CSC 411: Network Systems Security: CW 1: due 20th Nov 2015

Instructions:

Send your answer to the following 5 question in softcopy to wokelo@uonbi.ac.ke encrypted using W. Okelo-Odongo's public key and signed using your private key. If you send a file attachment, please ensure that the filename includes your surname and the string "csc411". You will also need to avail your public key. The lecturer's public key is available through server or email.

1) Assume a re-usable password authentication system that uses of an *"encrypted"* password file based on a one-way function, f(pw). Describe the dictionary attack on such a system. Explain how use of "salt" makes the dictionary attack difficult.

2) Briefly explain the *capabilities* based access authorization mechanism. Explain how the MAC (Message Authentication Code) could be employed to secure a *capability* against forgery.

3) Describe the memory protection mechanism based on the segmented memory architecture.

4) Consider the design and implementation of a biometric authentications system in which the template is stored in a card (token) carried by the owner. Explain how such a system works assuming that the card is to hold only the PIN of the owner, name of the owner, and a "signature" of the biometric template. (Note signature constructed using message digests (hash) and public key cryptography. I.e., describe the enrolment and the verification processes.

5) Explain why I/O protection is necessary for the successful realization of file access control mechanism such as that based on ACL.

6) Briefly describe the Diffie-Hellman key exchange system. Explain how it might be susceptible to man-in-the-middle attack. Explain how certificate authority system may be used to secure the Diffie-Hellman exchange from the man-in-the-middle vulnerability..

7) The time it takes to encrypt a message of n 64-bit blocks using a 64-bit key symmetric key cryptography algorithm is $\tau * n$. The time to encrypt the same using a public key cryptography algorithm is $\tau * 10^4 * n$.
How much faster, compared to the public key system, would a hybrid cryptographic system (described in the lecture notes) based on the above be? Show clearly how you have arrived at the answer.

8) In the context of a manual messaging systems, a common forgery attack involves the attacker cutting a signature from an intercepted message and pasting that signature on another bogus message.

Show that the digital message authentication system based on message digests and public key cryptography is relatively immune to this kind of attack. In this context explain the importance of "collision resistance property".