# Vulnerability examples

## Summary

In this class exercise, we will come up with real world examples for vulnerabilities that facilitate violation of each security tenet. This should be performed without the aid of any electronic device.

## Prerequisites

* None

## Details

* Information Security is defined as
  + “Preservation of confidentiality, integrity, availability, authenticity, accountability, non-repudiation, and reliability of information” (International Organization for Standardization 2009)
  + Additionally, we include Authority

Figure 1-ISO/IEC 27000:2009

* For the eight security tenets defined below, provide a real-world example of a vulnerability that facilitates violating that tenet. Write them down in the area provided below. After the exercise, the instructor will call on each group to provide an example to the class. Provide the instructor with your list afterwards.

### Definitions

1. Data confidentiality
   * Assures that private or confidential information is not made available or disclosed to unauthorized individuals (Stallings, Brown 2012)
   * Privacy-Assures that individuals control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed
2. Integrity
   * Data integrity-Assures that information and programs are changed only in a specified and authorized manner (Stallings, Brown 2012)
   * System integrity-Assures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system
3. Availability
   * Assures that systems work promptly and service is not denied to authorized users (Stallings, Brown 2012)
4. Authenticity
   * The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator. This means verifying that users are who they say they are and that each input arriving at the system came from a trusted source (Stallings, Brown 2012)
5. Authority
   * The right of an entity to access specific things (Saltzer, Schroeder 1975)
6. Accountability
   * The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity (Stallings, Brown 2012)
7. Non-repudiation
   * The ability to ensure that a person cannot deny the authenticity of their signature on a document or the sending of a message that they originated (McCullagh, Caelli, 2000)
8. Reliability
   * The ability of the software system to perform its functions in its operational environment for a specified time period

### Examples

1. Confidentiality
2. Integrity
3. Availability
4. Authenticity
5. Accountability
6. Non-repudiation
7. Reliability

### References

* Saltzer, Schroeder 1975
* International Organization for Standardization 2009
* Stallings, Brown 2012
* McCullagh, Caelli, 2000