Security Engineering

Objectives

- To introduce issues that must be considered in the specification and design of secure software
- To discuss security risk management and the derivation of security requirements from a risk analysis
- To describe good design practice for secure systems development.
- To explain the notion of system survivability and to introduce a method of survivability analysis.

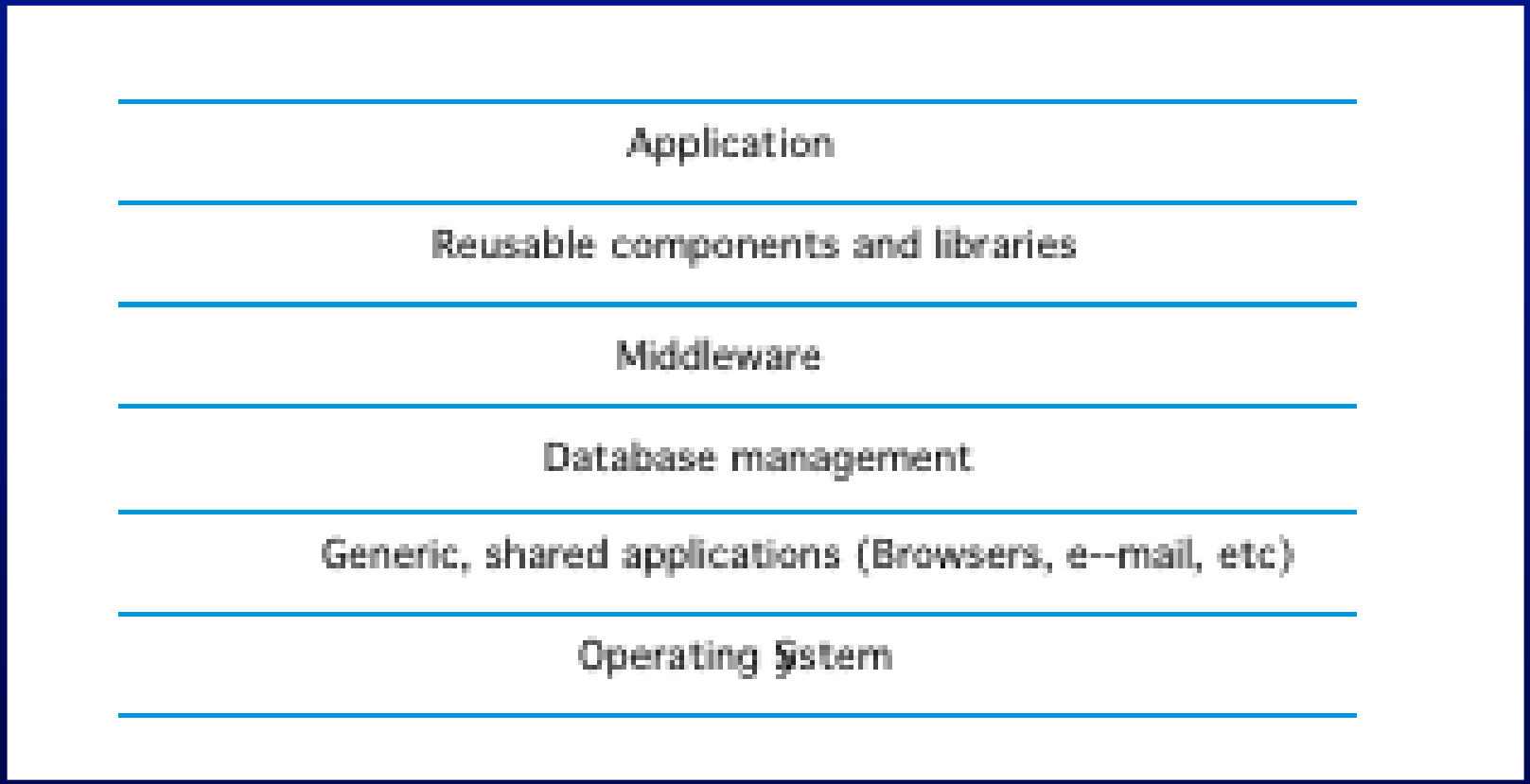
Topics covered

- Security concepts
- Security risk management
- Design for security
- System survivability

Security engineering

- Tools, techniques and methods to support the development and maintenance of systems that can resist malicious attacks that are intended to damage a computer-based system or its data.
- A sub-field of the broader field of computer security.

System layers



Application/infrastructure security

- Application security is a software engineering problem where the system is designed to resist attacks.
- Infrastructure security is a systems management problem where the infrastructure is configured to resist attacks.
- The focus of this chapter is application security.

Security concepts

Term	Definition
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.

Examples of security concepts

Term	Definition
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.

Security threats

- Threats to the confidentiality of a system or its data
- Threats to the integrity of a system or its data
- Threats to the availability of a system or its data

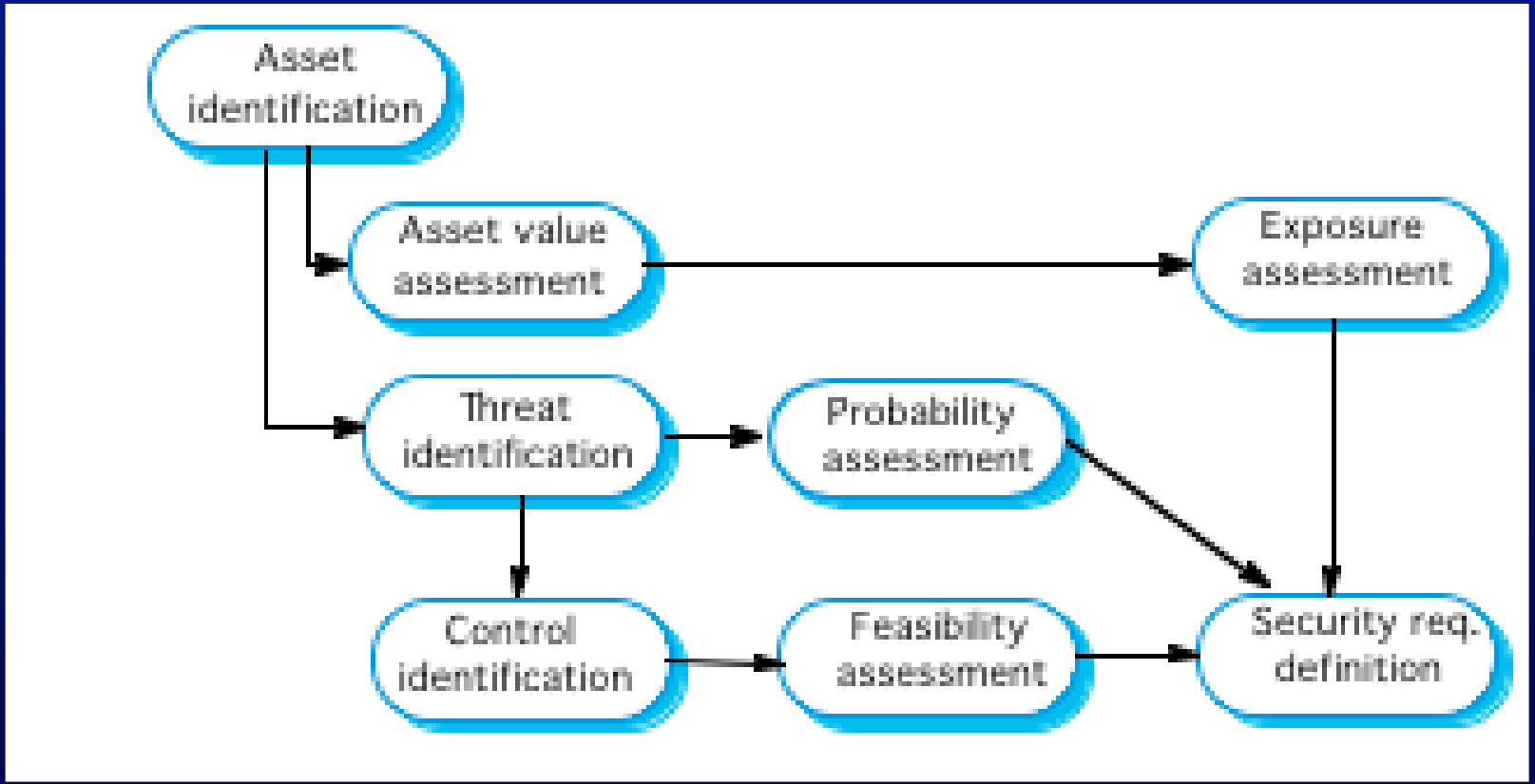
Security controls

- Controls that are intended to ensure that attacks are unsuccessful. This is analagous to fault avoidance.
- Controls that are intended to detect and repel attacks. This is analagous to fault detection and tolerance.
- Controls that are intended to support recovery from problems. This is analagous to fault recovery.

Security risk management

- Risk management is concerned with assessing the possible losses that might ensue from attacks on the system and balancing these losses against the costs of security procedures that may reduce these losses.
- Risk management should be driven by an organisational security policy.
- Risk management involves
  - Preliminary risk assessment
  - Life cycle risk assessment

Preliminary risk assessment



Asset analysis

Asset	Value	Exposure
The information system	High. Required to support all clinical consultations. Potentially safety critical.	High. Financial loss as clinics may have to be cancelled. Costs of restoring system. Possible patient harm if treatment cannot be prescribed.
The patient database	High. Required to support all clinical consultations. Potentially safety critical.	High. Financial loss as clinics may have to be cancelled. Costs of restoring system. Possible patient harm if treatment cannot be prescribed.
An individual patient record	Normally low although may be high for specific high-profile patients	Low direct losses but possible loss of reputation.

Threat and control analysis

Threat	Probability	Control	Feasibility
Unauthorised user gains access as system manager and makes system unavailable	Low	Only allow system management from specific locations which are physically secure.	Low cost of implementation but care must be taken with key distribution and to ensure that keys are available in the event of an emergency.
Unauthorised user gains access as system user and accesses confidential information	High	Require all users to authenticate themselves using biometric mechanism. Log all changes to patient information to track system usage.	Technically feasible but high cost solution. Possible user resistance. Simple and transparent to implement and also supports recovery.

Security requirements

- Patient information must be downloaded at the start of a clinic session to a secure area on the system client that is used by clinical staff.
- Patient information must not be maintained on system clients after a clinic session has finished.
- A log on a separate computer from the database server must be maintained of all changes made to the system database.

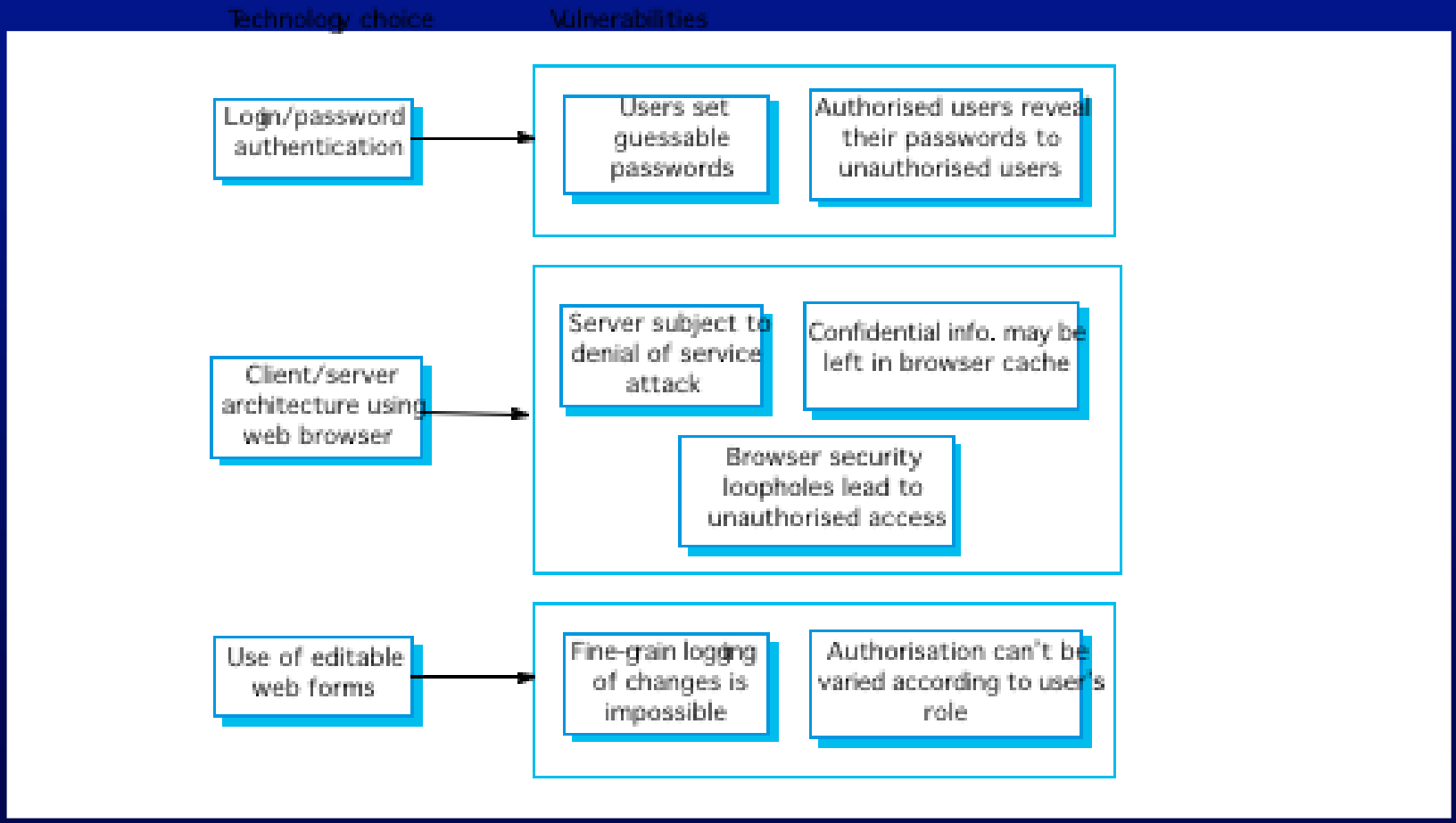
Life cycle risk assessment

- Risk assessment while the system is being developed and after it has been deployed
- More information is available - system platform, middleware and the system architecture and data organisation.
- Vulnerabilities that arise from design choices may therefore be identified.

Examples of design decisions

- System users authenticated using a name/password combination.
- The system architecture is client-server with clients accessing the system through a standard web browser.
- Information is presented as an editable web form.

Technology vulnerabilities



Design for security

- Architectural design - how do architectural design decisions affect the security of a system?
- Good practice - what is accepted good practice when designing secure systems?
- Design for deployment - what support should be designed into a system to avoid the introduction of vulnerabilities when a system is deployed for use?

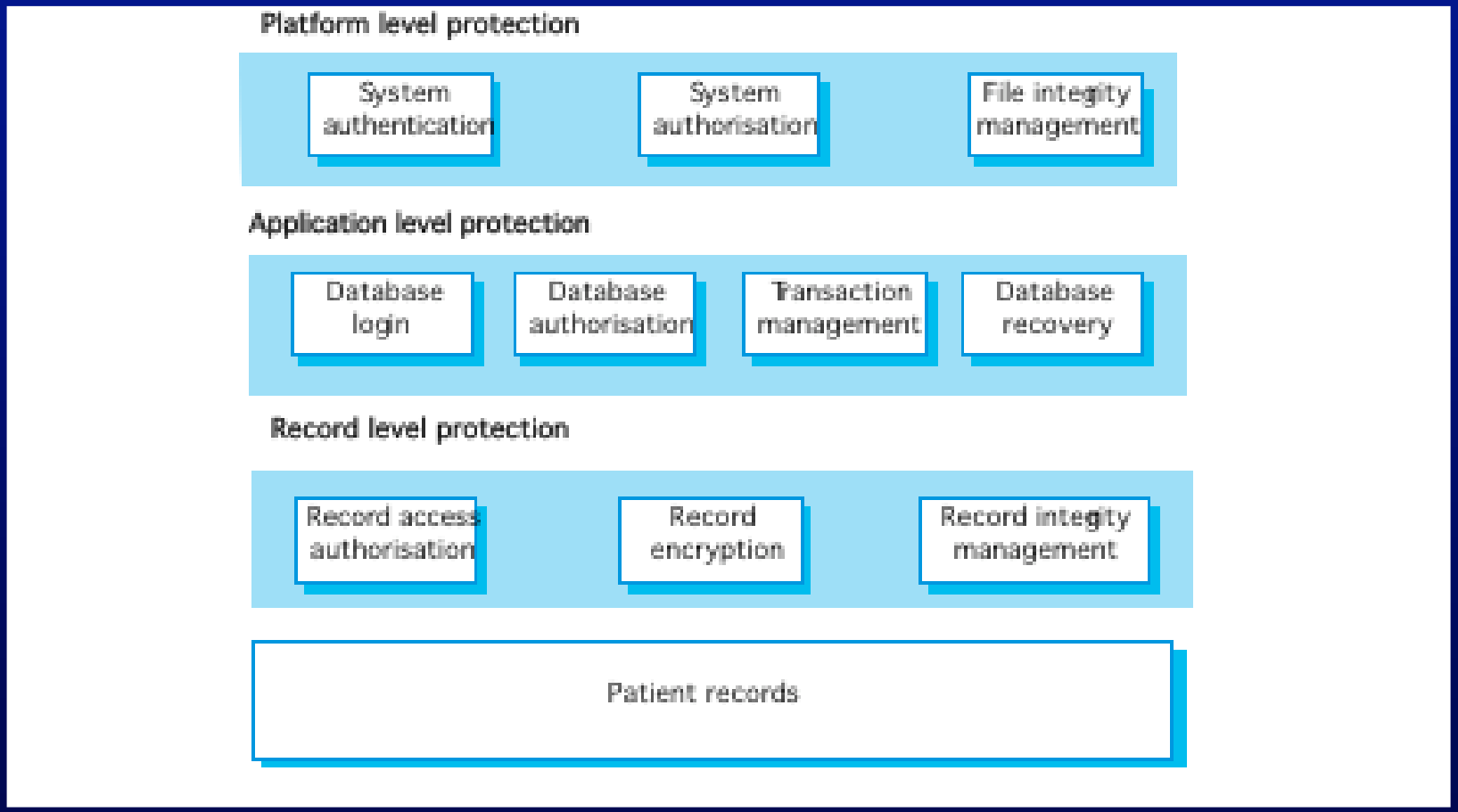
Architectural design

- Protection
  - How should the system be organised so that critical assets can be protected against external attack?
- Distribution
  - How should system assets be distributed so that the effects of a successful attack are minimised?
- Potentially conflicting
  - If assets are distributed, then they are more expensive to protect.

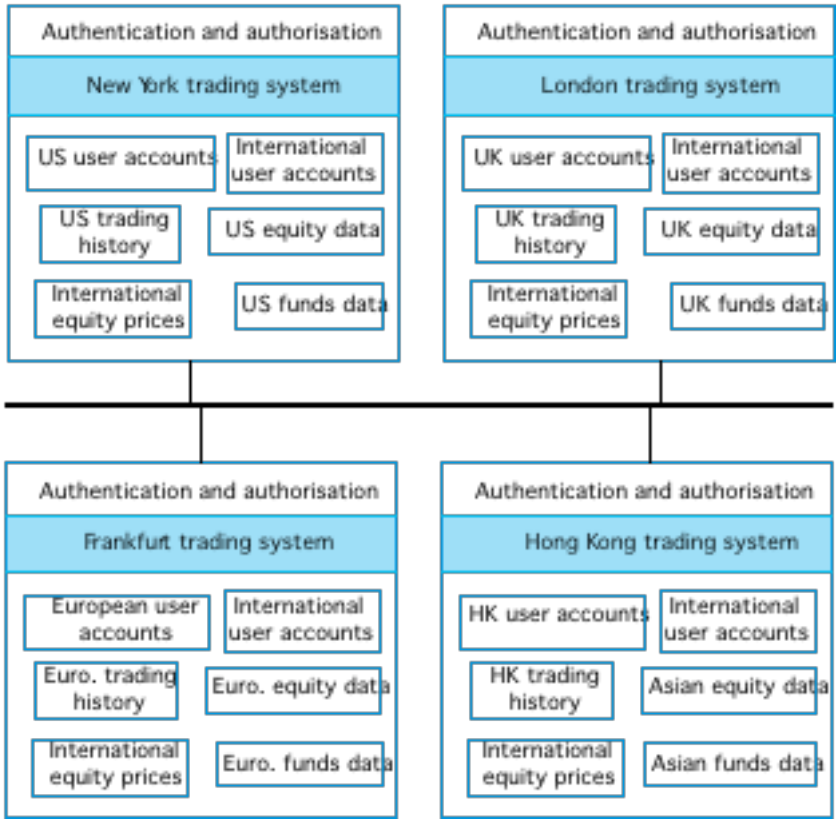
Protection

- Platform-level protection
- Application-level protection
- Record-level protection

Layered protection



A distributed equity system



Design guidelines

- Design guidelines encapsulate good practice in secure systems design
- Design guidelines serve two purposes:
  - They raise awareness of security issues in a software engineering team.
  - They can be used as the basis of a review checklist that is applied during the system validation process.

Design guidelines 1

- Base security decisions on an explicit security policy
- Avoid a single point of failure
- Fail securely
- Balance security and usability
- Be aware of the possibilities of social engineering

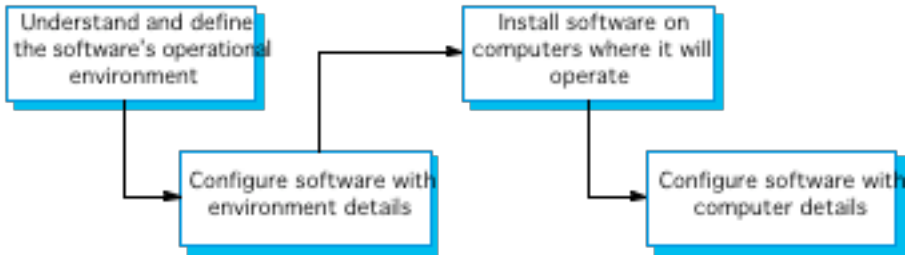
Design guidelines 2

- Use redundancy and diversity to reduce risk
- Validate all inputs
- Compartmentalise your assets
- Design for deployment
- Design for recoverability

Design for deployment

- Deployment involves configuring software to operate in its working environment, installing the system and configuring it for the operational platform.
- Vulnerabilities may be introduced at this stage as a result of configuration mistakes.
- Designing deployment support into the system can reduce the probability that vulnerabilities will be introduced.

System deployment



Deployment support

- Include support for viewing and analysing configurations
- Minimise default privileges and thus limit the damage that might be caused
- Localise configuration settings
- Provide easy ways to fix security vulnerabilities

System survivability

- Survivability is an emergent system property that reflects the systems ability to deliver essential services whilst it is under attack or after part of the system has been damaged
- Survivability analysis and design should be part of the security engineering process

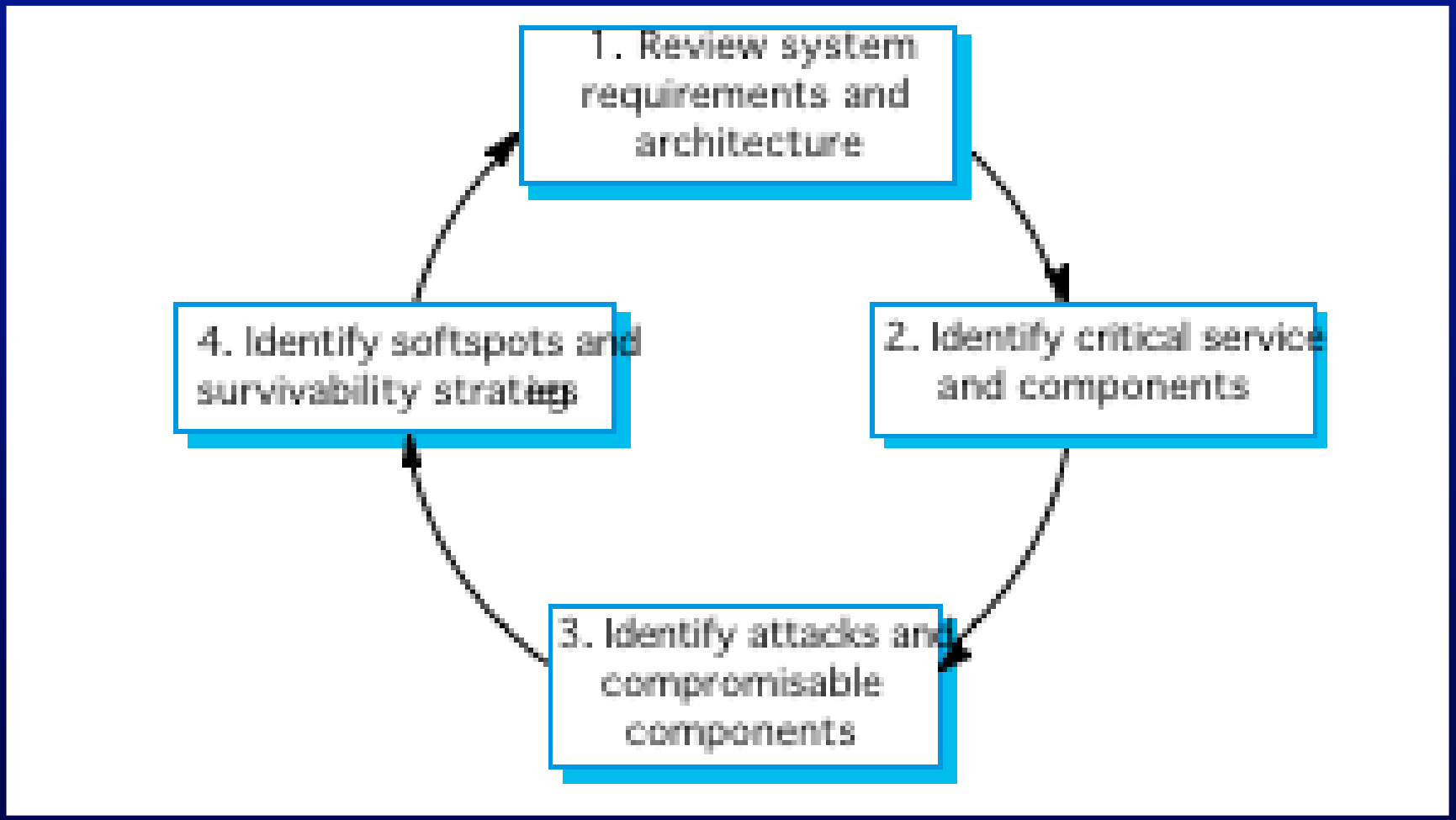
Service availability

- Which system services are the most critical for a business?
- How might these services be compromised?
- What is the minimal quality of service that must be maintained?
- How can these services be protected?
- If a service becomes unavailable, how quickly can it be recovered?

Survivability strategies

- Resistance
  - Avoiding problems by building capabilities into the system to resist attacks
- Recognition
  - Detecting problems by building capabilities into the system to detect attacks and failures and assess the resultant damage
- Recovery
  - Tolerating problems by building capabilities into the system to deliver services whilst under attack

System survivability method



Key activities

- System understanding
  - Review golas, requirements and architecture
- Critical service identification
  - Identify services that must be maintained
- Attack simulation
  - Devise attack scenarios and identify components affected
- Survivability analysis
  - Identify survivability strategies to be applied

Trading system survivability

- User accounts and equity prices replicated across servers so some provision for survivability made
- Key capability to be maintained is the ability to place orders for stock
- Orders must be accurate and reflect the actual sales/purchases made by a trader

Survivability analysis

Attack	Resistance	Recognition	Recovery
Unauthorised user places malicious orders	Require dealing password to place orders that is different from login password.	Send copy of order by email to authorised user with contact phone number (so that they can detect malicious orders) Maintain user's order history and check for unusual trading patterns.	Provide mechanism to automatically 'undo' trades and restore user accounts. Refund users for losses that are due to malicious trading. Insure against consequential losses.
Corruption of transactions database	Require privileged users to be authorised using a stronger authentication mechanism, such as digital certificates.	Maintain read-only copies of transactions for an office on an international server. Periodically compare transactions to check for corruption. Maintain cryptographic checksum with all transaction records to detect corruption.	Recover database from backup copies. Provide a mechanism to replay trades from a specified time to recreate transactions database.

Key points

- Security engineering is concerned with how to develop systems that can resist malicious attacks
- Security threats can be threats to confidentiality, integrity or availability of a system or its data
- Security risk management is concerned with assessing possible losses from attacks and deriving security requirements to minimise losses
- Design for security involves architectural design, following good design practice and minimising the introduction of system vulnerabilities

Key points

- Key issues when designing a secure architecture include organising the structure to protect assets and distributing assets to minimise losses
- General security guidelines sensitise designers to security issues and serve as review checklists
- Configuration visualisation, setting localisation, and minimisation of default privileges help reduce deployment errors
- System survivability reflects the ability of a system to deliver services whilst under attack or after part of the system has been damaged.