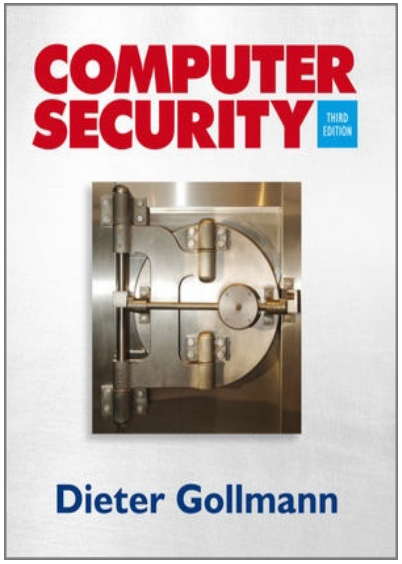
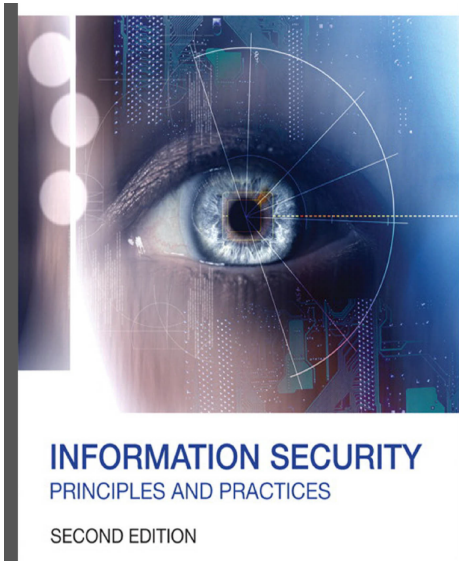
502049 – Introduction to Information Security

Ngoc Tu Huynh, PhD

huynhngoctu@tdtu.edu.vn

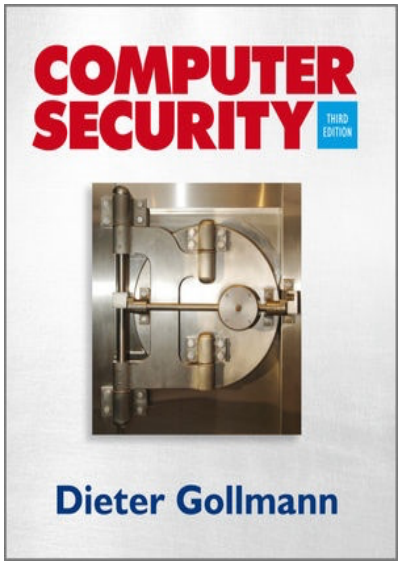


Textbook

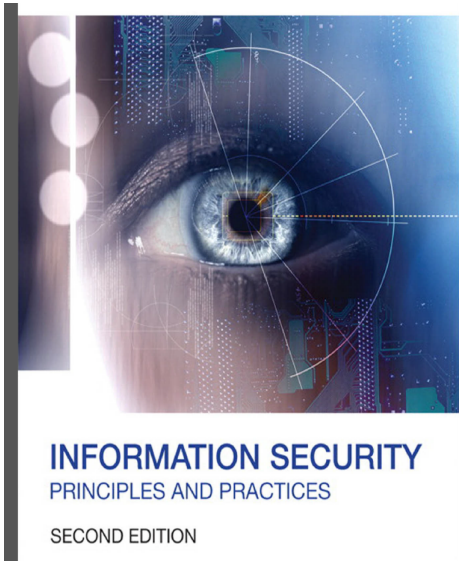


Further readings

Chapter 1: Security management concepts and principles



Chapter 2:
Managing Security



Chapter 2:
Information Security
Principles of Success

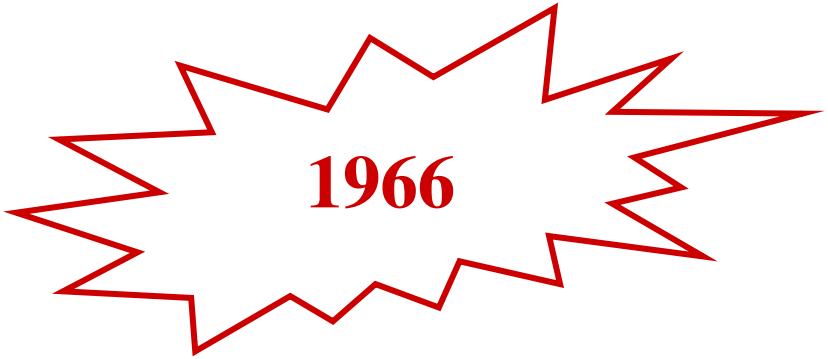
Agenda

- Security: case studies
- Security management
  - Security policies
  - Security metrics
  - Management standards
- Risk & Threat Analysis
  - Vulnerabilities
  - Threats
  - Risk
  - Baseline protection
- Security Principle

Security: case studies

Insider Fraud

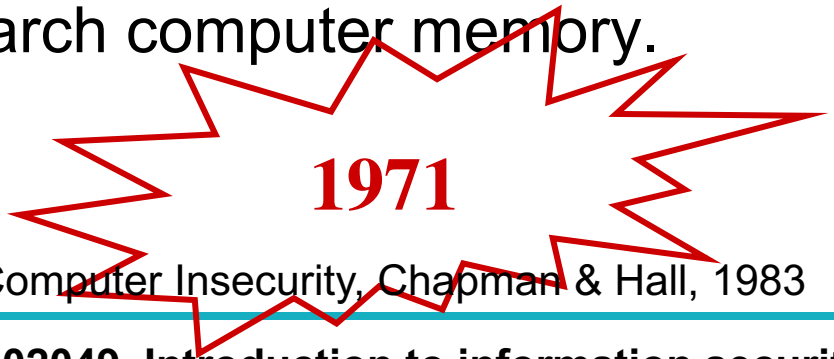
- Programmer writing code for a bank made the program ignore overdrafts on his account.
- Discovered when the computer broke down and accounts were processed manually.
- Suspended sentence (money repaid).
- Fired, but re-hired as contractor.



From: A.R.D. Norman: Computer Insecurity, Chapman & Hall, 1983

Espionage – Identity Fraud

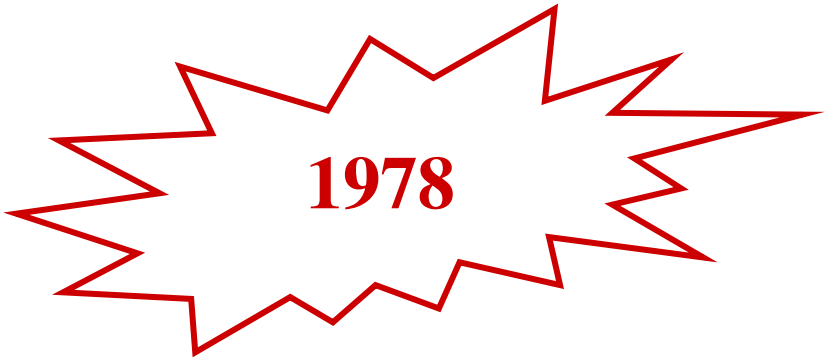
- Setting: competitors A and B with a common customer C; communication by phone to secret (unlisted) phone numbers.
- Employee of A finds out about the secret number C uses to call B (displayed over a terminal).
- Uses this number to ring B pretending to be C.
- Searches the filesystem, requests code to be sent to his terminal and punched cards to be sent.
- Discovered when B asks C about the cards and C knows nothing about it.
- Believed to be the first case where a warrant was used to search computer memory.



From: A.R.D. Norman: Computer Insecurity, Chapman & Hall, 1983

Password Sniffing

- Student wrote program for time-sharing system and left it on disk for curious users.
- On execution the program would “crash” and then ask for username and password.
- Username and password were collected and later used to delete the victims’ files.



From: A.R.D. Norman: Computer Insecurity, Chapman & Hall, 1983

Denial of Service

- MyDoom worm
  - CERT Incident Note IN-2004-01
  - Spread over email and Kazaa p2p network
  - Email: users had to click on an attachment to activate the worm: MyDoom was so successful because the attachment looked like a genuine error message
  - Distributed Denial-of-Service attack on www.sco.com
  - Trigger date to stop spreading/DoS-attacking on February 12, 2004

Spam

- Unsolicited email, but when does email become spam?
  - Have you read about the Nigerian astronaut stranded in space?
- A major nuisance, but unsolicited mass mailings are not a new problem.
- Addressed through legislation: in Europe based on EC Directive 2002/58/EC, increasingly also in US.
- Technical measures: spam filters, visual puzzles ("catchpas"), etc.

Telecomm Fraud

- First generation cell phones: user identifiers transmitted unprotected; easy to intercept and used to make calls charged to the victim.
- PABX (private automatic branch exchange) fraud: route calls via an unprotected company PABX; calls charged to the victim.
- SMS fraud: SMS message asks receiver to call back a number that is automatically re-directed to an expensive 900 number.

Newsticker (2008)

- RBS WorldPay belatedly admitted last week that hackers broke into its systems.
- The attack against the electronic payment services firm leaves to to 1.5 million payroll and gift card holders in the US at risk of fraud. Up to 1.1 million social security records were also exposed as a result of the breach.
- …
- The attack has been linked to the fraudulent misuse of 100 payroll cards, all of which have since been deactivated.
- Details of the attack itself, much less who might have pulled it off, remain sketchy. RBS WorldPay has pledged to improve its security defences to prevent similar attacks in future.

http://www.theregister.co.uk/2008/12/29/rbs_worldpay_breach/

The long arm of the law (2010)

- Russian authorities have arrested the alleged mastermind behind the 2008 cyber-attack on RBS WorldPay's computer network, which lead to the theft of over $9 million, according to the Financial Times.
- Viktor Pleshchuk, who was one of eight suspects from Eastern Europe named in a US federal grand jury indictment last year, has been detained by the the Russian Federal Security Service (FSB), along with "several" other people, says the paper.
- US authorities believe Pleshchuk and Estonian Sergei Tsurikov were the ringleaders behind the attack, which compromised the encryption used by the processor to protect customer data on payroll debit cards.
- This allowed the gang to raise the limits on accounts before handing over 44 counterfeit payroll debit cards to a network of "cashers" who withdrew over $9 million in less than 12 hours from more than 2100 ATMs in at least 280 cities worldwide, including in the US, Russia, Ukraine, Estonia, Italy, Hong Kong, Japan and Canada.

http://www.finextra.com/news/fullstory.aspx?newsitemid=21211

Security

- All cases of “security” problems.
- Security covers a wide range of issues; our list of attacks is by no means exhaustive.
- When thinking about security, start from the application, not from the technology.
- Attacks may exploit weak points of the “business model” rather than technical flaws.
- Security problems can rarely be eliminated, but they can be managed.

Security

- Systems may fail for various reasons.
- Reliability deals with accidental failures.
- Usability addresses problems arising from operating mistakes made by users.
- Security deals with intentional failures: there is at some stage a decision by a person do something he is not supposed to do.
- Reasons: crime, malice, curiosity, stupidity, …

Security is a People Problem

- You are on this course because people don't behave the way we wish they would.
- Security problems are here to stay.
- Technical solutions can only address a part of the problem.
- Technical measures have to be managed in a wider security culture.
- The legal system has to define the boundaries of acceptable behaviour.
- Social engineering is a powerful attack method.

Security Management

Security Management

- Protection of the assets of an organisation is the responsibility of management.
- However, security measures may restrict people in their working patterns, so there may be a temptation to flaunt security rules.
- This is particularly likely if security instructions do not come from a superior authority but from some other branch of the organisation.

Security Awareness

- To be effective, security policies must be supported by top management: issue a security charter.
  - A crisp document explaining general rules.
- Don't treat users as the enemy: users have to understand that they protect their own assets.
- Security awareness programs should be part of the general security strategy.
- Not every member in an organisation has to become a security expert, but all members should know:
  - Why security is important for themselves and for the organisation.
  - What is expected of each member.
  - Which good practices they should follow.

The Price of Security

- Price paid for security should not exceed the value of the assets you want to protect.
- To decide what to protect you should perform some kind of risk analysis.
- You have to know your assets.
- You have to understand how your assets might be damaged.
- Total cost of security measures goes beyond the cost of “security technology” (e.g. firewalls or intrusion detection systems).

Assets

- Hardware: laptops, servers, routers, PDAs, mobile phones, smart cards, …
- Software: applications, operating systems, database systems, source code, object code, …
- Data & information: essential data for running and planning your business, design plans, digital content, data about customers, …
- Services & revenue
- Reputation of enterprise, trust, brand name
- Employees' time

Damage

- Disclosure of information, espionage
- Modification of data
- Being unable to do your job because required resources are not available
- Identity spoofing (identity “theft”)
- Unauthorised access to services
- Lost revenue
- Damaged reputation
- Theft of equipment
- …

Security policies

- Question: Is this system secure?
- Answer: Wrong question; please be more specific about your protection requirements.
  - Protect PC from virus and worm attacks?
  - No unauthorized access to corporate LAN?
  - Keep sensitive documents secret?
  - Verify identity of partners in a business transaction?
- Security policies formulate security objectives.

Types of Policies [Sterne]

- Organisational security policy: laws, rules, and practices that regulate how an organisation manages and protects resources to achieve its security policy objectives.
  - Organisations must comply with given regulations
- Automated security policy: restrictions and properties that specify how a computing system prevents violations of the organisational security policy.
  - A detailed technical specification

Security Metrics

- It would be very useful if we could measure security to convince managers or customers of the benefits of a new security mechanism,
- First step: obtain values for security relevant factors.
  - In SANS terminology this is a security measurement.
  - Some values can be established objectively, other values are subjective.
- Second step: consolidate measurements into a single value that is used for comparing the current security state against a baseline or a past state.
  - In SANS terminology, the values given to management for making security comparisons are called security metrics.

Security Metrics

- Ideally, a security metric gives a quantitative result, not just a qualitative statement about the security of a product or system.
  - Product: a package of software, firmware and/or hardware, designed for use within a multiplicity of systems.
  - System: a specific IT installation, with a particular purpose and operational environment.
- Security metrics for a product: number of security flaws (bugs) detected, or the attack surface, i.e. the number of interfaces to outside callers or the number of dangerous instructions in the code.
- These measurements deliver quantitative results but do they really measure security?
- Secure products can be deployed in insecure ways!

Security Metrics

- Security metrics for a system: check configurations of the products deployed; may be valuable status information but does not give quantitative results.
- Alternatively measure the cost of mounting attacks:
  - Time an attacker has to invest in the attack.
  - Expenses the attacker has to incur.
  - Knowledge necessary to conduct the attack.
- The cost of discovering an attack is often much larger than the cost for mounting the attack; when attack scripts are available, launching attacks can be easy.
- Another alternative: focus on the assets in the system and measure the risks these assets are exposed to.

Management Standards

- Prescriptive security management standards that stipulate which security measures have to be taken in an organisation exist for specific industry branches.
- Typical examples are regulations for the financial sector, or rules for dealing with classified material in government departments.
- Other management standards are best described as codes of best practice for security management.
- The most prominent of these standards is ISO 27002.
- This is not a technical standard for security products or a set of evaluation criteria for products or systems.

Regulations

- Personal data
  - OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data
  - EU Data Protection Directive
  - EU Directive on privacy and electronic communications
  - California SB1386
- Health
  - HIPAA (US)
  - FDA regulations for pharmaceutical companies
- Financial sector
  - Rules for banks, insurances, stock exchanges, …
  - Sarbanes-Oxley Act of 2002 on Accounting Information Systems (“SOX”)
- and more …

ISO 27002

1. Risk assessment and treatment
2. Information security policy
   - We have just covered this point
3. Organization of information security
4. Asset management
5. Human resources security
6. Physical and environmental security
7. Communications and operations management
8. Access control
9. Information systems acquisition, development and maintenance
10. Information security incident management
11. Business continuity management
12. Compliance

http://www.iso27001security.com/html/27002.html

Organization of Information Security

- Responsibilities for security within an enterprise have to be properly organized.
- Qualifications of chief security officer?
  - Formerly: Ex-police, ex-military
  - Today: Increasingly lawyers, IT experts
- Management has to get an accurate view of the state of security within an enterprise.
- Reporting structures to facilitate efficient communication and implementation of security decisions.
- Security has to be maintained when outsourcing services to third parties.

Asset Management

- To know what is worth protecting, and how much to spend on protection, an enterprise has to have a clear picture of its assets and of their value.

Human Resources Security

- Your own personnel or contract personnel can be a source of insecurity.
- Have procedures for new employees joining and for employees leaving (e.g., collect keys and entry badges, delete user accounts of leaving members.)
- Enforced holiday periods can stop staff hiding the traces of fraud they are committing.
- Background checks on new hires can be a good idea.
  - In some sectors such checks may be required by law.
  - But there may also be privacy laws that restrict which information an employer may seek about its employees.

Physical and Environmental Security

- Physical security measures (fences, locked doors, …) protect access to sensitive areas in a building.
  - E.g., only authorized personnel has access to server rooms.
  - Can prevent unauthorized access to sensitive information and theft of equipment.
- Logistics security: protection of goods shipped to retailers, or between manufacturing sites.
- Event security: no radio microphones in sensitive meetings; checking entry to meeting room, where can visitors go on your premises?
- Environmental factors can influence the likelihood of natural disasters.
  - E.g., is the area subject to flooding?

Communications and Operations Management

- Day-to-day management of IT systems and of business processes has to ensure that security is maintained.

Access Control

- Access control can apply to data, services, and computers.
- Particular attention should be applied to remote access, e.g. through Internet or dial-in connections.
- Automated security policies define how access control is being enforced.

Systems Acquisition, Development and Maintenance

- Security issues should be considered when an IT system is being developed.
- Operational security depends on proper maintenance (e.g., patching vulnerable code, updating virus scanners).
- IT support has to be conducted securely (how do you deal with users who have forgotten their password?)
- IT projects have to be managed with security in mind. (Who is writing sensitive applications, who gets access to sensitive data?)

Incident Management

- It is important to know what to do when a security incident happens or seems to happen.
- Known & documented processes in the organisation.
  - "Return on experience"?
- Legal aspects:
  - Are there statutory requirements for reporting the incident? To an authority? To your customers?
  - How to collect evidence if a case should be taken to court → computer forensics.
- Technical aspects: Tools, etc.
- Further resources: IT Infrastructure Library (ITIL)

Business Continuity Planning

- Put measures in place so that your business can cope with major failures or disasters.
- Measures start with keeping backups of important data kept in a different building and may go on to the provision of reserve computing facilities in a remote location.
- You have to account for losing key staff members.

Compliance

- Organisations have to comply with legal, regulatory, and contractual obligations, as well as with standards and their own organisational security policy.
- Auditing process should be put to efficient use while trying to minimize its interference with business processes.
- In practice, compliance often poses a greater challenge than fielding technical security measures.

ISO 27002 – Summary

- Achieving compliance with ISO 27002 can itself be quite an onerous task.
- Current state of your organisation vis-à-vis the standard has to be established; any shortcomings identified must be addressed.
- Software tools that partially automate this process exist, helping to apply best practice.
- Compliance ≠ Security

ĐẠI HỌC TÔN ĐỨC THẮNG
TON DUC THANG UNIVERSITY

Risk Analysis

Risk Analysis

- Many areas of engineering and business have developed their own disciplines and terminology for risk analysis.
- We will give a brief overview of risk analysis for IT security.
- Within IT security, risk analysis is being applied
  - comprehensively for all information assets of an enterprise,
  - specifically for the IT infrastructure of an enterprise,
  - during the development of new products or systems, e.g. in software security.
- Informally, risk is the possibility that some incident or attack can cause damage to your enterprise.

Attacks

- An attack against an IT system is a sequence of actions, exploiting weak points in the system until the attacker's goals have been achieved.
- To assess the risk posed by an attack we have to evaluate the amount of damage being done and the likelihood for the attack to occur.
- This likelihood will depend on the attacker's motivation and on how easy it is to mount the attack.
- In turn, this will further depend on the security configuration of the system under attack.

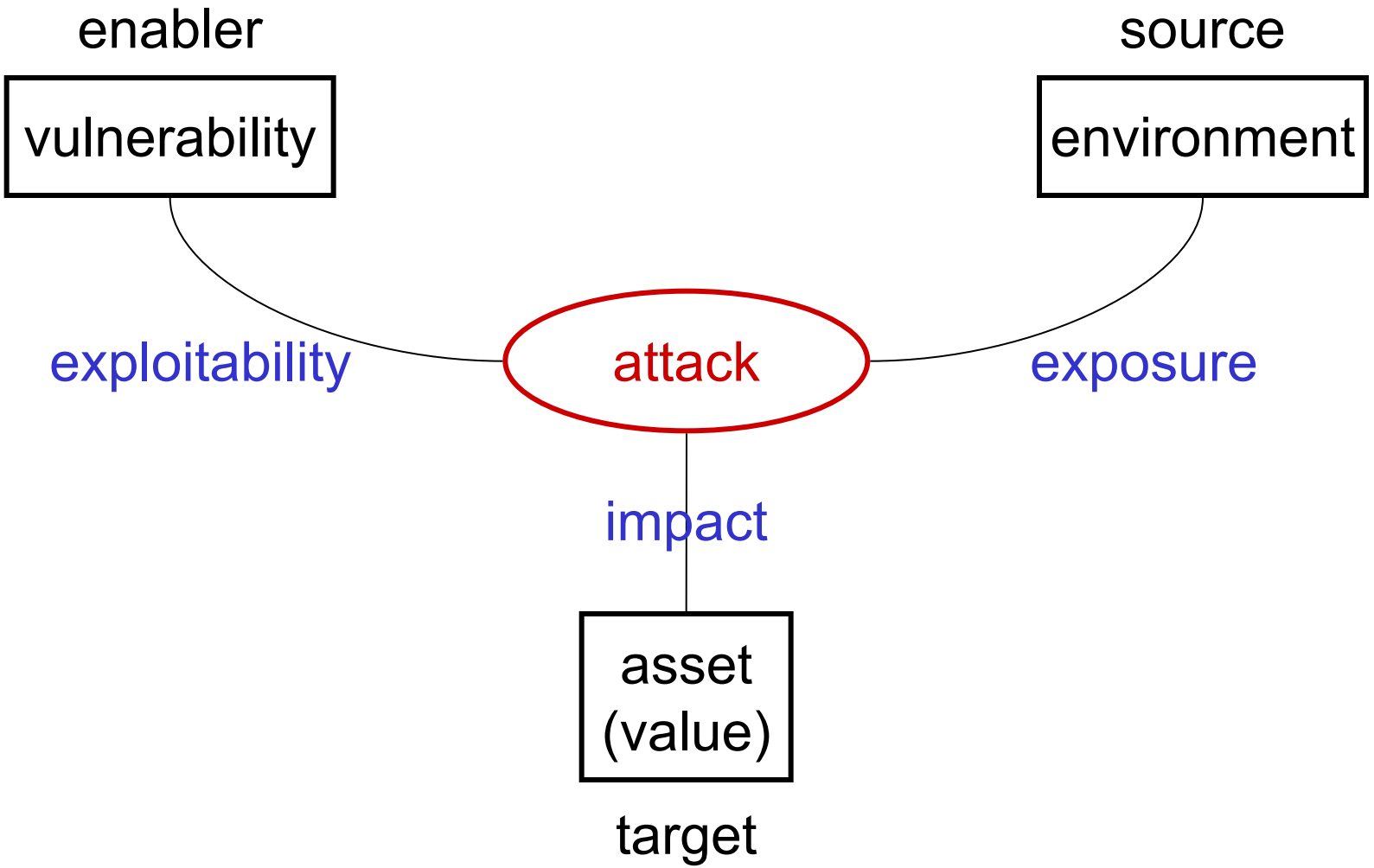
Risk Analysis

- To organize the process of risk analysis, we will look at assets, vulnerabilities, and threats.
- Risk is a function of assets, vulnerabilities, and threats:

$$\text{Risk} = \text{Assets} \times \text{Threats} \times \text{Vulnerabilities}$$

- During risk analysis values are assigned to assets, vulnerabilities, and threats.

Factors in Risk Analysis



Quantitative or Qualitative?

- Quantitative risk analysis: values are taken from a mathematical domain like a probability space.
  - For example, we could assign monetary values to assets and probabilities to threats and then calculate the expected loss.
- Qualitative risk analysis: values taken from domains that don't have an underlying mathematical structure.
  - Risk calculated based on rules that capture the consolidated advice of security experts.

Assets (repeat)

- First, assets have to be identified and valued; this step should be relatively easy.
- In an IT system, assets include:
  - Hardware: laptops, servers, routers, PDAs, mobile phones, smart cards, …
  - Software: applications, operating systems, database systems, source code, object code, …
  - Data & information: essential data for running and planning your business, design plans, digital content, data about customers, …
  - Services & revenue
  - Reputation of enterprise, trust, brand name
  - Employees' time

Valuation of Assets

- Assets such as hardware can be valued according to their monetary replacement costs.
- For other assets such as data & information this is more difficult.
  - If your business plans are leaked to the competition or private data about your customers is leaked to the public there are indirect losses due to lost business opportunities.
  - For lost or stolen equipment you have to consider the value of the data stored on it, and the value of the services that were running on it.
- Value assets according to their importance.
- As a good metric for importance, ask yourself how long your business could survive when a given asset has been damaged: a day, a week, a month?

Vulnerabilities

- Weaknesses of a system that could be accidentally or intentionally exploited to damage assets.
- Typical vulnerabilities in an IT system are:
  - Accounts with system privileges where the default password, such as “MANAGER”, has not been changed.
  - Programs with unnecessary privileges or known flaws.
  - Weak access control settings on resources, e.g. having kernel memory world writable.
  - Weak firewall configurations that allow access to vulnerable services.
- Sources for vulnerability updates: CERTs (Computer Emergency Response Teams), SANS, BugTraq, …

Rating Vulnerabilities

- Rate vulnerabilities according to their impact (level of criticality):
  - A vulnerability that allows an attacker to take over a systems account is more critical than a vulnerability that gives access to an unprivileged user account.
  - A vulnerability that allows an attacker to completely impersonate a user is more critical than a vulnerability where the user can only be impersonated in a single specific service.
- Vulnerability scanners provide a systematic and automated way of identifying vulnerabilities.
- Some vulnerability scanners also give a rating for the vulnerabilities they detect.

Microsoft Severity Rating System

- Critical: Exploitation could allow propagation of an Internet worm without user action.
- Important: Exploitation could result in compromise of the confidentiality, integrity, or availability of users data, or of the integrity or availability of processing resources.
- Moderate: Exploitability mitigated to a significant degree, e.g. by default configuration or by auditing.
- Low: Exploitation extremely difficult, or impact is minimal.

Common Vulnerability Scoring Scheme

Basic metrics		Temporal metrics	Environmental metrics	
Access vector	Confidentiality impact	exploitability	Collateral damage potential	Confidentiality requirement
Access complexity	Integrity impact	Remediation level	Target distribution	Integrity requirement
Authenti-cation	Availability impact	Report confidence		Availability requirement

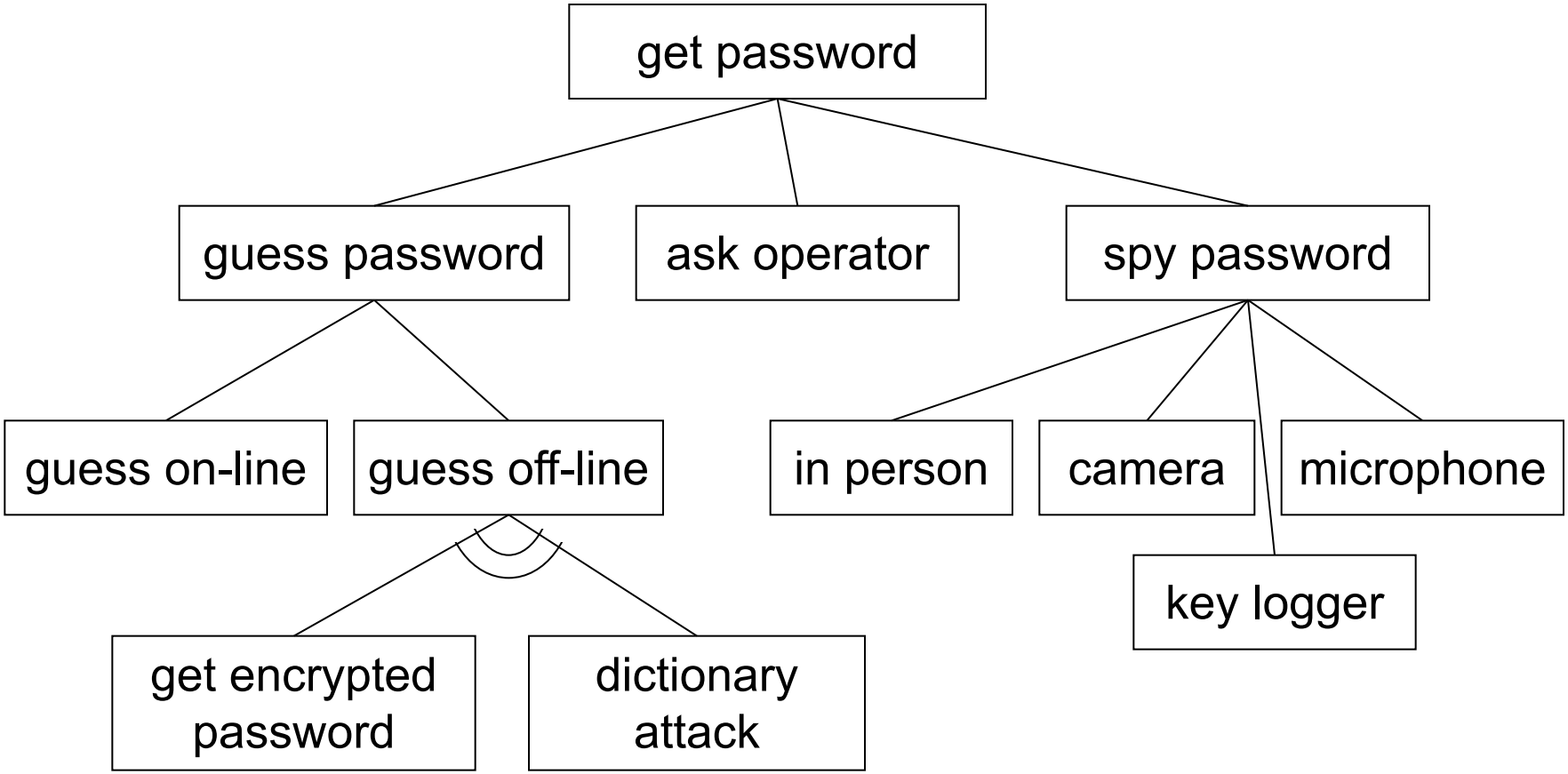
Threats

- Threats: actions by adversaries who try to exploit vulnerabilities to damage assets.
- Various ways for identifying threats:
  - Categorize threats by the damage done to assets.
  - Identify source of attacks. Would the adversary be a member of your organisation or an outsider, a contractor or a former member? Has the adversary direct access to your systems or is the attack launched remotely?

Attack Trees

- We can analyze how an attack is executed in detail.
- An attack may start with innocuous steps, gathering information needed to move on to gain privileges on one machine, from there jump to another machine, until the final target is reached.
- To get a fuller picture of potential threats, attack trees can be constructed.

Attack Tree – example



Rating Threats

- Rate threats according to their likelihood.
- The likelihood of a threat depends on
  - difficulty of the attack,
  - motivation of the attacker,
  - number of potential attackers.
- Attack scripts automate attacks; they are likely to be available to a larger set of attackers.
- Hence, such attacks would be rated more likely than an individual hand-crafted attack.

Calculating Risk

- In quantitative risk analysis, expected losses can be computed based on monetary values for the assets and probabilities for the likelihood of threats.
  - Advantage: uses a well established mathematical theory ($\rightarrow$ probability theory)
  - Drawback: the ratings obtained are often quite imprecise and based on educated guesses.
  - The quality of the results we obtain cannot be better than the quality of the inputs provided.
- Quantitative risk analysis works in some areas.
- More often we can only obtain ratings where there is no justification to have these inputs processed by an established mathematical calculus.

Calculating Risk

- In qualitative risk analysis, rate
  - assets on a scale of *critical – very important – important – not important*.
  - vulnerabilities on a scale of *has to be fixed immediately – has to be fixed soon – should be fixed – fix if convenient*.
  - threats on a scale of *very likely – likely – unlikely – very unlikely*.
- For a finer granularity of scaling you could e.g. use numerical values from 1 to 10.
- Guidance must be given on how to assign ratings.
- The mapping of the ratings for assets, vulnerabilities, and threats to risks is often given by a table that reflects the judgement of security experts.

The MEHARI Approach

	n=1	n=2	n=3	n=4
i=4	2	2	3	4
i=3	1	2	2	3
i=2	1	1	2	2
i=1	1	1	1	2

damage potential as function of impact and number of targets

	f=1	f=2	f=3	f=4
e=4	1	2	2	3
e=3	1	1	2	3
e=2	1	1	2	2
e=1	1	1	1	2

likelihood as function of exploitability and feeling of impunity

	l=1	l=2	l=3	l=4
d=4	2	3	4	4
d=3	2	2	3	3
d=2	1	2	2	3
d=1	1	1	1	2

risk as function of likelihood and damage potential

Risk Mitigation

- Risk analysis produces a prioritized list of threats, with recommended countermeasures to mitigate risk.
- Analysis tools usually have a knowledge base of countermeasures for the threats they can identify.
- General risk mitigation strategies:
  - Accept risk (and live with it); there may be good reasons to do so.
  - Avoid risk: eliminate a vulnerability that causes the risk; drop product feature that has a vulnerability.
  - Limit risk: use controls to make a threat less likely.
  - Transfer risk: buy insurance.

Baseline Protection

- It may seem obvious that one should do a risk analysis before deciding on which security measures to implement.
- This ideal approach may not work for two reasons:
  - Conducting a risk analysis for a large organisation takes time, but its IT systems and the world around will keep changing; when the analysis is ready, it is already out of date.
  - Costs of a full risk analysis may be difficult to justify to management.
- Organisations may opt for baseline protection as an alternative; this approach analyzes the security requirements for typical cases and recommends security measures deemed adequate.
  - BSI Baseline Protection Manual

ĐẠI HỌC TÔN ĐỨC THẮNG
TON DUC THANG UNIVERSITY

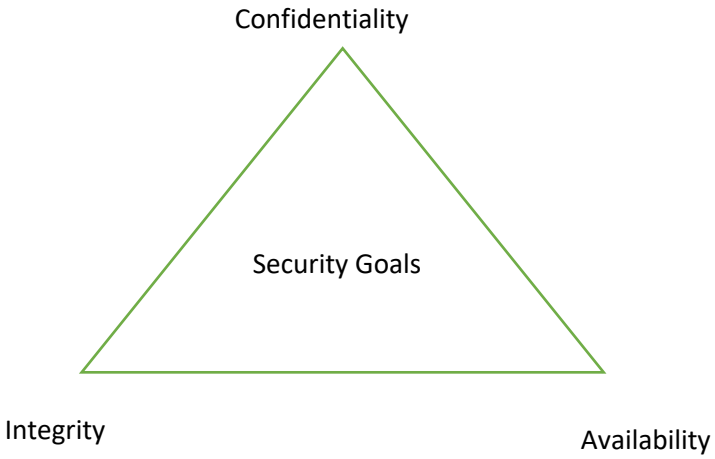
Information Security Principles

Principle 1:There Is No Such Thing as Absolute Security

- Given enough time, tools, skills, and inclination, a hacker can break through any security measure
- Security testing can buy additional time so the attackers are caught in the act

Principle 2: The Three Security Goals Are Confidentiality, Integrity, and Availability

- All information security measures try to address at least one of the three goals:
  - Confidentiality
  - Integrity
  - Availability
- The three security goals form the CIA triad



Principle 2: The Three Security Goals Are Confidentiality, Integrity, and Availability (cont.)

- Protect the *confidentiality* of data
  - Confidentiality models are primarily intended to ensure that no unauthorized access to information is permitted and that accidental disclosure of sensitive information is not possible
- Preserve the *integrity* of data
  - Integrity models keep data pure and trustworthy by protecting system data from intentional and accidental changes
- Promote the *availability* of data for authorized use
  - Availability models keep data and resources available for authorized use during denial-of-service attacks, natural disasters, and equipment failures

Principles 3: Defense in Depth as Strategy

- Defense in depth
  - Involves implemented security in overlapping layers that provide the three elements needed to secure assets: prevention, detection, and response
  - The weaknesses of one security layer are offset by the strengths of two or more layers

Principle 4: When Left on Their Own, People Tend to Make the Worst Security Decisions

- Takes little to convince someone to give up their credentials in exchange for trivial or worthless goods
- Many people are easily convinced to double-click the attachment or links inside emails

Principle 5: Computer Security Depends on Two Types of Requirements: Functional and Assurance

- Functional requirements
  - Describe what a system should do
- Assurance requirements
  - Describe how functional requirements should be implemented and tested

Does the system do the right things in the right way?

- ***Verification**: The process of confirming that one or more predetermined requirements or specifications are met*
- ***Validation**: A determination of the correctness or quality of the mechanisms used in meeting the needs*

Principle 6: Security Through Obscurity Is Not an Answer

- Many people believe that if hackers don't know how software is secured, security is better
  - Although this seems logical, it's actually **untrue**
- Obscuring security leads to a false sense of security, which is often more dangerous than not addressing security at all

Principle 7: Security = Risk Management

- Security is not concerned with eliminating all threats within a system or facility but with **eliminating known threats and minimizing losses** if an attacker succeeds in exploiting a vulnerability
- Spending more on security than the cost of an asset is a waste of resources
- Risk assessment and risk analysis are used to **place an economic value on assets to best determine appropriate countermeasures** that protect them from losses

Principle 7: Security = Risk Management (cont.)

- Two factors to determine risk
  - What is the consequence of a loss?
  - What is the likelihood the loss will occur?
- Consequences/likelihood matrix

Likelihood	Consequences
A (almost certain)	
B (likely)	
C (moderate)	
D (unlikely)	
E (rare)	

Principle 7: Security = Risk Management (cont.)

- Vulnerability
  - A known problem within a system or program
- Exploit
  - A program or a “cookbook” on how to take advantage of a specific vulnerability
- Attacker
  - The link between a vulnerability and an exploit

Principle 8: The Three Types of Security Controls Are Preventative, Detective, and Responsive

- A security mechanism serves a purpose by **preventing a compromise**, **detecting that a compromise or compromise attempt** is underway, or **responding to a compromise** while it is happening or after it has been discovered

Principle 9: Complexity Is the Enemy of Security

- The more complex a system gets, the harder it is to secure

Principle 10: Fear, Uncertainty, and Doubt (FUD) Do Not Work in Selling Security

- Information security managers must justify all investments in security using techniques of the trade
- When spending resources can be justified with good, solid business rationale, security requests are rarely denied

Principle 11: People, Process, and Technology Are All Needed to Adequately Secure a System or Facility

- **People controls**
  - **Dual control and separation of duties**
- **Process controls**
  - **Different people can perform the same operation the same way every time**
- **Technology alone without people and process controls can fail**
- **People, process, and technology controls are essential elements of security practices** including operations security, applications development security, physical security, and cryptography

Principle 12: Open Disclosure of Vulnerabilities Is Good for Security!

- Keeping a given vulnerability secret from users and from the software developer can only lead to a false sense of security
- The need to know trumps the need to keep secrets to give users the right to protect themselves

Summary

- Security management creates the context in which individual security mechanisms operate.
- Without good security management, even strong security mechanisms may be ineffective
- Important guidelines: ISO 27002 and the BSI Baseline Protection Manual.
- Risk analysis gives management information about the risks an organisation faces and the countermeasures that can be taken.
- Security management guidelines and risk analysis methods can be described as organized common sense.

Summary

- Computer security specialists must not only know the technical side of their jobs but also must understand the principles behind information security
- These principles are mixed and matched to describe why certain security functions and operations exist in the real world of IT