Database Security

Agenda

- Database security
- Types of threat
- Countermeasures
- Web security
- Other considerations

Database Security

- Data is a valuable resource that must be strictly controlled and managed, as with any corporate resource.
- Part or all of the corporate data may have strategic importance and therefore needs to be kept secure and confidential.

Database Security

- Countermeasures are mechanisms that protect the database against intentional or accidental threats.
- Security considerations do 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.

Agenda

- Database security
- Types of threat
- Countermeasures
- Web security
- Other considerations

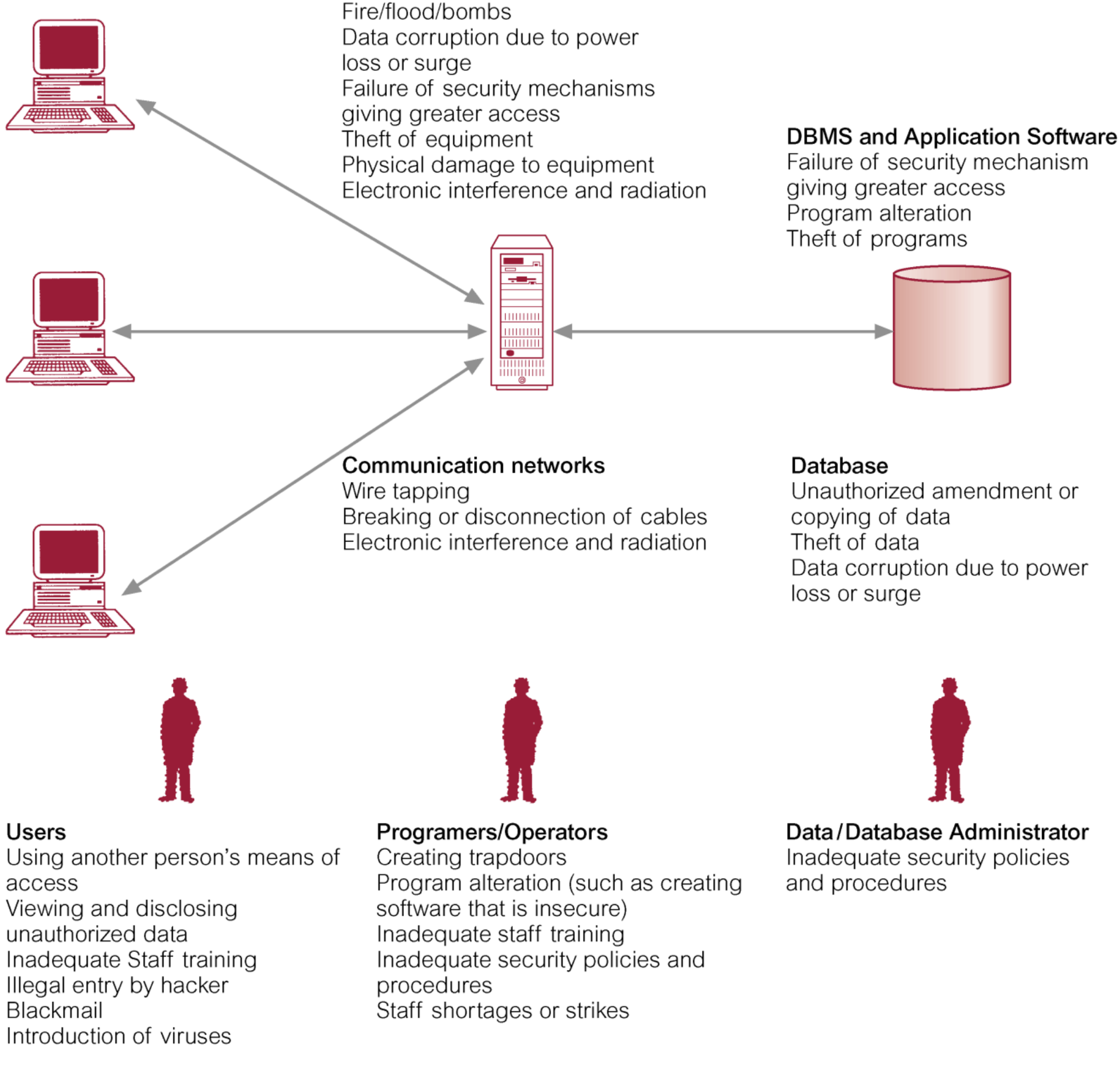
Database Security

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

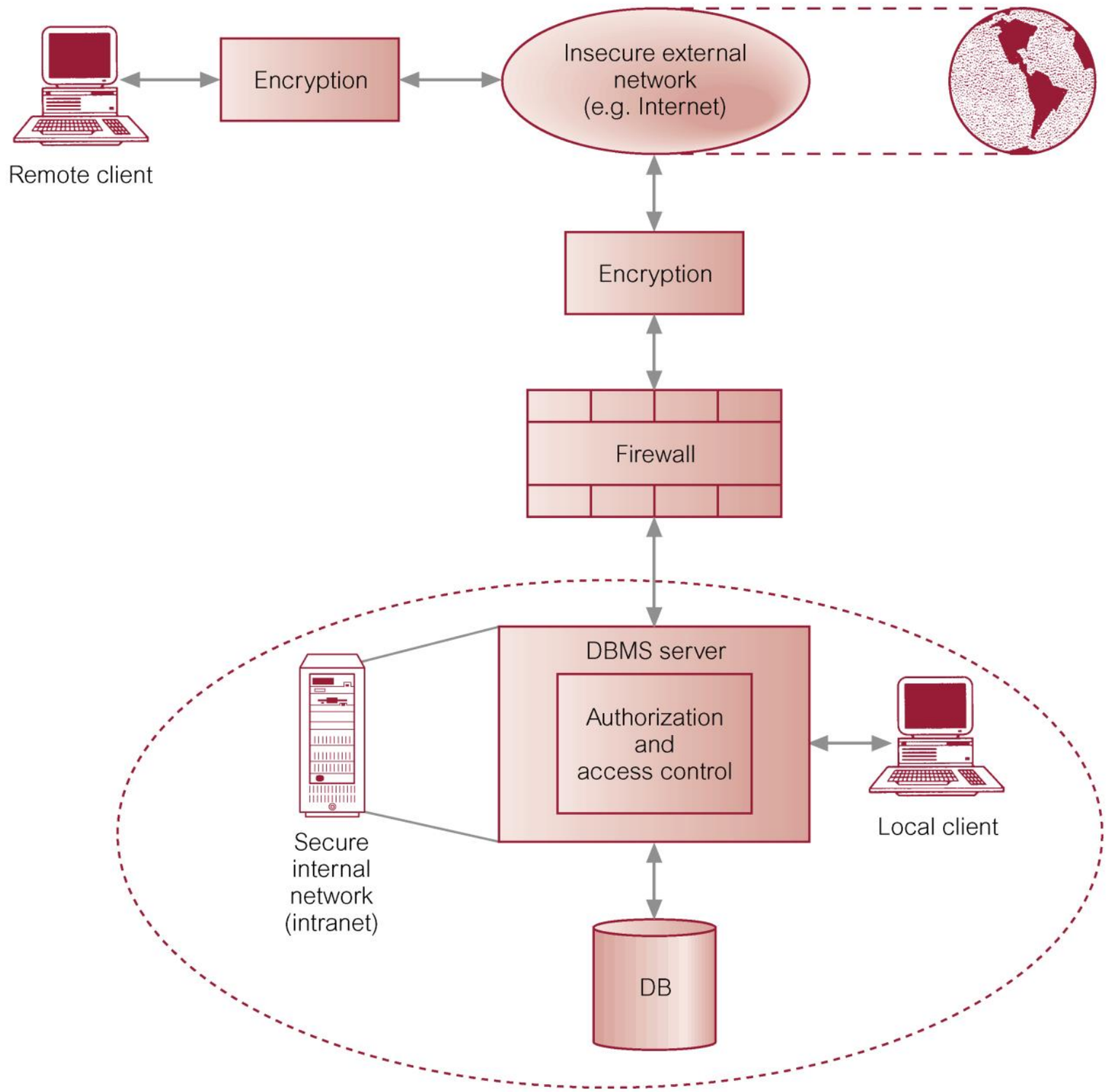
Types of threat

- Theft and fraud
- Loss of confidentiality (secrecy)
- Loss of privacy
- Loss of integrity
- Loss of availability

Summary of Threats to Computer Systems



Typical Multi-user Computer Environment



Agenda

- Database security
- Types of threat
- Countermeasures
- Web security
- Other considerations

Countermeasures – Computer-Based Controls

- Concerned with physical controls to administrative procedures and includes:
  1. Authorization
  2. Access controls
  3. Views
  4. Backup and recovery
  5. Integrity
  6. Encryption
  7. RAID technology

Countermeasures – Computer-Based Controls

1. Authorization
   - The granting of a right or privilege, which enables a subject to legitimately have access to a system or a system's object.
   - Authorization is a mechanism that determines whether a user is who he or she claims to be.
   - Passwords, keycards, biometrics, etc.

Countermeasures – Computer-Based Controls

2. Access control
   - Based on the granting and revoking of privileges.
   - A privilege allows a user to create or access (that is read, write, or modify) some database object (such as a relation, view, and index) or to run certain DBMS utilities.
   - Privileges are granted to users to accomplish the tasks required for their jobs.

Countermeasures – Computer-Based Controls

- Most DBMS provide an approach called Discretionary Access Control (DAC).
- SQL standard supports DAC through the GRANT and REVOKE commands.
- The GRANT command gives privileges to users, and the REVOKE command takes away privileges.

Countermeasures – Computer-Based Controls

3. View
   - Is the dynamic result of one or more relational operations operating on the base relations to produce another relation.
   - A view is a virtual relation that does not actually exist in the database, but is produced upon request by a particular user, at the time of request.

Countermeasures – Computer-Based Controls

4. Backup and recovery

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

Countermeasures – Computer-Based Controls

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

Countermeasures – Computer-Based Controls

7. RAID (Redundant Array of Independent Disks) Technology
   - Hardware that the DBMS is running 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 is one or more component failures.

RAID (Redundant Array of Independent Disks) Technology

- 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.

Other countermeasures

- Not all countermeasures against threats to security are computer-based; should also consider:

8. Physical security
   - Secure access to the physical location(s) where data is stored

9. Policies and procedures

Threats and Countermeasures

Scenario One:

- A laptop is stolen that contains a database with the names, DOBs, PPS numbers and blood types of 145,000 donors

- What type of threat to security does this represent?
- What countermeasures could have been used to prevent this?

Threats and Countermeasures

Scenario Two:

- A national brokerage firm uses an electronic funds transfer system to transmit sensitive financial data between locations.

- What type of potential threat to security does this represent?
- What countermeasures could be used to prevent this?

Agenda

- Database security
- Types of threat
- Countermeasures
- Web security
- Other considerations

DBMSs and Web Security

- Internet communication relies on TCP/IP as the underlying protocol. However, TCP/IP and HTTP were not designed with security in mind. Without special software, all Internet traffic travels ‘in the clear’ and anyone who monitors traffic can read it.

DBMSs and Web Security

- Must ensure while transmitting information over the Internet that:
  - inaccessible to anyone but sender and receiver (privacy);
  - not changed during transmission (integrity);
  - receiver can be sure it came from sender (authenticity);
  - sender can be sure receiver is genuine (non-fabrication);
  - sender cannot deny he or she sent it (non-repudiation).

DBMSs and Web Security

- Measures include:
  - Proxy servers
  - Firewalls
  - Message digest algorithms and digital signatures
  - Digital certificates
  - Kerberos
  - Secure sockets layer (SSL) and Secure HTTP (S-HTTP)
  - Secure Electronic Transactions (SET) and Secure Transaction Technology (SST)
  - Java security
  - ActiveX security

Agenda

- Database security
- Types of threat
- Countermeasures
- Web security
- Other considerations

May 2018…


I just wanted
to let you know
that you matter to me...
And I want to keep
in touch if you want
Who are you?
Some
Website
HAPPY
GDPR BREAK-UP Emails
WEEK!!
@twisteddoodles

Data Protection

- The General Data Protection Regulation is a regulation in EU law on data protection and privacy for all individuals within the European Union (EU)
- Must be considered when storing or processing data relating to an individual

Principles for data controllers

- Personal data must be:
  - Processed lawfully, fairly and in a transparent manner in relation to the data subject
  - Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
  - Adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed
  - Accurate and kept up to date and every reasonable step must be taken to ensure that personal data that is inaccurate is erased or rectified without delay
  - Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage

Legal bases for processing data

- The legal bases for lawful processing are:
  - The data subject has given consent to the processing of his or her personal data for one or more specific purposes
  - Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract
  - Processing is necessary for compliance with a legal obligation to which the controller is subject
  - Processing is necessary in order to protect the vital interests of the data subject or of another natural person
  - Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller