

EE 4215 –Security Technology

Assignment 3 – Due date: April 8, 2019 (Monday) – mid-night

Electronic submission only on Canvas

Name: _____

Date: _____

Student ID: _____

Mark: _____

Submission guidelines:

- Please prepare your assignment in “PDF” format.
- For observe the departmental rules for late submission (i.e. 50% deduction per day).

Security Management

- 1) Assume that you are a manager responsible for the security of e-Banking systems in a bank. You heard that Hong Kong Monetary Authority (HKMA) had a guideline called the “Supervision of E-banking”
 - a) Google for the document, and give the URL showing where the above HKMA guideline for e-Banking can be found.
 - b) Read the HKMA guideline. Briefly describe at least three major technology-related controls relevant to e-banking that you need to consider in your e-Banking infrastructure.

[**Hint:** you only need to give a brief description (that is, a few lines) summarizing the main points. Please don't simply copy pages of paragraphs from the HKMA document without understanding.]

- c) Your e-Banking system is using a Cisco firewall to protect the Internet perimeter and your IT colleagues are familiar with this firewall. Now, to strengthen the security, it is proposed to purchase for another firewall to set up another tier of internal firewall. Your IT colleagues proposed to purchase the same Cisco firewall and use it as an internal firewall. Would you approve this proposal? Why?

Public Key Systems

- 2) Use the Euclidean Algorithm to find the greatest common divisor of 12,345 and 67,890.
- 3) In the RSA cryptosystem, it is possible that $M = C$, that is the plaintext and the ciphertext are identical. For modulus $N = 3127$, and encryption exponent $e = 17$, find a message M that encrypts to itself.

Technical Tools

4) Network packet sniffing.

- a) Install Wireshark to your machine. Please show evidence (e.g. screen dump) that you have downloaded and installed this package into your personal computer.
- b) Describe the purpose of this program. How do you start capturing the packets, and how do you use filters for just TCP packets?
- c) Start capturing the packets. While packet collection is still running, attempt to access to your email. Describe:
 - How you access to your email (e.g. using webmail, or pop3, etc)
 - Can your username and password be seen during the sniffing process?
 - During the sniffing process, can you observe other network protocols in addition to the protocol that you used for email access? If so, name two such protocols and briefly explain why they exist.

5) Install a mobile banking app to your iOS or Android device (if you don't have these devices, do this exercise with a web browser connecting to an e-banking site).

- a) Name the app or web environment you will use in this exercise.
- b) Google for "*web debugging proxy*". Pick one of such tools (e.g. "*Fiddler Web Debugger*", "*Burp Suite*", etc) and attempt to use it as a proxy to capture the list of URLs visited by your chosen mobile banking app.

Go to the login name, and arbitrary input values to attempt to login (You don't really need to login with a valid username / password; a failed login is good enough. But please only try it once)

Show the list of URLs that will be involved in the login process. Are all requests to the bank protected by SSL?

- c) Display the digital certificate of the HSBC HK website, and elaborate what kind of encryption standards are being used in this certificate.

~ END ~