Security

- The security of a system is a system property that reflects the system’s ability to protect itself from accidental or deliberate external attack
- Security is becoming increasingly important as systems are networked so that external access to the system through the Internet is possible
- Security is an essential pre-requisite for availability, reliability and safety

Fundamental security

- If a system is a networked system and is insecure then statements about its reliability and its safety are unreliable
- These statements depend on the executing system and the developed system being the same. However, intrusion can change the executing system and/or its data
- Therefore, the reliability and safety assurance is no longer valid

Security terminology

Term	Definition
Exposure	Possible loss or harm in a computing system. This can be loss or damage to data or can be a loss of time and effort if recovery is necessary after a security breach.
Vulnerability	A weakness in a computer-based system that may be exploited to cause loss or harm.
Attack	An exploitation of a system vulnerability. Generally, this is from outside the system and is a deliberate attempt to cause some damage.
Threats	Circumstances that have potential to cause loss or harm. You can think of these as a system vulnerability that is subjected to an attack.
Control	A protective measure that reduces a system vulnerability. Encryption would be an example of a control that reduced a vulnerability of a weak access control system.

Damage from insecurity

- Denial of service
  - The system is forced into a state where normal services are unavailable or where service provision is significantly degraded
- Corruption of programs or data
  - The programs or data in the system may be modified in an unauthorised way
- Disclosure of confidential information
  - Information that is managed by the system may be exposed to people who are not authorised to read or use that information

Security assurance

- Vulnerability avoidance
  - The system is designed so that vulnerabilities do not occur. For example, if there is no external network connection then external attack is impossible
- Attack detection and elimination
  - The system is designed so that attacks on vulnerabilities are detected and neutralised before they result in an exposure. For example, virus checkers find and remove viruses before they infect a system
- Exposure limitation
  - The system is designed so that the adverse consequences of a successful attack are minimised. For example, a backup policy allows damaged information to be restored

Best Practices of Software Security

1. **Requirements and Code technical reviews**
2. **Extensive Unit Testing (including out of range testing)**
3. **Architectural risk analysis**
4. **Penetration testing**
5. **Risk based security testing**
6. **Misuse cases**
7. **Security requirements**
8. **Security operation**

Key points

- Reliability is related to the probability of an error occurring in operational use. A system with known faults may be reliable
- Safety is a system attribute that reflects the system’s ability to operate without threatening people or the environment
- Security is a system attribute that reflects the system’s ability to protect itself from external attack
- Dependability improvement requires a socio-technical approach to design where you consider the humans as well as the hardware and software