login attempts per day.*

**Answer.** *Advantage: Prevents online brute force attacks. Disadvantage: Inconvenient to users that make mistakes.*

*Require users to change their password every month.*

**Answer.** *Advantage: Lower chance of attacker guessing password. Disadvantage: Difficult for user to remember.*

# Question 6 [2 marks]

A symmetric key cipher uses a [ 48 | 50 | 48 | 50 ]-bit key. An attacker has obtained a ciphertext and is attempting a brute-force attack to find the key. The attacker plans to purchase computers so that in the worst case they can find the key within [ $2^{24}$ | $2^{24}$ | $2^{23}$ | $2^{24}$ ] seconds. If each computer can decrypt at a speed of [ $2^{16}$ | $2^{15}$ | $2^{16}$ | $2^{16}$ ] per second, how many computers are needed? Show your calculations.

**Answer.** *With a k-bit key, attempting at a rate of* $2^a$ *per second per computer, to find the key within* $2^s$ *seconds, it will require:*
$\frac{2^k}{2^a \times 2^s} = 2^{k-(a+s)}$ *seconds*

- *48-bit key,* $2^{16}$ *attempts per second, in* $2^{24}$ *seconds:* $2^{48-(16+24)} = 256$
- *50-bit key,* $2^{15}$ *attempts per second, in* $2^{24}$ *seconds:* $2^{50-(15+24)} = 2048$
- *48-bit key,* $2^{16}$ *attempts per second, in* $2^{23}$ *seconds:* $2^{48-(16+23)} = 512$
- *50-bit key,* $2^{16}$ *attempts per second, in* $2^{24}$ *seconds:* $2^{50-(16+24)} = 1024$