PV222
Security Architectures

Lecture 6

Security Design Principles

& Case Studies

Security Design Principles Overview

- Introduce the different aspects of what makes up modern Information Security.
- The traditional CIA (confidentiality – integrity – availability) view of security.
- Introduce the notion of network security, and why it is necessary.
- Introduce the concept of security *services* and *mechanisms* – primarily in the scope of ISO 7498-2.
- Provide an overview of key design principles in computer security.

Information Security

- Security is about the protection of assets.
- Thus, **information security** is the basis for protecting our **information assets**.
- There are three broad classes of protection measures:
  - **Prevention**: prevent your assets from being damaged.
  - **Detection**: detect when you assets have been damaged, by whom and how.
  - **Reaction**: recover your assets, or recover from the damage to your assets.

Security

- How can our information assets be compromised?
- The most frequently used definition covers three aspects of information protection:
  - **Confidentiality**: prevention of unauthorised disclosure of information.
  - **Integrity**: prevention of unauthorised modification of information.
  - **Availability**: prevention of unauthorised withholding of information or resources.
- Commonly abbreviated to: **CIA**.

Security

- Other definitions for various protection properties of interest also exist.
- Some other common properties discussed in the literature:
  - **Accountability**: actions affecting security can be traced and attributed to the responsible party.
  - **Non-repudiation**: provision of *unforgeable evidence* that a specific action occurred.
  - Others: **Authentication**, **Authorisation**, …

Threats

- Security is only desirable when an organisation needs to protect its information from a threat.
- The associated threats which CIA are responsible for countering are:
  - **Exposure of data**: the threat that someone who is unauthorised can access the data.
  - **Tampering with data**: the threat that the data could be altered from what it should be.
  - **Denial of service**: the threat that the data or service is unavailable when it is required.

Adversaries

- People whose aim it is to circumvent your security are generally called **adversaries**.
  - They are sometimes called **intruders**, but not all adversaries are external to the system.
- Adversaries act in two different ways:
  - **Passive** adversaries only want to access information that they should not be allowed to see.
  - **Active** adversaries are more malicious, in that they want to: make changes to data; masquerade as a legitimate user; etc…

Adversaries

- When designing a system, it is important to consider the background and capability of your potential adversary.
- Here are some common category of adversary in the literature:
  - Casual prying by nontechnical users.
  - Snooping by insiders.
  - Determined attempts to make money.
  - Commercial or military espionage.

Network Security

Why Network Security?

- Organisations and individuals are increasingly reliant on networks of all kinds for day-to-day operations:
  - email used in preference to letter, fax, telephone for many routine communications
  - B2B and C2B e-commerce still growing rapidly
  - the Internet is a vast repository of information of all kinds: competitors and their prices, stock markets, cheap flights, …
  - increased reliance on networks for supply chains of all kinds: from supermarkets to aircraft components
  - utility companies control plant, banks move money, governments talk to citizens over networks
  - growth of mobile telephony for voice and data

Why Network Security?

- Networks are becoming increasingly inter-connected and their security consequently more complex:
  - if I send sensitive data over my internal network, then who else can see it or even alter it? My competitors?
  - can a hacker who gets into my internal network then get access to other resources (competitor accounts, stored data)? Can he use my network as a stopping-off point for further attacks? Am I then liable?
  - a compelling Internet presence is essential for my company, but if someone can see my website, can they alter it too?
  - how can consumers trust that a given website is that of a reputable company and not one who will mis-use their credit card details?

Why Network Security?

- Safeguarding the confidentiality, integrity and availability of data carried on these various networks is therefore essential.
- Authenticity and accountability are often also important: who did what and when?
- It's not *only* about security of Internet-connected systems.
  - Insider threats are often more potent than threats originating on the Internet
- It's not *only* about TCP/IP networks.
  - Many networks use special-purpose protocols and architectures.
  - However TCP/IP dominates in LANs and the Internet.

Security Policies for Networks

- In the remainder of this section, we follow the approach set out in ISO 7498-2:
  - a companion document to ISO7498-1 (the OSI seven layer model),
  - provides a useful overview of the security issues pertinent to networks,
  - equips us with a handy set of definitions to fix our terminology.

Security Policies for Networks

- In a secure system, the rules governing security behaviour should be made explicit in the form of an **Information Security Policy**.
- **Security policy**: "the set of criteria for the provision of security services"
  - essentially, a set of rules
  - may be very high level or quite detailed
- **Security domain**: the scope of application of a security policy
  - where, to what information and to whom the policy applies

The Security Life-Cycle

- A generic model for the **security life-cycle**, including network security issues, is as follows:
  - define security policy,
  - analyse security threats (according to policy) and associated risks, given existing safeguards,
  - define security services to meet/reduce threats, in order to bring down to acceptable levels,
  - define security mechanisms to provide services,
  - provide on-going management of security.

Security Threats for Networks

- A **threat** is:
  - a person, thing, event or idea which poses some danger to an asset (in terms of confidentiality, integrity, availability or legitimate use).
  - a possible means by which a security policy may be breached.
- An **attack** is a realisation of a threat.
- **Safeguards** are measures (e.g. controls, procedures) to protect against threats.
- **Vulnerabilities** are weaknesses in safeguards.

Risk

- **Risk** is a measure of the cost of a vulnerability (taking into account the probability of a successful attack).
- **Risk analysis** determines whether expenditure on new or better safeguards is warranted.
- Risk analysis can be **quantitative** or **qualitative**.

Threats

- Threats can be classified as:
  - **deliberate** (e.g. hacker penetration);
  - **accidental** (e.g. a sensitive file being sent to the wrong address).
- Deliberate threats can be further sub-divided:
  - **passive** (e.g. monitoring, wire-tapping);
  - **active** (e.g. changing the value of a financial transaction).
  - In general passive threats are easier to realise than active ones.

Fundamental Threats

- Four fundamental threats (matching four "standard" security goals: confidentiality, integrity, availability, legitimate use):
  - Information leakage,
  - Integrity violation,
  - Denial of service,
  - Illegitimate use.

Primary Enabling Threats

- Realisation of any of these primary enabling threats can lead directly to a realisation of a fundamental threat:
  - Masquerade,
  - Bypassing control,
  - Authorisation violation,
  - Trojan horse,
  - Trapdoor.
- First three are **penetration** threats, last two are **planting** threats.

Security Services and Mechanisms

- A security threat is a possible means by which a security policy may be breached (e.g. loss of integrity or confidentiality).
- A security **service** is a measure which can be put in place to address a threat (e.g. provision of confidentiality).
- A security **mechanism** is a means to provide a service (e.g. encryption, digital signature).

Security Service Classification

- Security services in ISO 7498-2 are a special class of safeguard to a communications environment.
- Five main categories of security service:
  - Authentication (including entity authentication and origin authentication),
  - Access control,
  - Data confidentiality,
  - Data integrity,
  - Non-repudiation.
- Sixth category: “other” – includes physical security, personnel security, computer security, life-cycle controls, …

Authentication

- **Entity authentication** provides checking of a claimed identity at a point in time.
  - Typically used at start of a connection.
  - Addresses masquerade and replay threats.
- **Origin authentication** provides verification of source of data.
  - Does not protect against replay or delay.
  - More examples later in the course…

Access Control

- Provides protection against unauthorised use of resource, including:
  - use of a communications resource,
  - reading, writing or deletion of an information resource,
  - execution of a processing resource.
- Example: file permissions in Unix/Windows 2000 file systems.

Data Confidentiality

- Protection against unauthorised disclosure of information.
- Four types:
  - Connection confidentiality,
  - Connectionless confidentiality,
  - Selective field confidentiality,
  - Traffic flow confidentiality.
- Example: encrypting routers as part of Swift funds transfer network.

Data Integrity

- Provides protection against active threats to the validity of data.
- Five types:
  - Connection integrity with recovery,
  - Connection integrity without recovery,
  - Selective field connection integrity,
  - Connectionless integrity,
  - Selective field connectionless integrity.

Non-repudiation

- Protects against a sender of data denying that data was sent (**non-repudiation of origin**).
- Protects against a receiver of data denying that data was received (**non-repudiation of delivery**).
- Example: analogous to signing a letter and sending via recorded delivery.

Security Mechanisms

- Exist to provide and support security services.
- Can be divided into two classes:
  - **Specific security mechanisms**, used to provide specific security services, and
  - **Pervasive security mechanisms**, not specific to particular services.

Specific Security Mechanisms

- Eight types:
  - encipherment,
  - digital signature,
  - access control mechanisms,
  - data integrity mechanisms,
  - authentication exchanges,
  - traffic padding,
  - routing control,
  - notarisation.

Specific Mechanisms 1

- Encipherment mechanisms = encryption algorithms.
  - Can provide data and traffic flow confidentiality.
- Digital signature mechanisms
  - Signing procedure (private),
  - Verification procedure (public).
  - Can provide non-repudiation, origin authentication and data integrity services.
- Both can be basis of some authentication exchange mechanisms.

Specific Mechanisms 2

- Access Control mechanisms
  - A server using client information to decide whether to grant access to resources
  - Covered earlier in this course.
- Data integrity mechanisms
  - Protection against modification of data.
    - Provide data integrity and origin authentication services. Also basis of some authentication exchange mechanisms.
- Authentication exchange mechanisms
  - Provide entity authentication service.
  - Covered in detail later on in this course.

Specific Mechanisms 3

- Traffic padding mechanisms
  - The addition of “pretend” data to conceal real volumes of data traffic.
  - Provides traffic flow confidentiality.
- Routing control mechanisms
  - Used to prevent sensitive data using insecure channels.
  - e.g. route might be chosen to use only physically secure network components.
- Notarisation mechanisms
  - Integrity, origin and/or destination of data can be guaranteed by using a 3rd party trusted notary.
    - Notary typically applies a cryptographic transformation to the data.

Pervasive Security Mechanisms

- Five types identified:
  - trusted functionality,
  - security labels,
  - event detection,
  - security audit trail,
  - security recovery.

Pervasive Mechanisms 1

- Trusted functionality
  - Any functionality providing or accessing security mechanisms should be trustworthy.
  - May involve combination of software and hardware.
- Security labels
  - Any resource (e.g. stored data, processing power, communications bandwidth) may have security label associated with it to indicate security sensitivity.
  - Similar labels may be associated with users. Labels may need to be securely bound to transferred data.

Pervasive Mechanisms 2

- Event detection
  - Includes detection of
    - attempted security violations,
    - legitimate security-related activity.
  - Can be used to trigger event reporting (alarms), even logging, automated recovery.
- Security audit trail
  - Log of past security-related events.
  - Permits detection and investigation of past security breaches.
- Security recovery
  - Includes mechanisms to handle requests to recover from security failures.
  - May include immediate abort operations, temporary invalidation of an entity, addition of entity to a blacklist.

Services v Mechanisms

- ISO 7498-2 indicates which mechanisms can be used to provide which services.
- Illustrative NOT definitive.
- Omissions include:
  - use of integrity mechanisms to help provide authentication services,
  - use of encipherment to help provide non-repudiation service (as part of notarisation).

Security Services and Layers

- ISO 7498-2 lays down which security services can be provided in which of the 7 layers.
- Layers 1 and 2 may only provide confidentiality services.
- Layers 3/4 may provide many services.
- Layer 7 may provide all services.
- A set of principles dictate which services can/should be provided at which layers.

Computer Security

Security Design Principles

- In 1974 **Jerome H. Saltzer** and **Michael D. Schroeder** published one of the seminal papers in computer security.
- The paper was titled: *“The Protection of Information in Computer Systems”*.
- It was responsible for collating and presenting some of the most fundamental design principles in computer security.
- Probably, the most famous of these was:
  - **The Principle of Least Privilege**
- We will now study the eight principles.

Economy of Mechanism

- The principle of **economy of mechanism**:
  - Keep the design as simple as possible.
  - A well-known principle which should ideally apply to every aspect of a system.
  - It deserves special emphasis here because:
    - *Design and implementation errors that result in unwanted access will not be noticed during normal use.*
    - This is because normal use will not include attempts to exercise improper access paths.
  - As a result, careful inspection and examination are needed.
  - For such techniques to be useful, a small and simple design is essential.

Fail-safe Defaults

- The principle of **fail-safe defaults**:
  - The default situation is a lack of access.
  - The protection mechanism identifies conditions under which access is permitted.
  - In a large system, some objects will be inadequately considered, so a default lack of permission is safer.
  - If the default is to allow access, then *any mistake will tend to fail by allowing access*. This is likely to go unnoticed in normal use.
  - If the default is to deny access, the *any mistake will result in an access request being denied*. This is more likely to be quickly detected.

Complete Mediation

- The principle of **complete mediation**:
  - **Every** access to **every** object **must** be checked.
  - This results in a system-wide view of access control.
  - This results in a fundamental requirement for identifying the source of every request.
  - Performance enhancements through remembering results (often known as *caching*) should be considered carefully – and skeptically.

Open Design

- The principle of **open design**:
  - The design should not be kept secret.
  - We should not depend on the ignorance of any potential attacker.
  - The protection should be limited to the possession of specific – hence more easily protected – keys or passwords.
  - This allows the mechanism to be analysed by many reviewers without compromising safeguards.
  - The analogue in cryptographic design is known as **Kerckoffs's principle**.

Separation of Privilege

- The principle of **separation of privilege**:
  - A protection mechanism that requires two keys to unlock it is more robust and flexible than one that allows access to the presenter of only a single key.
  - Once the mechanism is locked, the two keys can be separately managed, and distinct users, processes or organisations made responsible for them.
  - This principle is often used in *bank safe-deposit boxes*.
  - In a computer system the *separate keys* applies to any situation where two or more conditions must be met.

Least Privilege

- The principle of **least privilege**:
  - Each process or user should operate using the least set of privileges necessary to complete the job.
  - This principle limits the damage that can result from accident or error.
  - It reduces the number of potential interactions among privileged programs to a minimum.
  - Also, if a privilege is misused, then it reduces number of process which must be audited.
  - The military rule of "*need-to-know*" is an example of this principle.

Least Common Mechanism

- The principle of **least common mechanism**:
  - Minimize the mechanisms common to more than one user and depended on by all users.
  - Every shared mechanism represents a potential information path between users and must be designed with great care to ensure that it does not unintentionally compromise security.
  - Given the choice of:
    - (i) *implementing a new function as a supervisor procedure shared by all users*;
    - (ii) *a library procedure that can be handled as though it were a user's own*.
  - Choose the latter course.

Psychological Acceptability

- The principle of **psychological acceptability**:
  - It is essential that the human interface be designed for ease of use.
  - This ensures that the users regularly and routinely apply the correct protection mechanisms.
  - Also, this should extend to the user's mental image of their protection goals. This will minimise the number of potential mistakes.

Other Design Principles

- In their paper, Saltzer and Schroeder also discuss two design principles which can be translated from physical security systems.
  - **Work factor**
  - **Compromise recording**
- In their paper they discuss how these design principles only apply imperfectly in computer systems.
- However, more recent research rely on variants of these assumptions in the absence of a security proofs or guarantees.

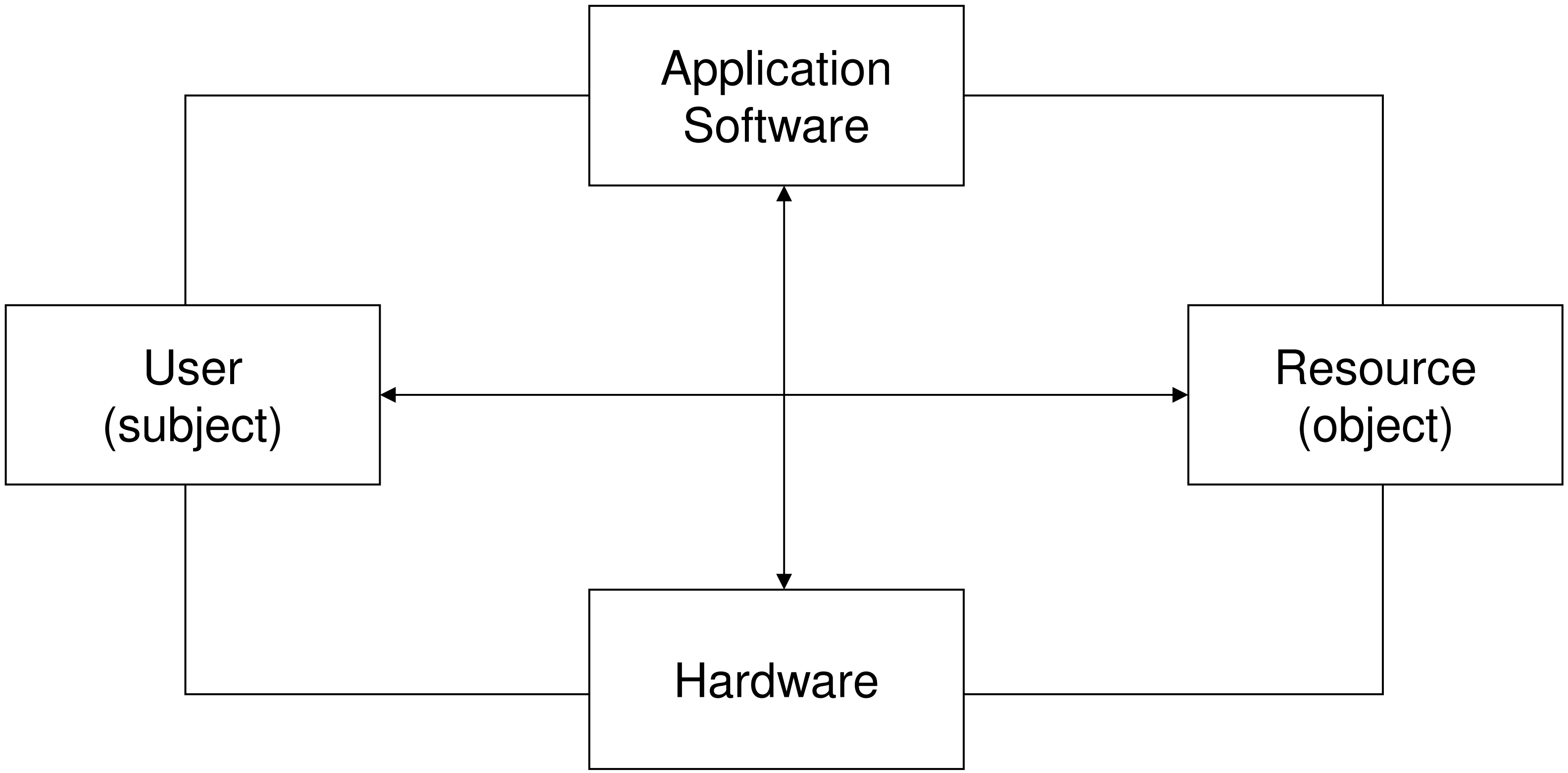
Work Factor

- **Work factor**:
  - Compare the cost of breaking the mechanism with the resources of the potential attacker.
  - The limit here is that calculating the work factor implies a direct attack (e.g. a brute-force search), whereas many attacks rely on an indirect attack.
  - Relying only on your calculation of the work factor can lead to an false sense of security.

Compromise Recording

- **Compromise Recording**:
  - Reliably record that a compromise has happened can be used in place of more elaborate mechanisms which completely prevent the loss.
  - For example, many computer systems record the date and time of most recent: login; use of a protected file; etc…
  - If this record is tamperproof and reported to the owner, it may help discover unauthorised use.
  - This idea has had a resurgence in information security with the advent of *tamper-proof* design. In this field, this is known as *tamper-evidence*.
  - Easier to implement in physical systems. Logical damage can be undone by a clever attacker.

Design Parameters for Computer Security



The Dimensions of Computer Security – Gollmann, "*Computer Security*" 2nd edition.

Design Decisions for Computer Security

- Gollmann introduces a number of design decisions which need to be evaluated when implementing a protection mechanism:
  1. In a given application, should the protection mechanisms in a computer system focus on: *data*; *operations*; or *users*?
  2. In which layer of the computer system should a security mechanism be placed?
  3. Do you prefer simplicity – and higher assurance – to a feature-rich security environment?
  4. Should the tasks of defining and enforcing security be given to a central entity or should they be left to individual components in the system?
  5. How do you prevent the attacker getting access to the layer below the protection mechanism?

Case Studies

Sample business requirements

Session Outline

Implementing a solution to some Identity Management Challenges – Options, Analysis and Recommendations

1. **Immigration Management**: for improving traveller identification at a Border Control.
2. **Energy Service Provision**: for introducing an on-line customer service.
3. **Employee Support**: for migrating resources from office environment to peripatetic based working.

Immigration Management – Options

- Adding additional controls on existing Passport or new electronic machine readable Travel Document
- Authentication of Issuing Authority of electronic credential:
  - Cryptography
  - Tokens
- Integrity of passport data and confidentiality of authentication/biographic data protection – asymmetric or symmetric cryptography
- Which biometric and how
  - Existing human interaction (face)
  - Automatic comparisons (fingerprint, face, and iris)
  - On board matching or with authorised equipment

Immigration Management – Analysis

- Which mechanism – User Authentication /Identity verification / biometric identification:
  - Authorised user does not prove identity
  - Knowledge is transferable (i.e. PINS and passwords)
  - Tokens are transferable (unless tied to identity verification)
  - Biometrics do not provide absolutes
  - Identity claimed using identity verification not biometric identification
- A heterogeneous environment
  - Federated Identity
  - PKI
  - Other examples (EMV)
- Enrolment Logistics
  - Local face-to-face
  - Remote processes

Immigration Management – Recommendations

- ICAO recommendations for improving traveller identification at a Border Control
  - ePassport (face, fingerprint and iris images) on embedded RFID “contactless chip” protected by access protocols (BAC and EAC)
  - Data and biometrics digitally signed by Issues Authority and inserted into RFID Integrated Circuit Card
  - ePassport may contain Document Signer Certificate
  - Country Signing CA Certificates circulated out-of-bounds
  - ICAO PKD Scheme distributing Certificates
  - RFID Readers work only with authorised EAC Inspection Systems
  - Inspection Systems use X.509 Certificates and Certificate Chaining
  - Protected X.509 Directories accessed using LDAP or OCSP

Energy Service Provision – Options

- User authentication, identity verification or biometric identification
- New mechanism or exploit existing id schemes
  - Federated Identity
  - Microsoft InfoCard
  - User ID and Password
  - Biometrics are not transferable
  - Soft tokens
- Enrolment Logistics
  - Remote
  - Local face-to-face
  - Identity biometric not required

Energy Service Provision – Analysis

- User Authentication
  - Knowledge is transferable
  - Tokens are transferable
  - Biometrics to not provide absolutes
  - Identity claimed for authenticated Users (Customer)
- Direct relationship
  - Federated Identity
  - PKI (SSL certificates)
  - Kerberos
- Recovery of authentication mechanism
  - Soft tokens
  - Knowledge previously acquired as part of enrolment process e.g. autobiographical data is well remembered (usually)

Energy Service Provision – Recommendations

- User authentication
- User ID assigned to existing Customer Account References
- Password assigned to each User ID
  - May be shared
  - May be changed
  - May be any length or value
  - Changes will not be forced
- Passwords automatically reminded to Users
  - Based upon successful authentication of recovery password
  - Successful send email to pre-arranged email address
  - Unsuccessful out-of-band process generate a letter to Customer

Employee Support – Options

- User authentication, identity verification or biometric identification
- Generic or bespoke mechanism?
- Intuitively usable mechanism or transparent biometric mechanism
- Static product or dynamic process biometrics?
- Enrolment
  - Local face-to-face
  - Remote

Employee Support – Analysis

- Transparent Biometric identification
  - Employee recognised automatically (known candidate)
  - Biometrics do not provide absolutes
  - Augment or replace other mechanism
- Direct Authenticated Relationship
  - PKI (SSL)
  - Kerberos
- Recover
  - Failure to Enrol
  - Failure to Acquire
  - Type 1 Errors (False Rejection Rate)
  - Type 2 Errors (False Acceptance Rate)
  - Setting the match threshold

Employee Support – Recommendations

- Keystroke Dynamics employee identification on secret phrase
- User Authentication of secret phrase used for recovery purposes
- Enrolment prior to laptop release
  - Secret phrase learnt by individual
  - Secret phrase learnt by machine
- Threshold set to assist user convenience
  - Fewer False Rejects
  - More False Accepts
  - Re-assess in a year to evaluate against risks and operational experience
- SSL for mutual authentication

Acknowledgements

- Information on the definitions of information security partly derived from:
  - Chapters 1 and 2 of D. Gollmann, "*Computer Security*", 2nd edition.
- Information on 7498-2 derived from original lecture notes by Kenny Paterson.
- Information on design principles taken from:
  - J.H. Saltzer and M.D. Schroeder, "*The Protection of Information in Computer Systems*", Communications of the ACM, v.17 n.7, July 1974.
- Information on the design decisions for computer security taken from:
  - Chapter 2 of D. Gollmann, "*Computer Security*", 2nd edition.