

## System security engineering

**Name:**

1. Explain why security engineering is a whole life-cycle activity?

Because security problems are a result of activities that may arise at any stage in the life cycle – e.g. development errors, configuration errors, management errors, operational processes, etc.

2. What are the principal types of security failure?

Denial of service, corruption of data managed by the system  
Disclosure of information, unauthorised use of system resources  
Unauthorised amendments to software, unauthorised changes to policies

3. What are the goals of system security engineering?

To identify threats faced by the system  
To identify process and product requirements to counter these threats  
To identify constraints that improve security  
To identify recovery requirements

4. What is the distinction between process and product security?

Product security is concerned with avoiding vulnerabilities in the system product

Process security is concerned with avoiding vulnerabilities in the development and operational processes that may be exploited to attack the system.

5. What are the stages in the system security engineering process?

Asset identification, Threat analysis and risk assessment  
Technology analysis, Threat assignment,  
Security requirements specification

6. Why are insider threats particularly difficult to address?

Because technical mechanisms designed to stop attacks at the system boundaries cannot be used.  
An attack by an insider may appear to be a legitimate use of the system.

7. List 10 different types of security requirement

Identification requirements, authentication requirements, authorisation requirements  
Immunity requirements, integrity requirements, intrusion detection requirements,  
Non-repudiation requirements, privacy requirements, security auditing requirements  
System maintenance security requirements

8. Give three examples of possible recovery requirements for an information system.

The system database shall be backed up each day

A backup server shall be identified and application software shall be pre-installed on that backup system

Detailed records of configuration data for all applications shall be maintained