Brandenburg University of Technology
Cottbus-Senftenberg
IT Security Group

Introduction into Cyber Security
– 1st Exercise Sheet –

Discussion on: October 24th, 2018

Topics

The first exercise sheet serves as an introduction to the topic as well as the repetition of some basics from the first chapters of the lectures.

Instructions

The exercise sheets are to be worked on by you in self-study. In the exercise classes, usually only the control / discussion of the solutions takes place. The following preparation is therefore obligatory:

1. Read the exercise sheet with the tasks carefully. In case you have questions, please resolve them in advance with the tutor or your fellow students.

2. Use the lecture slides to repeat the content of the current subject and check your knowledge.

Careful preparation and processing of the exercise sheets (in addition to attending the lecture) is an essential prerequisite for success in the final exam.

Task 1: Terminology

Check your background knowledge and answer the following questions.

a) What are the interests and goals of data security? Provide a brief description for each goal.

b) What additional goals are pursued in the concept of multilateral data security? Explain these protection goals briefly and explain how they might conflict with the classical ones.

c) Cyber security distinguishes between preventive and reactive security. Define the two areas from each other and name two examples of measures for each area.

d) Why is it that preventive measures are not sufficient for complete protection?

e) Describe the threats, which are directed directly against the security goals of data security. Provide an example for each threat.

f) Characterize the threats from e) with the following attributes:

- discoverable / undiscoverable
- preventable / unpreventable
- reversible / irreversible

Task 2: Security Goals

Consider the scenario of sending and receiving mails. Think about the different parties which are involved on the various layers of communication (for example sender, receiver, mail provider, routers, ...). Reason about the diversity regarding the interest in information gained about the communication between the sender and receiver.

a) Specify the existing security threats. Which security goals are endangered?

b) List concurrent requirements regarding the information exchange.

c) Name suitable security mechanisms against the given threats. How could a secure information exchange be achieved with respect to the concurrent requirements?

Task 3: Symmetric encryption block modes

Review the formulas for encrypting a plaintext block m_i and decrypting a ciphertext block c_i for the different modes discussed in the lecture (ECB, CBC, CFB, OFB and CTR mode).

In the following, let an encryption function E for bit strings of length 3 be given by the permutation cipher (in decimal notation):

$$\begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 1 & 3 & 2 & 7 & 5 & 0 & 4 & 6 \end{pmatrix}$$

For example E(101) = 000. Further a plaintext $m = 010111001111$ and a ciphertext $c' = E(m') = 100010110100$ are given. The MSB of m is 0.

a) Encrypt plaintext m with encryption function E in ECB mode.

b) Assume ciphertext c' is encrypted with E in CBC mode using initialization vector $IV = 111$. Decrypt ciphertext c'.

c) Encrypt the resulting plaintext of step (b) with E in CFB mode. Use $IV = 001$ as initialization vector.

d) Finally decrypt the resulting ciphertext of step (c) with E in OFB mode using initialization vector $IV = 100$.