Outline for September 29, 2023

Reading: text, §14, 4.1–4.2  Assignments: Homework 1, due October 9; Project teams, question, due Oct 11

1. Principles of secure design
   (a) Bases: simplicity, restrictiveness
   (b) Principle of least privilege
      i. Principle of least authority
   (c) Principle of fail-safe defaults
   (d) Principle of economy of mechanism
   (e) Principle of complete mediation
   (f) Principle of open design
   (g) Principle of separation of privilege
   (h) Principle of least common mechanism
   (i) Principle of least astonishment
      i. Principle of psychological acceptability

2. Policy
   (a) Sets of authorized, unauthorized states
   (b) Secure systems in terms of states
   (c) Defining confidentiality, integrity, availability
   (d) Policy models and mechanisms