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.

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) Cybersecuritydistinguishesbetweenpreventiveandreactivesecurity. Deﬁnethetwoareas 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?