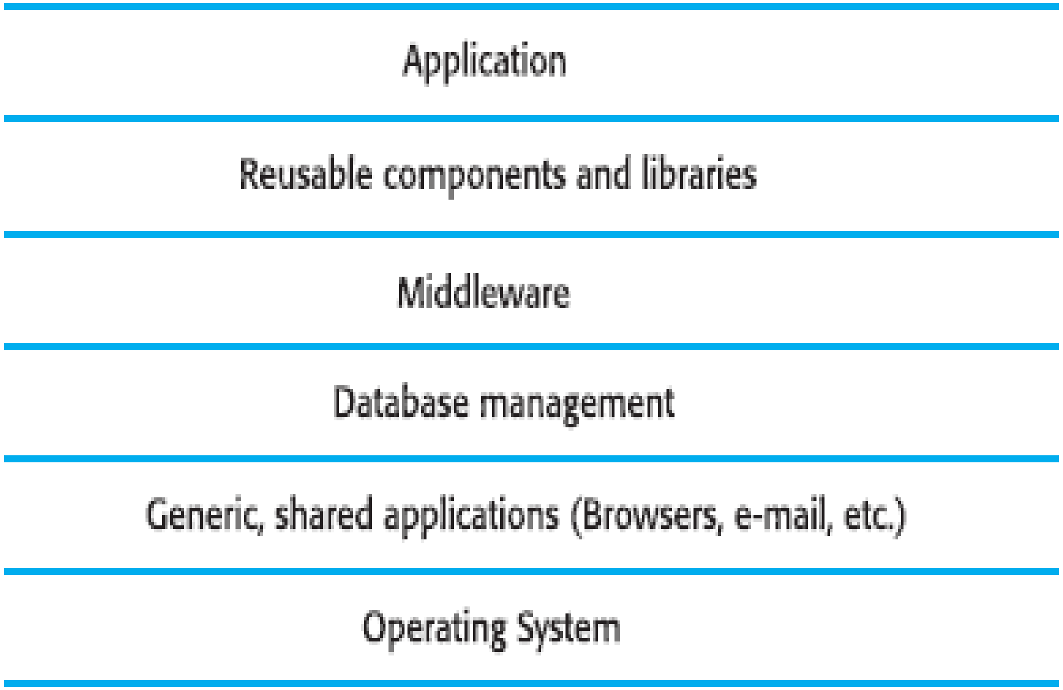
Security Engineering

Chapter 30 – Sommerville 8th Edition

Security Engineering

- **Security engineering** is a specialized field of engineering that focuses on the security aspects in the design of systems that need to be able to deal robustly with possible sources of disruption, ranging from natural disasters to malicious acts.
- It is similar to other systems engineering activities in that its primary motivation is to support the delivery of engineering solutions that satisfy pre-defined functional and user requirements, but with the added dimension of preventing misuse and malicious behavior. These constraints and restrictions are often asserted as a security policy.

Figure 30.1 System layers where security may be compromised



Application

Reusable components and libraries

Middleware

Database management

Generic, shared applications (Browsers, e-mail, etc.)

Operating System

Security Concepts

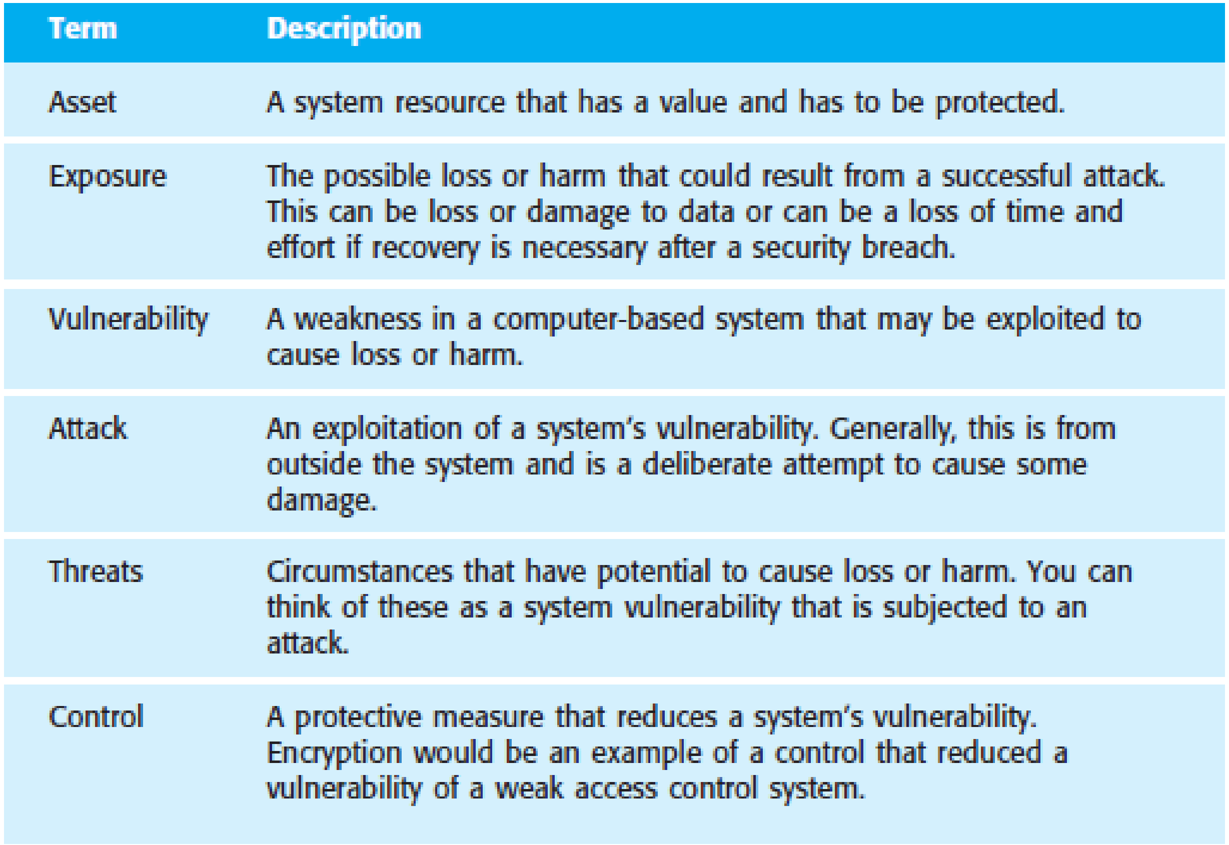
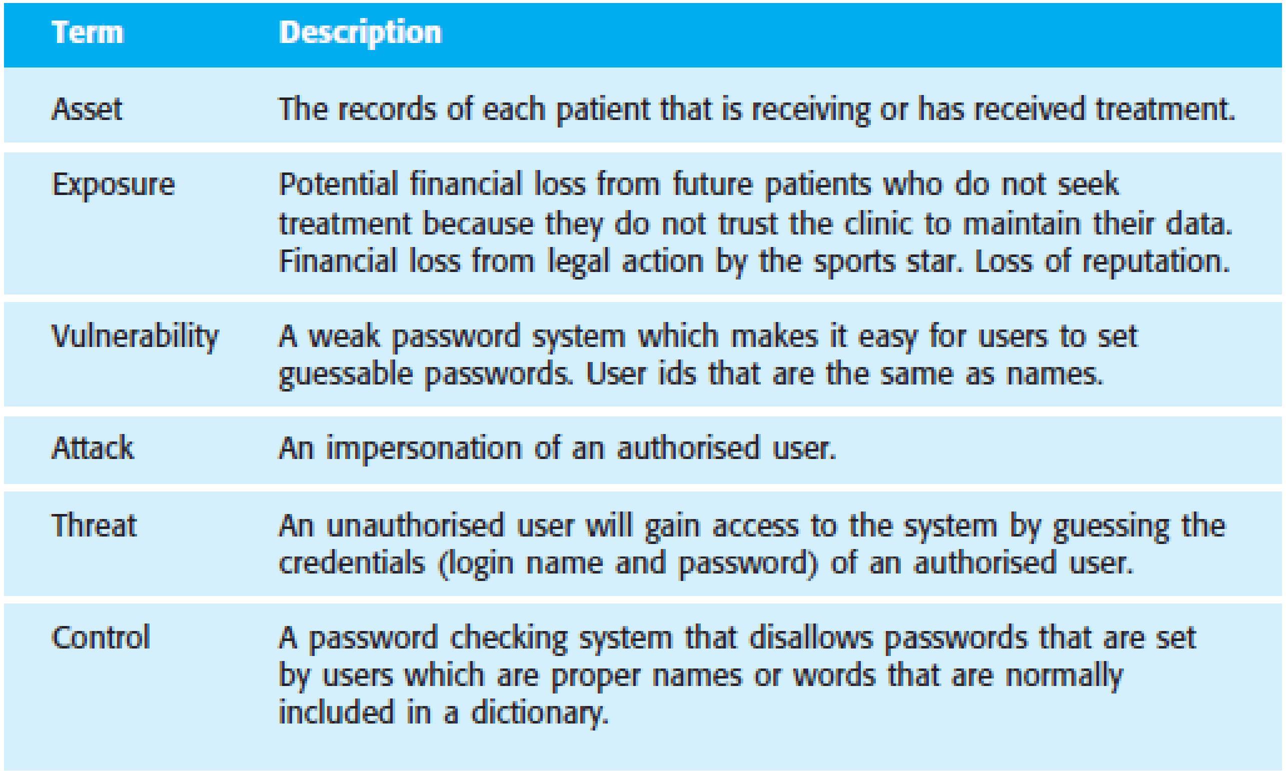


Figure 30.2 Security concepts

Term	Description
Asset	A system resource that has a value and has to be protected.
Exposure	The possible loss or harm that could result from a successful attack. 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's 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's vulnerability. Encryption would be an example of a control that reduced a vulnerability of a weak access control system.

Security Concepts - Example

Figure 30.3 Security concept examples



Term	Description
Asset	The records of each patient that is receiving or has received treatment.
Exposure	Potential financial loss from future patients who do not seek treatment because they do not trust the clinic to maintain their data. Financial loss from legal action by the sports star. Loss of reputation.
Vulnerability	A weak password system which makes it easy for users to set guessable passwords. User ids that are the same as names.
Attack	An impersonation of an authorised user.
Threat	An unauthorised user will gain access to the system by guessing the credentials (login name and password) of an authorised user.
Control	A password checking system that disallows passwords that are set by users which are proper names or words that are normally included in a dictionary.

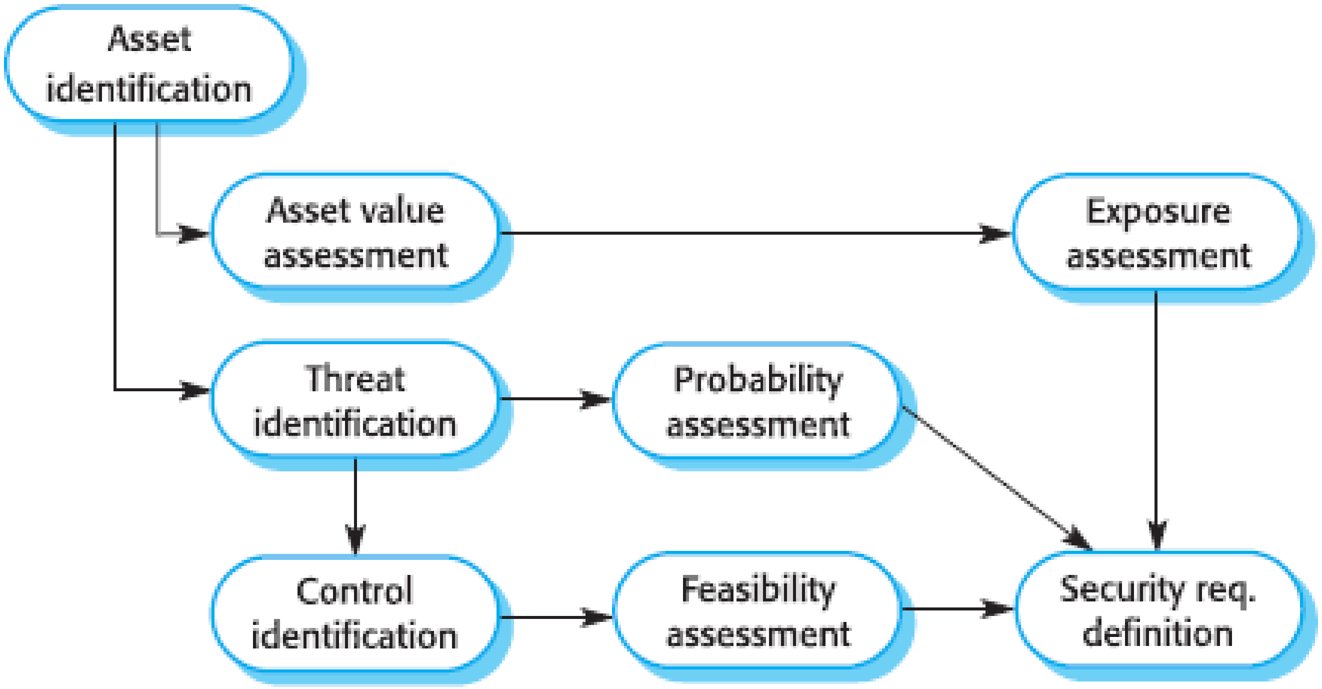
Risk Assessment in Security Engineering

- Risk assessment starts before the decision to acquire the system has been made and should continue throughout the system development process. An important consideration is the amount of information that you have available about the system so risk assessment is a staged process:
- 1. *Preliminary risk assessment* At this stage, decisions on the detailed system requirements, the system design or the implementation technology have not been made. The aim of this assessment process is, firstly, to assess whether or not the benefits of developing the system justify the associated risks and then to derive specific security requirements for the system to be implemented. You do not have information about potential vulnerabilities in the system or the controls that are included in reused system components or middleware.

Risk Assessment in Security Engineering

- 2. *Life cycle risk assessment* This risk assessment takes place during the system development life cycle and is informed by the technical system design and implementation decisions. It informs the process of security requirements engineering. Known and potential vulnerabilities are identified and this knowledge is used to inform decision-making about the system functionality and how it is to be implemented, tested and deployed.

Preliminary Risk Assessment



Preliminary Risk Assessment Stages

- 1. Asset identification where the system assets that may require protection are identified. The system itself or particular system functions may be identified as assets as well as the data associated with the system.
- 2. Asset value assessment where you estimate the value of the identified assets.
- 3. Exposure assessment where you assess the potential losses associated with each asset.
- 4. Threat identification where you identify the threats to system assets.
- 5. Probability assessment where you estimate the probability of each threat.
- 6. Control identification where you propose the controls that might be put in place to protect an asset.
- 7. Feasibility assessment where you assess the technical feasibility and the costs of the proposed controls.
- 8. Security requirements definition where the exposure, threats and control assessments are used to derive a set of system security requirements. These may be requirements for the system infrastructure or the application system.

Life Cycle Risk Assessment

- The important distinction between life cycle risk assessment and preliminary risk assessment is that, in life cycle risk assessment, knowledge of the system architecture and data organisation is available.
- Procurement decisions have been made so the system platform and middleware have been chosen. A development strategy, such as ‘configure a generic application’, may have been chosen.
- This means that you have much more detailed information about what needs to be protected and you will know something about the vulnerabilities in the system.
- Some of these vulnerabilities will be inherent in the design choices made (e.g. a vulnerability in any password-based system is that an authorised user reveals their password to an unauthorised user) but you may have to make assumptions about other possible vulnerabilities.

Life Cycle Risk Assessment

- Security risk assessment should be part of all life cycle activities from requirements engineering to system deployment. The process followed is similar to the preliminary risk assessment process with the addition of activities concerned with vulnerability identification and assessment.
- Vulnerability assessment identifies the assets that are likely to be affected by that vulnerability and relates these vulnerabilities to possible system attacks. The outcome of the risk assessment is a set of engineering decisions that affect the system design or implementation or limit the way in which it is used.

Life Cycle Risk Assessment

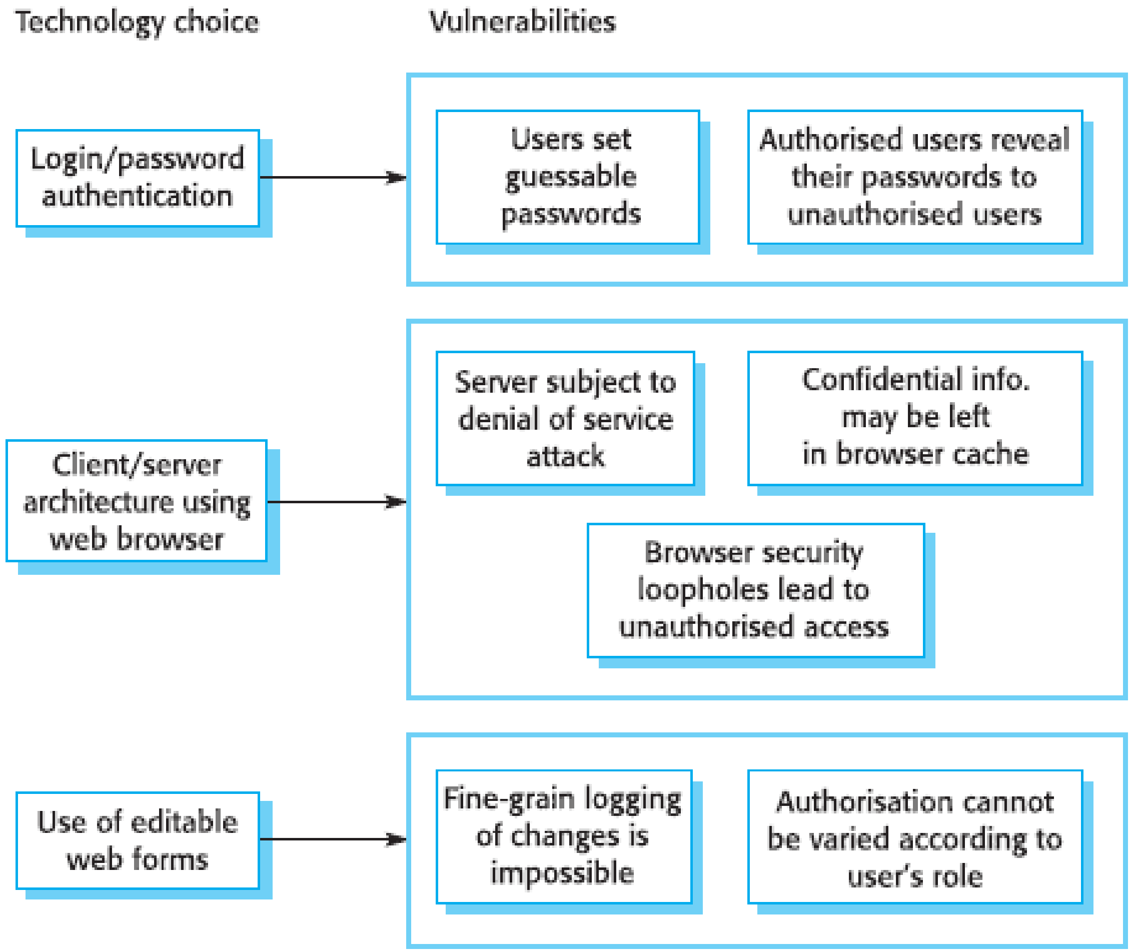


Figure 30.7 Vulnerabilities associated with technology choices

Technology choice

Vulnerabilities

Login/password authentication

Users set guessable passwords

Authorised users reveal their passwords to unauthorised users

Client/server architecture using web browser

Server subject to denial of service attack

Confidential info. may be left in browser cache

Browser security loopholes lead to unauthorised access

Use of editable web forms

Fine-grain logging of changes is impossible

Authorisation cannot be varied according to user's role

THANK YOU!!!