Lec15

> Security and dependability
>
> Security and organizations
>
> Security requirements
>
> Secure systems design
>
> Security testing and assurance

Security dimensions

Confidentiality

§ Information in a system may be disclosed or made accessible to people or programs that are not authorized to have access to that information.

Integrity

§ Information in a system may be damaged or corrupted making it unusual or unreliable.

Availability

§ Access to a system or its data that is normally available may not be possible.

Security levels

Infrastructure security, which is concerned with maintaining the security of all systems and networks that provide an infrastructure and a set of shared services to the organization.

Application security, which is concerned with the security of individual application systems or related groups of systems.

Operational security, which is concerned with the secure operation and use of the organization's systems.

Application security is a software engineering problem where the system is designed to resist attacks.（System 拒绝被攻击

Infrastructure security is a systems management（系统管理

System security management

User and permission management

§ Adding and removing users from the system and setting up appropriate permissions for users

Software deployment and maintenance

§ Installing application software and middleware and configuring these systems so that vulnerabilities are avoided.

Attack monitoring, detection and recovery

§ Monitoring the system for unauthorized access, design strategies for resisting attacks and develop backup and recovery strategies.

Operational security

Primarily a human and social issue

Concerned with ensuring the people do not take actions that may compromise system security

Users sometimes take insecure actions to make it easier for them to do their jobs

There is therefore a trade-off between system security and system effectiveness.

Security and dependability

Term	Definition
Asset	Something of value which has to be protected. The asset may be the software system itself or data used by that system.
Attack	An exploitation of a system's vulnerability. Generally, this is from outside the system and is a deliberate attempt to cause some damage.
Control	A protective measure that reduces a system's vulnerability. Encryption is an example of a control that reduces a vulnerability of a weak access control system
Exposure	Possible loss or harm to 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.
Threat	Circumstances that have potential to cause loss or harm. You can think of these as a system vulnerability that is subjected to an attack.
Vulnerability	A weakness in a computer-based system that may be exploited to cause loss or harm.

Term	Example
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 authorized user.
Threat	An unauthorized user will gain access to the system by guessing the credentials (login name and password) of an authorized user.
Control	A password checking system that disallows user passwords that are proper names or words that are normally included in a dictionary.

Threat types

Interception threats that allow an attacker to gain access to an asset.

Interruption threats that allow an attacker to make part of the system unavailable.

Modification threats that allow an attacker to tamper with a system asset.

Fabrication threats that allow an attacker to insert false information into a system.

Security assurance

 Vulnerability avoidance

 Attack detection and elimination

 Exposure limitation and recovery

Security and dependability

 Security and reliability

If a system is attacked and the system or its data are corrupted as a consequence of that attack, then this may induce system failures that compromise the reliability of the system.

如果系统受到攻击并且系统或其数据因该攻击而损坏，则这可能会导致系统故障，从而危及系统的可靠性。

 Security and availability

A common attack on a web-based system is a denial of service attack, where a web server is flooded with service requests from a range of different sources. The aim of this attack is to make the system unavailable.

对基于 Web 的系统的常见攻击是拒绝服务攻击，其中 Web 服务器充斥着来自各种不同来源的服务请求。这种攻击的目的是使系统不可用

 Security and safety

An attack that corrupts the system or its data means that assumptionsabout safety may not hold. Safety checks rely on analysing the sourcecode of safety critical software and assume the executing code is acompletely accurate translation of that source code. If this is not thecase, safety-related failures may be induced and the safety case made for the software is invalid.

破坏系统或其数据的攻击意味着关于安全的假设可能不成立。安全检查依赖于分析安全关键软件的源代码，并假设执行代码是该源代码的完全准确翻译。否则，可能会引发与安全相关的故障，并且为软件制定的安全案例无效。

 Security and resilience

Resilience is a system characteristic that reflects its ability to resist andrecover from damaging events. The most probable damaging event on networked software systems is a cyberattack of some kind so most of the work now done in resilience is aimed at deterring, detecting and recovering from such Chapter 13 Security Engineerin gattacks.

复原力是一种系统特性，反映了其抵御破坏性事件和从破坏性事件中恢复的能力。网络软件系统上最可能的破坏性事件是某种网络攻击，因此现在在弹性方面所做的大部分工作旨在阻止、检测和从第 13 章安全工程中的此类攻击中恢复。

Security risk assessment and management

Risk management involves

 Preliminary risk assessment

 Life cycle risk assessment

 Operational risk assessment

Preliminary risk assessment

The aim of this initial risk assessment is to identify generic risks that are applicable to the system and to decide if an adequate level of security can be achieved at a reasonable cost

> 此初始风险评估的目的是识别适用于系统的一般风险，并决定是否可以以合理的成本实现足够的安全级别。

 The risk assessment should focus on the identification and analysis of high-level risks to the system.

 The outcomes of the risk assessment process are used to help identify security requirements.

Design risk assessment

在development的时候

评估的结果会影响到security requirements and the addition of new requirements

识别潜在的漏洞，为系统决策提供信息；实现测试与部署

Operational risk assessment

 This risk assessment process focuses on the use of the system and the possible risks that can arise from human behavior.

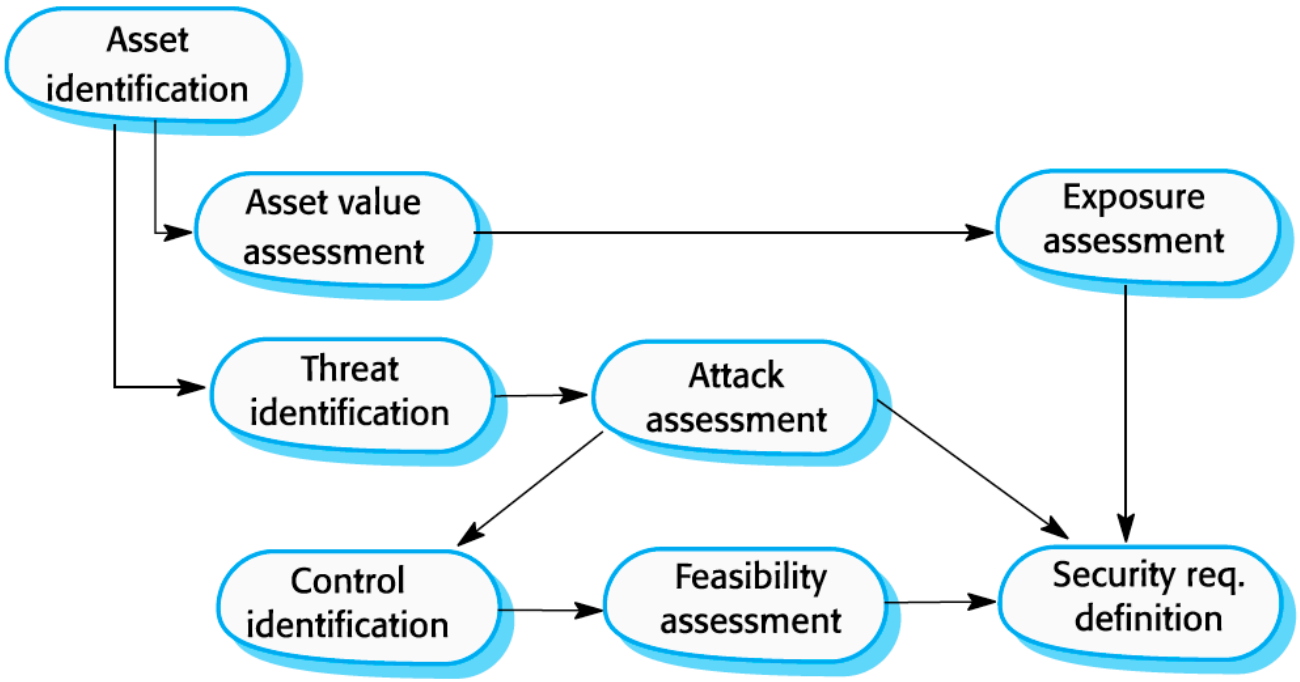
 该风险评估过程侧重于系统的使用以及人类行为可能产生的风险。

 Operational risk assessment should continue after a system has been installed to take account of how the system is used.

 系统安装后应继续进行操作风险评估，以考虑系统的使用情况。

 Organizational changes may mean that the system is used in different ways from those originally planned. These changes lead to new security requirements that have to be implemented as the system evolves.

 组织变化可能意味着系统的使用方式与最初计划的方式不同。随着系统的发展，这些变化导致必须实施新的安全要求。



Security risk assessment

 Asset identification

  Identify the key system assets (or services) that have to be protected.

 Asset value assessment

  Estimate the value of the identified assets.

 Exposure assessment

  Assess the potential losses associated with each asset.

 Threat identification

  Identify the most probable threats to the system assets

 Attack assessment

  Decompose threats into possible attacks on the system and the ways that these may occur.

 Control identification

  Propose the controls that may be put in place to protect an asset.

 Feasibility assessment

  Assess the technical feasibility and cost of the controls.

 Security requirements definition

  Define system security requirements. These can be infrastructure or application system requirements.

Misuse cases（定义！！！）

 Misuse cases are **instances** of threats to a system

 Interception threats

  Attacker gains access to an asset

 Interruption threats

  Attacker makes part of a system unavailable

 Modification threats

  A system asset is tampered with

 Fabrication threats

  False information is added to a system

Secure systems design

 Security should be designed into a system – it is very difficult to make an insecure system secure after it has been designed or implemented

 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 compromises

 Adding security features to a system to enhance its security affects other attributes of the system

 Performance

  Additional security checks slow down a system so its response time orthroughput may be affected

 Usability

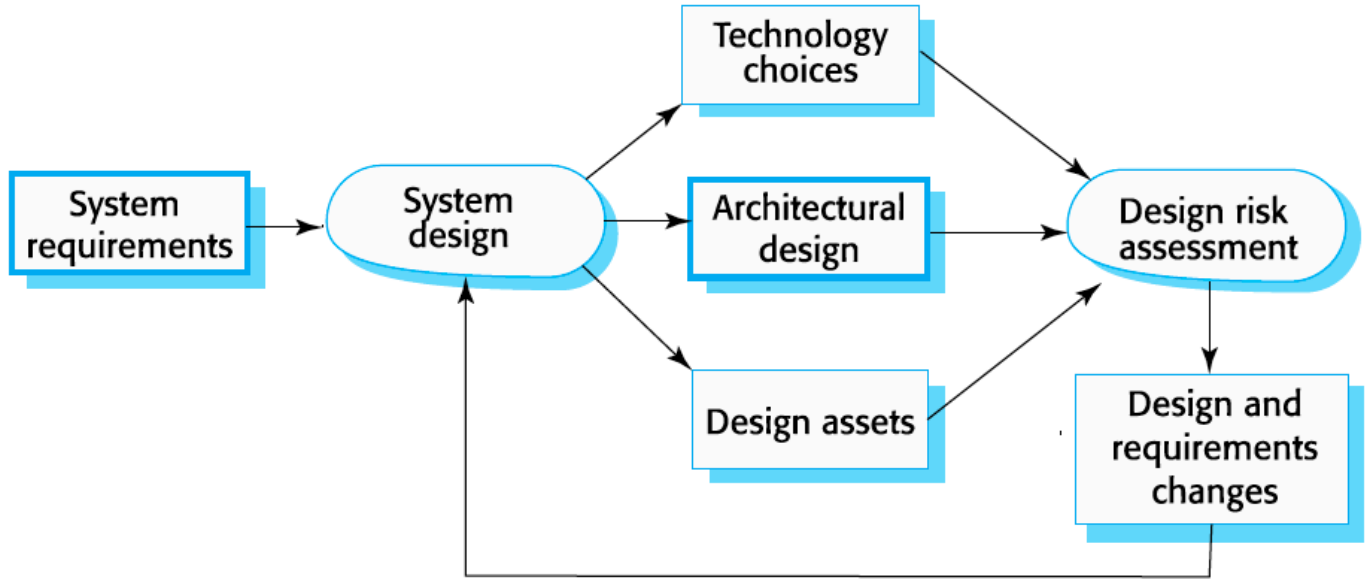
  Security measures may require users to remember information orrequire additional interactions to complete a transaction. This makes the system less usable and can frustrate system users.

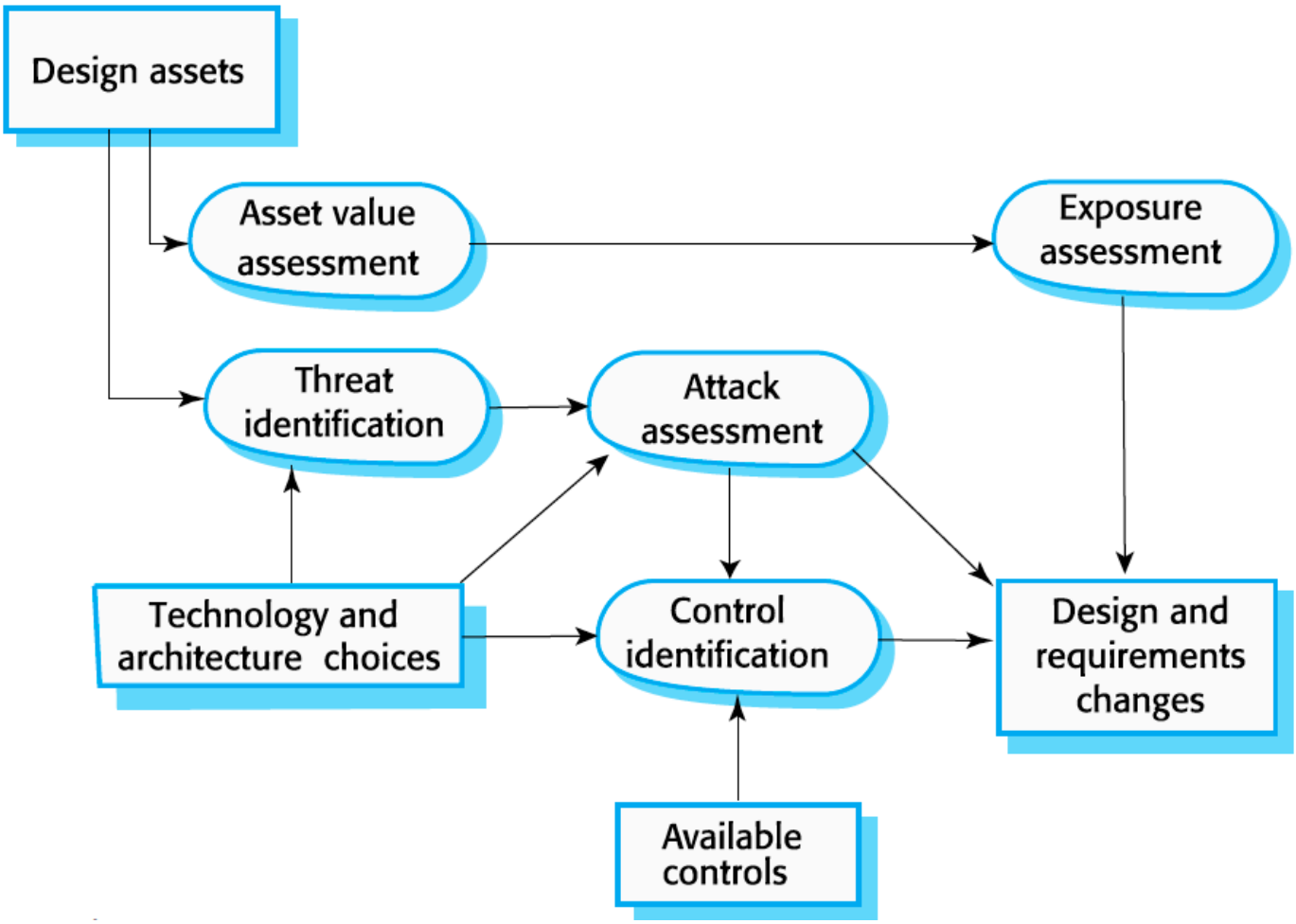
Design risk assessment

 Risk assessment while the system is being developed and after it has been deployed（研发时+部署后

 More information is available - system platform, middleware and the system architecture and data organisation.

 Vulnerabilities that arise from design choices may therefore be identified.（Vulnerabilities出现





Protection requirements

- Protection requirements may be generated when knowledge of information representation and system distribution
- Separating patient and treatment information limits the amount of information (personal patient data) that needs to be protected
- Maintaining copies of records on a local client protects against denial of service attacks on the server

 But these may need to be encrypted

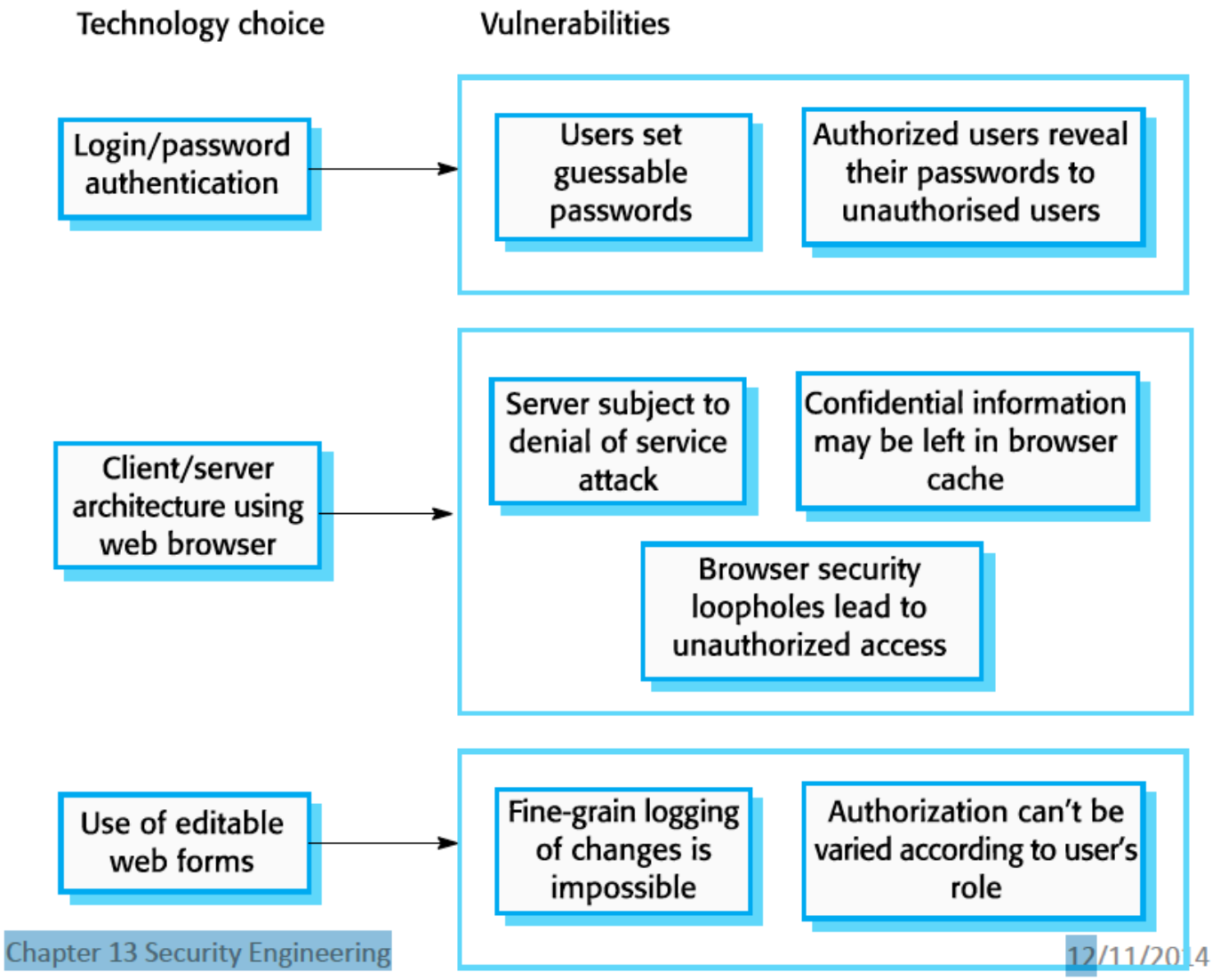
Design decisions from use of COTS

 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.

Vulnerabilities associated with technology



Security requirements

 A password checker shall be made available and shall be run daily. Weak passwords shall be reported to system administrators.

 Access to the system shall only be allowed by approved client computers.

 All client computers shall have a single, approved web browser installed by system administrators.

Architectural design

 Two fundamental issues have to be considered when designing an architecture for security.

  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 minimized?

 These are potentially conflicting

  If assets are distributed, then they are more expensive to protect. If assets are protected, then usability and performance requirements may be compromised.

Protection

 Platform-level protection

  Top-level controls on the platform on which a system runs.

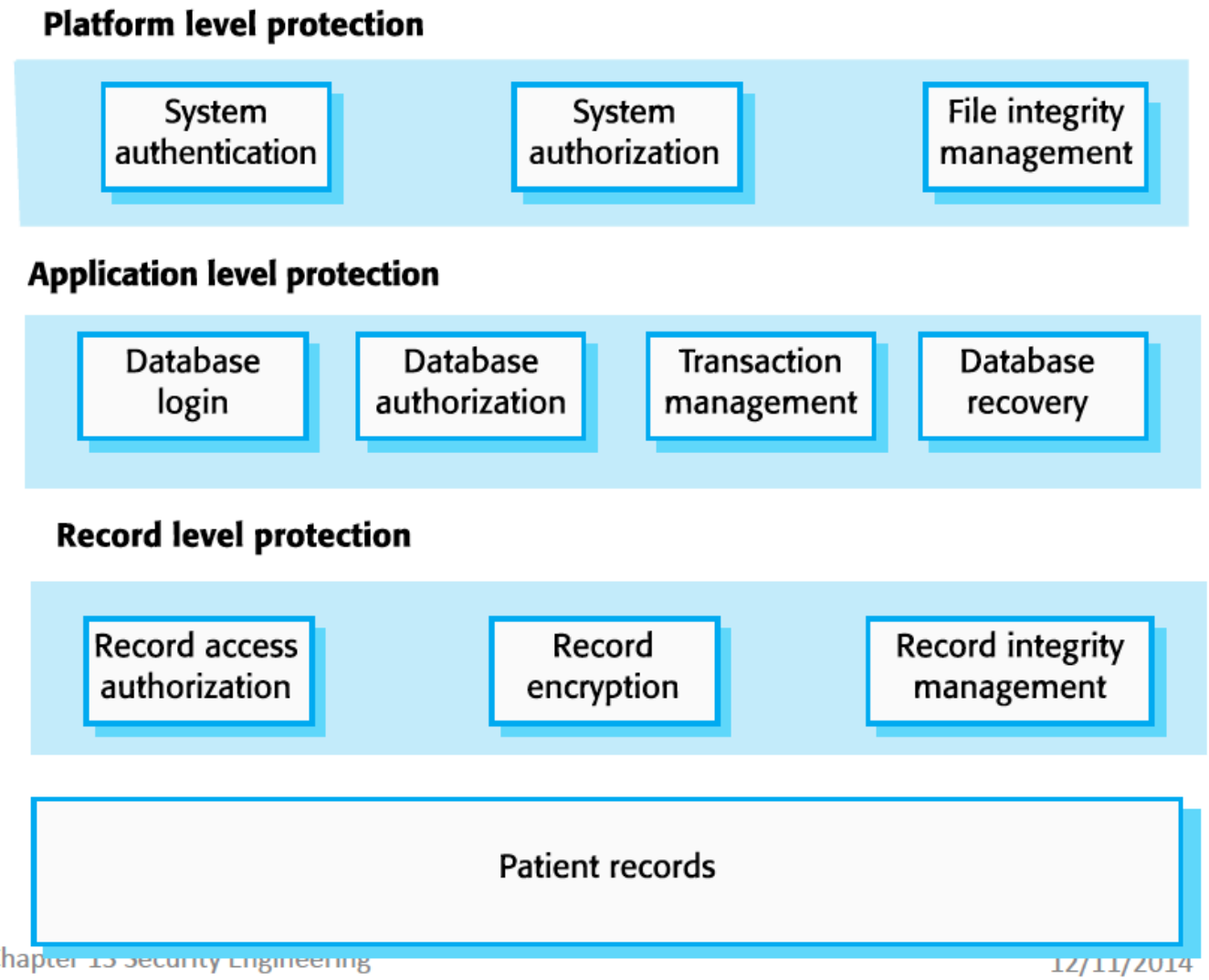
 Application-level protection

  Specific protection mechanisms built into the application itself e.g. additional password protection.

 Record-level protection

  Protection that is invoked when access to specific information is requested

 These lead to a layered protection architecture



Distribution

 Distributing assets means that attacks on one system do not necessarily lead to complete loss of system service

 Each platform has separate protection features and may be different from other platforms so that they do not share a common vulnerability

 Distribution is particularly important if the risk of denial of service attacks is high

Design guidelines for security engineering

 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. Security is considered when design decisions are made.

 They can be **used as the basis of a review checklist** that is applied during the system validation process.

 Design guidelines here are applicable during software specification and design

Design guidelines

Base decisions on an explicit security policy

Avoid a single point of failure

Fail securely

Balance security and usability

Log user actions

Use redundancy and diversity to reduce risk

Specify the format of all system inputs

Compartmentalize your assets

Design for deployment

Design for recoverability

Aspects of secure systems programming

Vulnerabilities are often **language-specific**

Security vulnerabilities are closely related to **program reliability**

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

 To **specify security requirements**, you should identify the assets that are to be protected and define how security techniques and technology should be used to protect these assets.

 Key issues when designing a secure systems architecture include **organizing the system structure to protect key assets** and **distributing the system assets to minimize the losses from a successful attack**.

 Security design guidelines sensitize system designers to security issues that they may not have considered. They provide a basis for creating security review checklists.(意识+checklist

 Security validation is difficult because security requirements state what should not happen in a system, rather than what should. Furthermore, system attackers are intelligent and may have more time to probe for weaknesses than is available for security testing.