# Exercise 1

## Chapter 1

Review:

1.1

What is meant by the CIA triad?

* Confidentiality – Only the authorized people can read it.
* Integrity - Data has not been tampered
* Availability - Some sort of service is running.

Problems:

1.1

Consider a student information system (SIS) in which students provide a university student number (USN) and a card for account access. Give examples of confidentiality, integrity, and availability requirements associated with the system and, in each case, indicate the degree of the importance of the requirement.

* Confidentiality: Only the student and administration can see the data
* Integrity: The cards and the student number can't be changed.
* Availability: The card or the scanner can't be destroyed. System must be up.

1.4

For each of the following assets, assign a low, moderate, or high impact level for the loss of confidentiality, availability, and integrity, respectively. Justify your answers.

a. An organization managing public information on its Web server.

* C: low → it’s public data.
* I: High → The public information must be correct.
* A: High → A lot of people is probably relying on the data.

b. A law enforcement organization managing extremely sensitive investigative

information.

* C: High → “Extremely sensitive”
* I: High → An adversary could change important information
* A: Moderate → Depends on the urgency

c. A financial organization managing routine administrative information (not privacy-

related information).

* C: Low → Not private
* I: Moderate → It’s routine administrative information, so probably not a lot will happen if tampered with.
* A: Low → Ordering new office supplies can wait.

d. An information system used for large acquisitions in a contracting organization

contains both sensitive, pre-solicitation phase contract information and routine administrative information. Assess the impact for the two data sets separately and the information system as a whole.

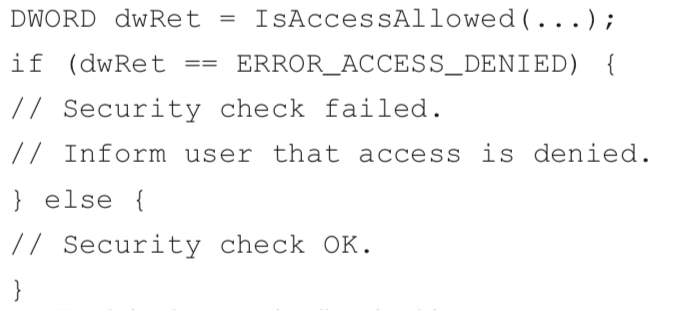
* Contract information
  + C: High → Sensitive information
  + I: Moderate → It’s pre-solicitating. Impact would be higher if it was the final offer.
  + A: Moderate → Depends on urgency
* Routine administrative
  + See c
* Information system as a whole
  + C: High as a whole
  + I: Moderate
  + A: High → Depends on urgency but as a whole the system always needs to be available.

e. A power plant contains a SCADA (supervisory control and data acquisition) system controlling the distribution of electric power for a large military installation. The SCADA system contains both real-time sensor data and routine administrative information. Assess the impact for the two data sets separately and the information system as a whole.

* Sensor data
  + C: High → It’s the military.
  + I: High → If the sensors are tampered with the plant could be given to much or to less power.
  + A:
* Routine information
* As a whole

1.5

Consider the following general code for allowing access to a resource:



1. Explain the security flaw in this program.

The code should be defensive. Should check for correctness and fail on all else. Right now if different error, you are clear.

1. Rewrite the code to avoid the flaw.

If (access granted) true

Else false.

## Chapter2

Review:

2.1

How is cryptanalysis different from brute-force attack?

* Cryptanalysis involves inspecting the cryptography and trying to break it through clever thinking. For example, decrypting a encrypted message using statistical analysis. A brute-force attack is an attack which just keeps trying different combinations until it gets it right. For example, trying to guess a private key. Cryptanalysis is much more effective but is not automatable.

2.5

What is one-way hash function?

* Something (plain-text and object etc.) with an arbitrary size is digested into a string, which can’t be reversed. Unlike encryption.

2.9

List and briefly define three uses of a public-key cryptosystem.

1. Verify that a person or a program is legit by decrypting their signature with their public key.
2. Secure contact between multiple individuals by publishing the public key.
3. Exchange a private key which is much faster than asymmetric encryption.

2.11

Do digital signatures provide confidentiality?

* No. Digital signatures is normally used when you put something public. It’s more important regarding integrity. Encryption would provide confidentiality (in some part).

Problems

2.1

Typically, in practice, the length of the message is greater than the block size of the encryption algorithm. The simplest approach to handle such encryption is known as electronic codebook (ECB) mode. Explain this mode. Mention a scenario where it cannot be applied. Explain briefly why it is not a secure mode of encryption.

2.5

In this problem, we will compare the security services that are provided by digital signatures (DS) and message authentication codes (MAC). We assume Oscar is able to observe all messages sent from Alice to Bob and vice versa. Oscar has no knowledge of any keys but the public one in case of DS. State whether and how (i) DS and (ii) MAC protect against each attack. The value auth(x) is computed with a DS or a MAC algorithm, respectively.

1. (Message integrity) Alice sends a message x = ;Transfer $1000 to Mark< in the clear and also sends auth(x) to Bob. Oscar intercepts the message and replaces “Mark” with “Oscar.” Will Bob detect this?
2. (Replay) Alice sends a message x = ;Transfer $1000 to Oscar< in the clear and also sends auth(x) to Bob. Oscar observes the message and signature and sends them 100 times to Bob. Will Bob detect this?
3. (Sender authentication with cheating third party) Oscar claims that he sent some message x with a valid auth(x) to Bob but Alice claims the same. Can Bob clear the question in either case?
4. (Authentication with Bob cheating) Bob claims that he received a message x with a valid signature auth(x) from Alice (e.g., “Transfer $1000 from Alice to Bob”) but Alice claims she has never sent it. Can Alice clear this question in either case?

2.6

Suppose H(M) is a cryptographic hash function that maps a message of an arbitrary bit length on to an n-bit hash value. Briefly explain the primary security requirements of the hash function H. Assume that H outputs 16-bit hash values. How many random messages would be required to find two different messages M and M' such that H(M) = H(M′).