# CIS 4360 Introduction to Computer Security

## Home Assignment 2, Fall 2011 — ANSWERS

This concerns the basic requirements for Computer Security.

Examples taken from: Matt Bishop's Introduction to Computer Security, Addison-Wesley.

1. The aphorism "security through obscurity" suggests that hiding information provides some level of security. Give an example of a situation in which hiding information does not add appreciably to the security of a system. Then give an example of a situation in which it does.
   **Answer.** An example of a situation in which hiding information does not add appreciably to the security of a system is hiding the implementation of the UNIX password hashing algorithm. The algorithm can be determined by extracting the object code from the relevant library routine. Revealing the algorithm does not appreciably simplify the task of an attacker because he still must guess the password itself. An example of a situation in which hiding information adds appreciably to the security of a system is hiding the password or a cryptographic key. This is private information affecting a single user. Revealing it would give the attacker access to the user's account.

2. **New question.** Assume that you are allowed to use only 26 characters from the alphabet to construct passwords.

   (a) How many different passwords are possible if a password has exactly $n$ characters where $n = 4$ and $n = 8$, and there is no distinction between upper case and lower case characters.
   **Answer:** For $n = 4$: $26^4$; for $n = 8$: $26^8$.

   (b) How many different passwords are possible if a password is at most $n$ characters long where $n = 4$ and $n = 8$, and there is no distinction between upper case and lower case characters.
   **Answer:** For $n = 4$: $26^4 + 26^3 + 26^2 + 26 = \frac{26^5-1}{25}$ ; for $n = 8$: $26^8 + 26^7 + 26^6 + 26^5 + 26^4 + 26^3 + 26^2 + 26 = \frac{26^9-1}{25}$ .

3. Show that the three security services: Confidentiality, Integrity, and Availability are sufficient to deal with the threats of: ($a$) Disclosure, ($b$) Disruption, ($c$) Deception (*deceive* = to cause to accept as true or valid what is false or invalid), ($d$) Usurpation (*usurp* = a wrongful seizure or exercise of authority or privilege belonging to another; an encroachment).

   **Answer**

   (a) Disclosure: Confidentiality prevents disclosure.

   (b) Disruption: Availability prevents Disruption.

   (c) Deception: Integrity prevents accepting corrupted (false or invalid) data/entities.

   (d) Usurpation: Availability and Integrity will prevent Usurpation. If you hold in possession data or entities wrongfully then their Availability is affected. If you also exercise their authority (e.g., by impersonating them) then Integrity is affected.

4. Is it possible to design and implement a system in which *no* assumptions about trust (i.e., no security assumptions) are made? Why or why not?
   **Answer.** No—unless we assume that all entities (principals) of the system will *always* abide by the rules (in a world where there is no need for trust). If the system is supposed to perform Task A, and Alice compromises it, then when Bob executes it the next time the proper task will not be performed.

Mike Burmester