DATABASE ADMINISTRATION AND SECURITY

OBJECTIVES

- The distinction between *data* administration and *database* administration.
- The purpose and tasks associated with data administration and database administration.
- The scope of database security.

OBJECTIVES

- Why database security is a serious concern for an organization.
- The type of threats that can affect a database system.
- How to protect a computer system using computer-based controls.

DATA ADMINISTRATION AND DATABASE ADMINISTRATION

- Data Administrator (DA) and Database Administrator (DBA) are responsible for managing and controlling activities associated with corporate data and corporate database, respectively.
- DA is more concerned with early stages of lifecycle and DBA is more concerned with later stages.

DATA ADMINISTRATION

- Management and control of corporate data, including:
  - database planning
  - development and maintenance of standards, policies, and procedures
  - conceptual and logical database design

DATA ADMINISTRATION TASKS 1/2

Selecting appropriate productivity tools

Assisting in the development of the corporate IT/IS and business strategies

Undertaking feasibility studies and planning for database development

Developing a corporate data model

Determining the organization's data requirements

Setting data collection standards and establishing data formats

Estimating volumes of data and likely growth

Determining patterns and frequencies of data usage

Determining data access requirements and safeguards for both legal and corporate requirements

Undertaking logical database design

DATA ADMINISTRATION TASKS 2/2

Liaising with database administration staff and application developers to ensure applications meet all stated requirements

Educating users on data standards and legal responsibilities

Keeping up to date with IT/IS and business developments

Ensuring documentation is complete, including the corporate data model, standards, policies, procedures, and controls on end-users

Managing the data dictionary

Liaising with end-users and database administration staff to determine new requirements and to resolve data access or performance problems

Developing a security policy

DATABASE ADMINISTRATION

- Management and control of physical realization of a database system, including:
  - physical database design and implementation
  - setting security and integrity controls
  - monitoring system performance
  - reorganizing the database

DATABASE ADMINISTRATION TASKS

Evaluating and selecting DBMS products

Undertaking physical database design

Implementing a physical database design using a target DBMS

Defining security and integrity constraints

Liaising with database system developers

Developing test strategies

Training users

Responsible for 'signing off' the implemented database system

Monitoring system performance and tuning the database, as appropriate

Performing backups routinely

Ensuring recovery mechanisms and procedures are in place

Ensuring documentation is complete, including in-house produced material

Keeping up to date with software and hardware developments and costs, and installing updates as necessary

COMPARISON OF DATA AND DATABASE ADMINISTRATION

Data administration	Database administration
Involved in strategic IS planning	Evaluates new DBMSs
Determines long-term goals	Executes plans to achieve goals
Determines standards, policies, and procedures	Enforces standards, policies, and procedures
Determines data requirements	Implements data requirements
Develops logical database design	Develops physical database design
Develops and maintains corporate data model	Implements physical database design
Coordinates database development	Monitors and controls database use
Managerial orientation	Technical orientation
DBMS independent	DBMS dependent

DATABASE SECURITY

- Mechanisms that protect the database against intentional or accidental threats.
- Not only apply to the data held in a database: breaches of security may affect other parts of the system, which may in turn affect the database.

DATABASE SECURITY

- Includes hardware, software, people, and data.
- Growing importance of security is the increasing amounts of crucial corporate data being stored on computer.

DATABASE SECURITY

- Outcomes to avoid:
  - theft and fraud
  - loss of confidentiality (secrecy)
  - loss of privacy
  - loss of integrity
  - loss of availability

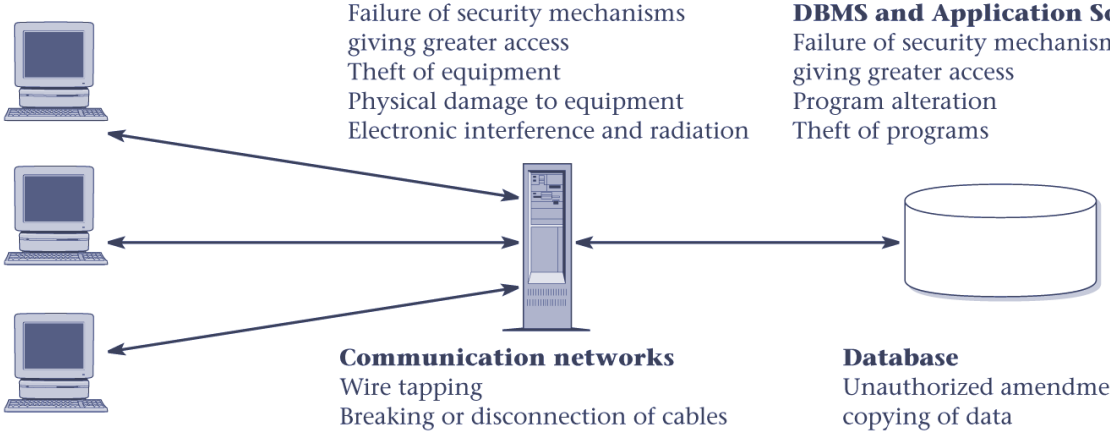
DATABASE SECURITY

- Threat
  - Any situation or event, whether intentional or unintentional, that may adversely affect a system and consequently the organization.

EXAMPLES OF THREATS AND POSSIBLE OUTCOMES

Threat	Theft and fraud	Loss of confidentiality	Loss of privacy	Loss of integrity	Loss of availability
Using another person's means of access	√	√	√		
Unauthorized amendment or copying of data	√			√	
Program alteration	√			√	√
Inadequate policies and procedures that allow a mix of confidential and normal output	√	√	√		
Wire tapping	√	√	√		
Illegal entry by hacker	√	√	√		
Blackmail	√	√	√		
Creating 'trapdoor' into system	√	√	√		
Theft of data, programs, and equipment	√	√	√		√
Failure of security mechanisms, giving greater access than normal	√	√	√		
Staff shortage or strikes				√	√
Inadequate staff training		√	√	√	√
Viewing and disclosing unauthorized data	√	√	√		
Electronic interference and radiation				√	√
Data corruption due to power loss or surge				√	√
Fire (electrical fault, lightning strike, arson), flood, bomb				√	√
Physical damage to equipment				√	√
Breaking cables or disconnection of cables				√	√
Introduction of viruses				√	√

SUMMARY OF THREATS TO COMPUTER SYSTEMS



Hardware
Fire/flood/bombs
Data corruption due to power loss or surge
Failure of security mechanisms giving greater access
Theft of equipment
Physical damage to equipment
Electronic interference and radiation

DBMS and Application Software
Failure of security mechanism giving greater access
Program alteration
Theft of programs

Communication networks
Wire tapping
Breaking or disconnection of cables
Electronic interference and radiation

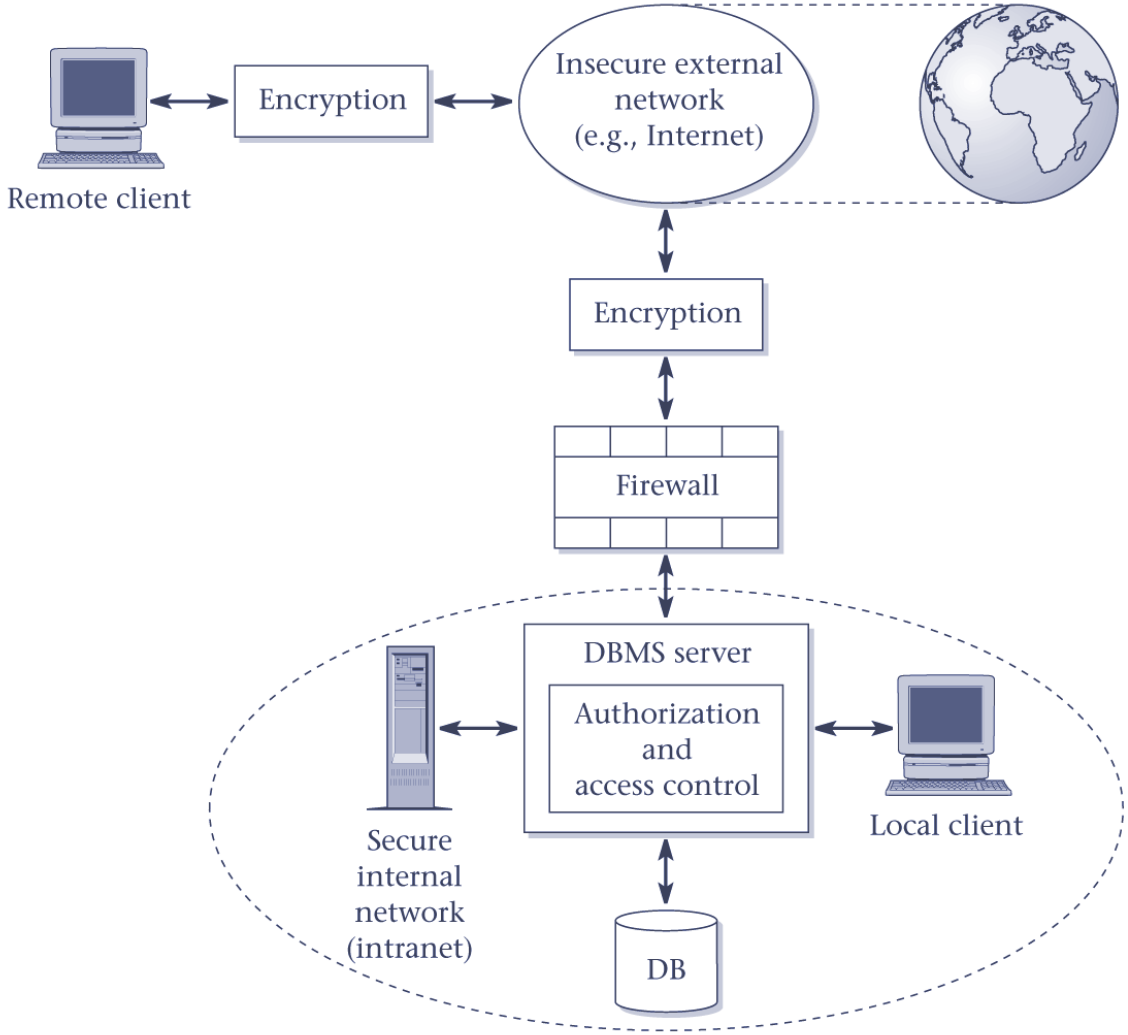
Database
Unauthorized amendment or copying of data
Theft of data
Data corruption due to power loss or surge

Users
Using another person's means of access
Viewing and disclosing unauthorized data
Inadequate staff training
Illegal entry by hacker
Blackmail
Introduction of viruses

Programers/Operators
Creating trapdoors
Program alteration (such as creating software that is insecure)
Inadequate staff training
Inadequate security policies and procedures
Staff shortages or strikes

Data/Database Administrator
Inadequate security policies and procedures

TYPICAL MULTI-USER COMPUTER ENVIRONMENT



COUNTERMEASURES – COMPUTER-BASED CONTROLS

- Authorization
- Views
- Backup And Recovery
- Integrity
- Encryption
- Redundant array of independent disks (RAID)

COUNTERMEASURES – COMPUTER-BASED CONTROLS

- Authorization
  - The granting of a right or privilege that enables a subject to have legitimate access to a database system or a database system's object.
- Authentication
  - A mechanism that determines whether a user is, who he or she claims to be.

COUNTERMEASURES – COMPUTER-BASED CONTROLS

- View
  - A view is a *virtual table* that does not necessarily exist in the database but can be produced upon request by a particular user, at the time of request.

COUNTERMEASURES – COMPUTER-BASED CONTROLS

- Backup
  - Process of periodically taking a copy of the database and log file (and possibly programs) onto offline storage media.
- Journaling
  - Process of keeping and maintaining a log file (or journal) of all changes made to database to enable recovery to be undertaken effectively in the event of failure.

COUNTERMEASURES – COMPUTER-BASED CONTROLS

- Integrity
  - Prevents data from becoming invalid, and hence giving misleading or incorrect results.
- Encryption
  - Encoding the data by a special algorithm that renders the data unreadable by any program without the decryption key.

REDUNDANT ARRAY OF INDEPENDENT DISKS (RAID)

- Hardware that the DBMS runs on must be *fault-tolerant*, meaning that the DBMS should continue to operate even if one of the hardware components fails.
- Suggests having redundant components that can be seamlessly integrated into the working system whenever there are failures.

REDUNDANT ARRAY OF INDEPENDENT DISKS (RAID)

- The main hardware components that should be fault-tolerant include disk drives, disk controllers, CPU, power supplies, and cooling fans.
- Disk drives are the most vulnerable components with the shortest times between failure of any of the hardware components.
- One solution is to provide a large disk array comprising an arrangement of several independent disks that are organized to improve reliability and at the same time increase performance.

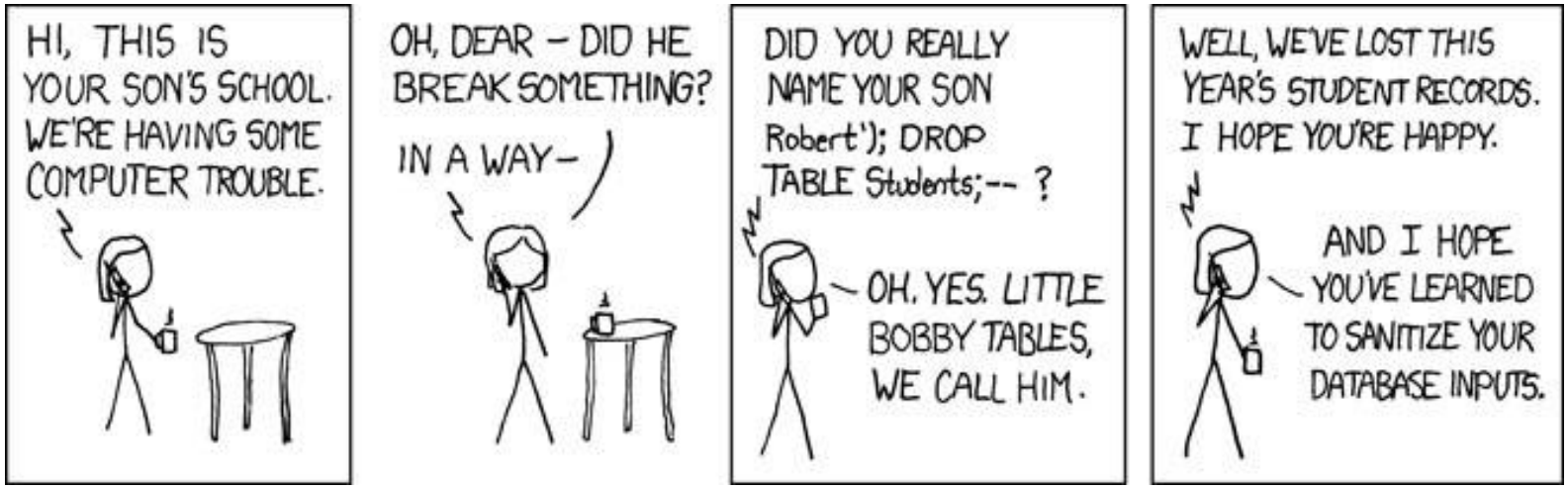
LINKS

- http://en.wikipedia.org/wiki/Database_security
- http://www.dbta.com/Categories/Database-Security_332.aspx
- http://www.craigsmullins.com/dbta_035.htm & http://www.craigsmullins.com/dbta_056.htm & http://www.craigsmullins.com/dbta_096.htm
- http://iase.disa.mil/stigs/ => checklists

SQL-INJEKTIOT JA NIIDEN EHKÄISY

JOUNI HUOTARI & JUHA PELTOMÄKI

ESIMERKKEJÄ



Lähde: http://xkcd.com/327/

Jos sovelluksessa on esim. merkkijono

String sql = ”SELECT fieldlist FROM table WHERE (name = **'” + param_nimi +”');**”

ja siihen sijoitetaan em. pojan nimi, lopputulos on

SELECT * FROM table WHERE (name = **'Robert');DROP TABLE Students;--';**

SUOJAUTUMINEN SQL-INJEKTIOILTA

- Virheilmoitusten kustomointi
  - Ei liikaa tietoa käyttäjälle
- Syötteiden tarkastus / suodatus
  - Vaaralliset käskyt / merkit
  - Käytetään valmisfunktioita
- Parametroitu SQL
  - Monissa ohjelmointikielissä kuten Javassa Prepared Statement: paikkamerkit kyselyn parametreille
  - Parametrit heittomerkkien väliin

ESIMERKKEJÄ

- SQL-injektio: http://fi.wikipedia.org/wiki/SQL-injektio
- Prevention: https://www.owasp.org/index.php/SQL_Injection_Prevention_Cheat_Sheet
- Peltomäen Juhan opetusmateriaali: http://homes.jamk.fi/~huojo/opetus/IIO30200/PHP-tietoturva.html