CN7028 – Database Systems

University of East London

Pioneering Futures Since 1898

Lecture #9

Database Security and Administration

Module leader

Dr Hisham AbouGrad

University of East London

Agenda

- Distinguish between Security and Integrity
- Provide examples of accidental and deliberate threats to databases
- Describe methods of providing security
- Describe how views provide security and how they are updated
- Describe what and how integrity constraints could be expressed and enforced
- How to protect a computer system using computer-based controls.
- Recognise the approaches for securing a DBMS on the Web.

University of East London

Learning Outcomes

After this session, you should be able to:

- ❑ Recognise the scope of database security.
- ❑ Understand why database security is a serious concern for organizations.
- ❑ Identify the types of threat that can affect a database system.
- ❑ Learn how to protect a computer system using computer-based controls.
- ❑ Know the different approaches for securing a DBMS.
- ❑ Distinction between data administration and database administration.
- ❑ Understand the purpose and tasks associated with data administration and database administration.

Integrity

University of East London

Integrity refers to the correctness of the data

- **Referential Integrity** - Concerned with relationships between tables eg, Does a foreign key value actually have a corresponding primary key in another table?
- **Entity Integrity** - Each row of a table has a unique and non-null primary key value

University of East London

Integrity Enhancement Feature – IEF

- **Consider five types of integrity constraints:**
  - required data
  - domain constraints
  - entity integrity
  - referential integrity
  - general constraints.
- ***searchCondition*** **can involve a table lookup:**

```
CREATE DOMAIN BranchNo AS CHAR(4)
CHECK (VALUE IN (SELECT branchNo
                 FROM Branch));
```

- **Domains can be removed using DROP DOMAIN:**

```
DROP DOMAIN DomainName
        [RESTRICT | CASCADE]
```

Required Data

```
position   VARCHAR(10)      NOT NULL
```

Domain Constraints

(a) CHECK

```
sex        CHAR      NOT NULL
                     CHECK (sex IN ('M', 'F'))
```

(b) CREATE DOMAIN

```
CREATE DOMAIN DomainName [AS] dataType
[DEFAULT defaultOption]
[CHECK (searchCondition)]
```

For example:

```
CREATE DOMAIN SexType AS CHAR
                CHECK (VALUE IN ('M', 'F'));
sex        SexType   NOT NULL
```

University of East London

IEF: Referential Integrity

- FK is column or set of columns that links each row in child table containing foreign FK to row of parent table containing matching PK.
- Referential integrity means that, if FK contains a value, that value must refer to existing row in parent table.
- ISO standard supports definition of FKs with FOREIGN KEY clause in CREATE and ALTER TABLE:

  FOREIGN KEY(branchNo) REFERENCES Branch

- Any INSERT/UPDATE attempting to create FK value in child table without matching CK value in parent is rejected.
- Action taken attempting to update/delete a CK value in parent table with matching rows in child is dependent on referential action specified using ON UPDATE and ON DELETE subclauses:
  - CASCADE - SET NULL
  - SET DEFAULT - NO ACTION

University of East London

IEF: Referential Integrity

Referential Integrity Actions

CASCADE: Delete row from parent and delete matching rows in child, and so on in cascading manner.

SET NULL: Delete row from parent and set FK column(s) in child to NULL. Only valid if FK columns are NOT NULL.

SET DEFAULT: Delete row from parent and set each component of FK in child to specified default. Only valid if DEFAULT specified for FK columns.

NO ACTION: Reject delete from parent. Default.

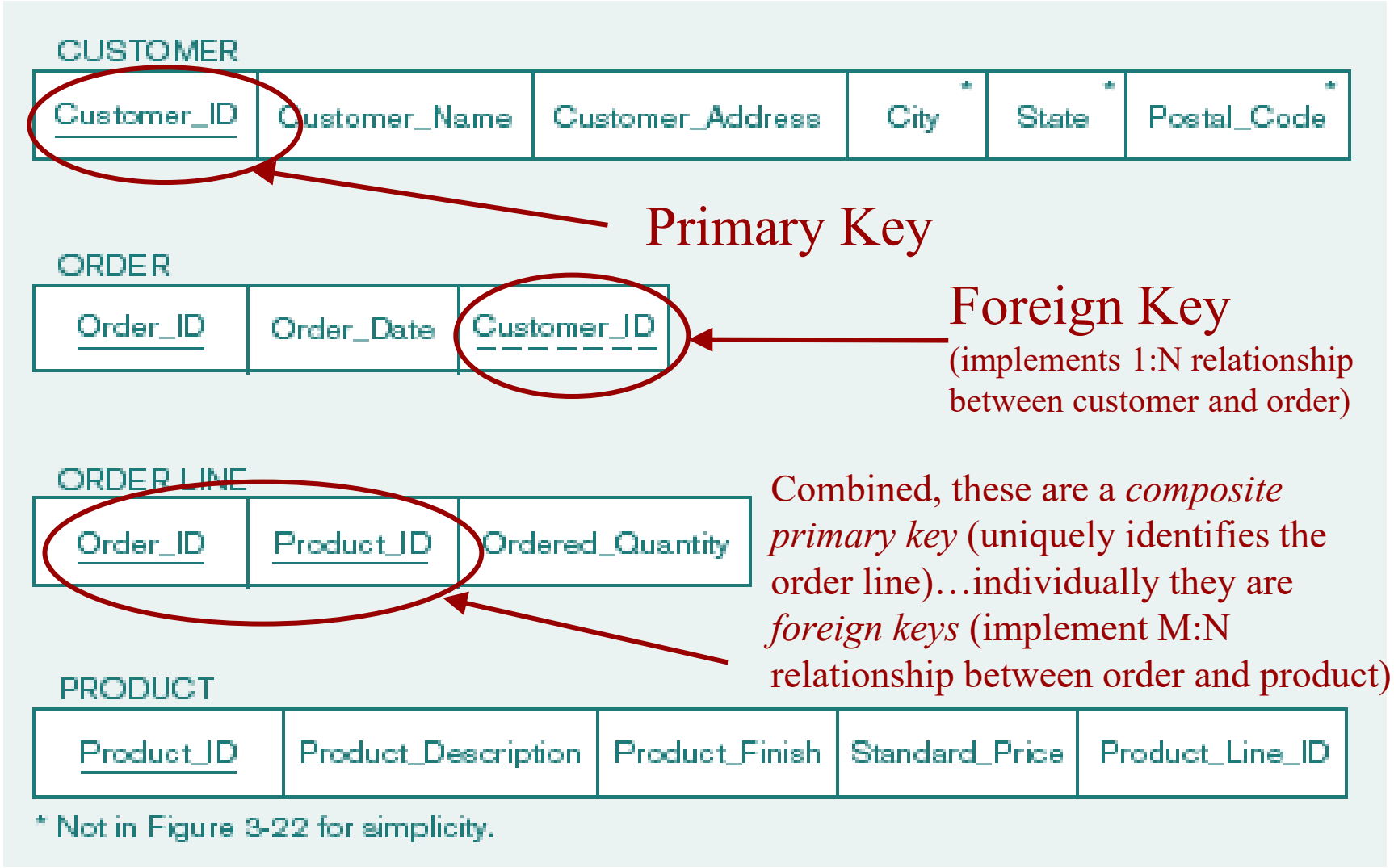
```
FOREIGN KEY (staffNo) REFERENCES Staff
    ON DELETE SET NULL

FOREIGN KEY (ownerNo) REFERENCES Owner
    ON UPDATE CASCADE
```

University of East London

IEF: Referential Integrity

Schema for four relations (Pine Valley Furniture Company)



University of East London

IEF: Entity Integrity

- Primary key of a table must contain a unique, non-null value for each row.
- ISO standard supports FOREIGN KEY clause in CREATE and ALTER TABLE statements:

```
PRIMARY KEY(staffNo)
PRIMARY KEY(clientNo, propertyNo)
```

- Can only have one PRIMARY KEY clause per table. Can still ensure uniqueness for alternate keys using UNIQUE:

```
UNIQUE(telNo)
```

University of East London

Integrity Constraints

Domain Constraints

Allowable values for an attribute. See Table 5-1

Entity Integrity

No primary key attribute may be null. All primary key fields **MUST** have data

Table 5-1 Domain Definitions for INVOICE Attributes

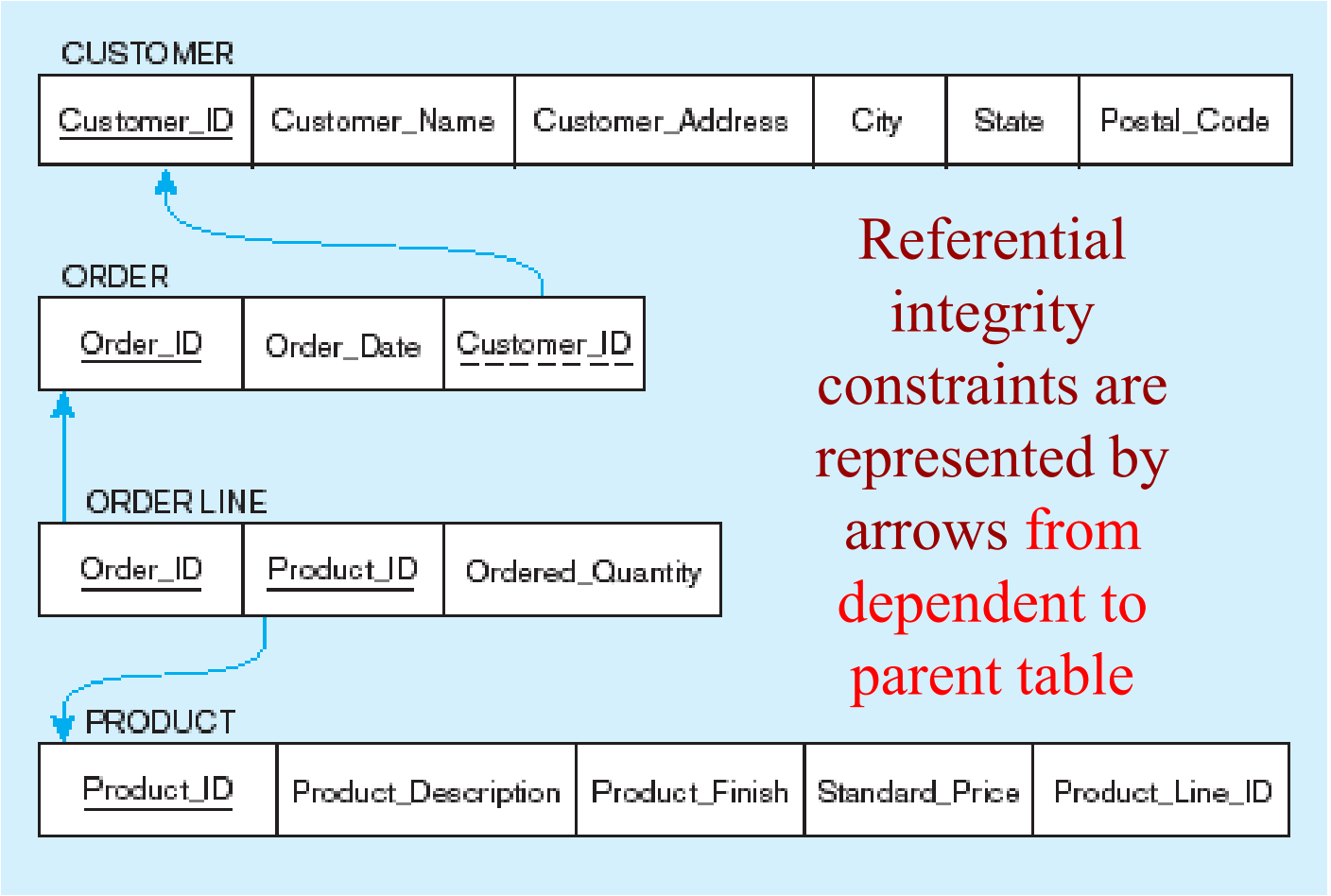
Attribute	*Domain Name*	*Description*	*Domain*
Customer_ID	Customer_IDs	Set of all possible customer IDs	character: size 5
Customer_Name	Customer_Names	Set of all possible customer names	character: size 25
Customer_Address	Customer_Addresses	Set of all possible customer addresses	character: size 30
City	Cities	Set of all possible cities	character: size 20
State	States	Set of all possible states	character: size 2
Postal_Code	Postal_Codes	Set of all possible postal zip codes	character: size 10
Order_ID	Order_IDs	Set of all possible order IDs	character: size 5
Order_Date	Order_Dates	Set of all possible order dates	date format mm/dd/yy
Product_ID	Product_IDs	Set of all possible product IDs	character: size 5
Product_Description	Product_Descriptions	Set of all possible product descriptions	character size 25
Product_Finish	Product_Finishes	Set of all possible product finishes	character: size 15
Standard_Price	Unit_Prices	Set of all possible unit prices	monetary: 6 digits
Product_Line_ID	Product_Line_IDs	Set of all possible product line IDs	integer: 3 digits
Ordered_Quantity	Quantities	Set of all possible ordered quantities	integer: 3 digits

University of East London

Integrity Constraints

- **Referential Integrity–rule states that any foreign key value**
  - MUST match a primary key value in the relation
  - Or the foreign key can be null

Referential integrity constraints (Pine Valley Furniture)



University of East London

Database Security

University of East London

What is Database Security?

- **Protecting the DB from unauthorised access: Data is a valuable resource that must be strictly controlled and managed, as with any corporate resource.**
- **Have to protect the privacy of individuals: Part or all of the corporate data may have strategic importance and therefore needs to be kept secure and confidential.**
- **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.**
- **Involves measures to avoid:**
  - Theft and fraud
  - Loss of confidentiality (secrecy)
  - Loss of privacy
  - Loss of integrity
  - Loss of availability

University of East London

Database Security: Privacy & Threats

- **Privacy**
  - Privacy is the right of individuals to have control over stored information about them
  - Organisations are legally bound to adopt security policies
  - A Database should only hold data that is required by the organization
- **Threat**
  - Any situation or event, whether intentional or unintentional, that will adversely affect a system and consequently an organization.
- **Accidental Threats**
  - User unintentionally requests an operation and is granted it due to an oversight of operation
  - A person is accidentally sent a message destined for someone else
  - Communication system error results in connecting a user to another's session
  - System fails to perform actions as it should

University of East London

Database Security: Privacy & Threats

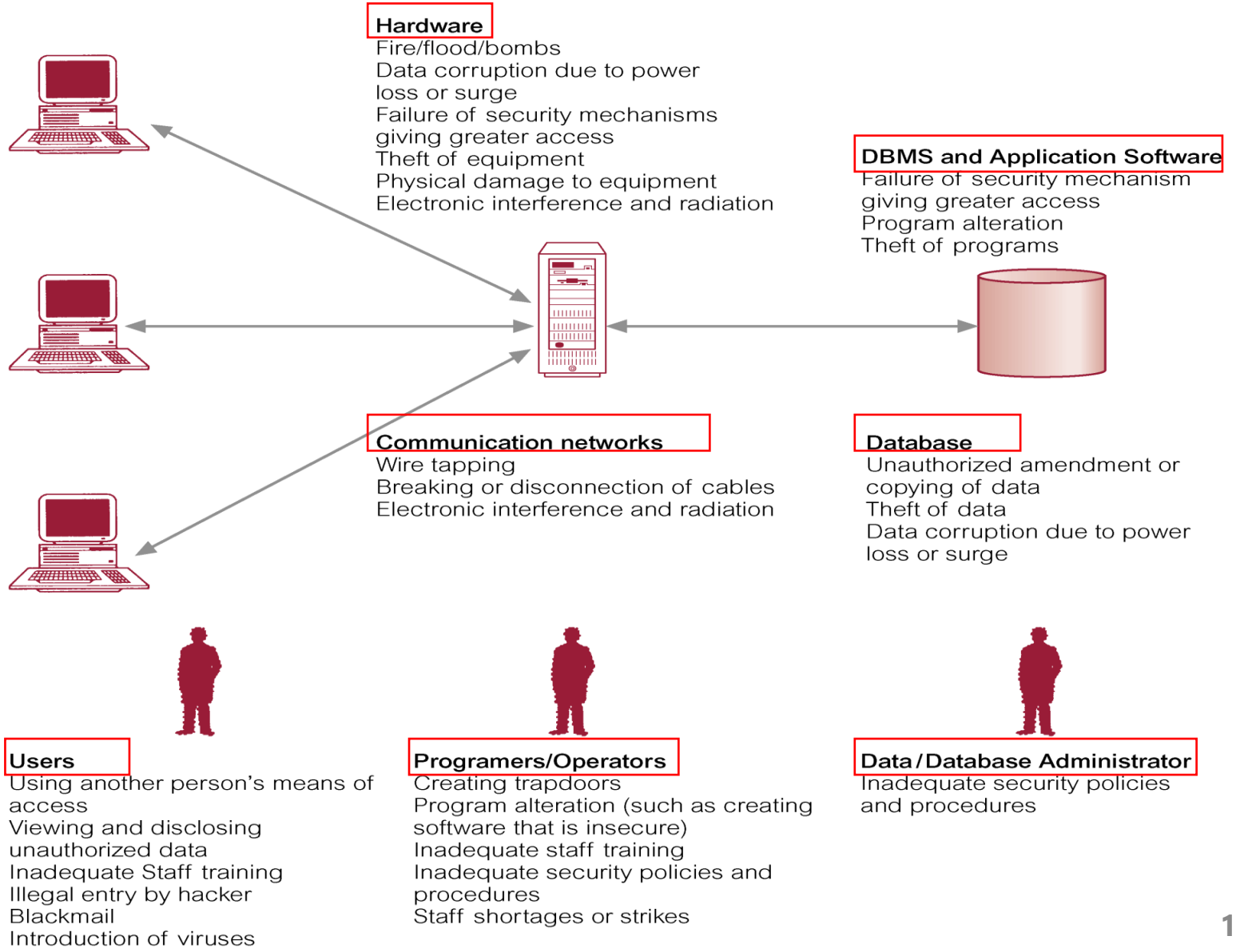
Deliberate/intentional Threats

- Reading Display screens
- Impersonating an authorised user
  - Using another person's id
- Writing programs to access the DB
  - Illegal entry by a hacker
  - Program alteration
- Removing hardware
- Bribing, Blackmailing

University of East London

Database Security: Privacy & Threats

Summary of Threats To Computer Systems

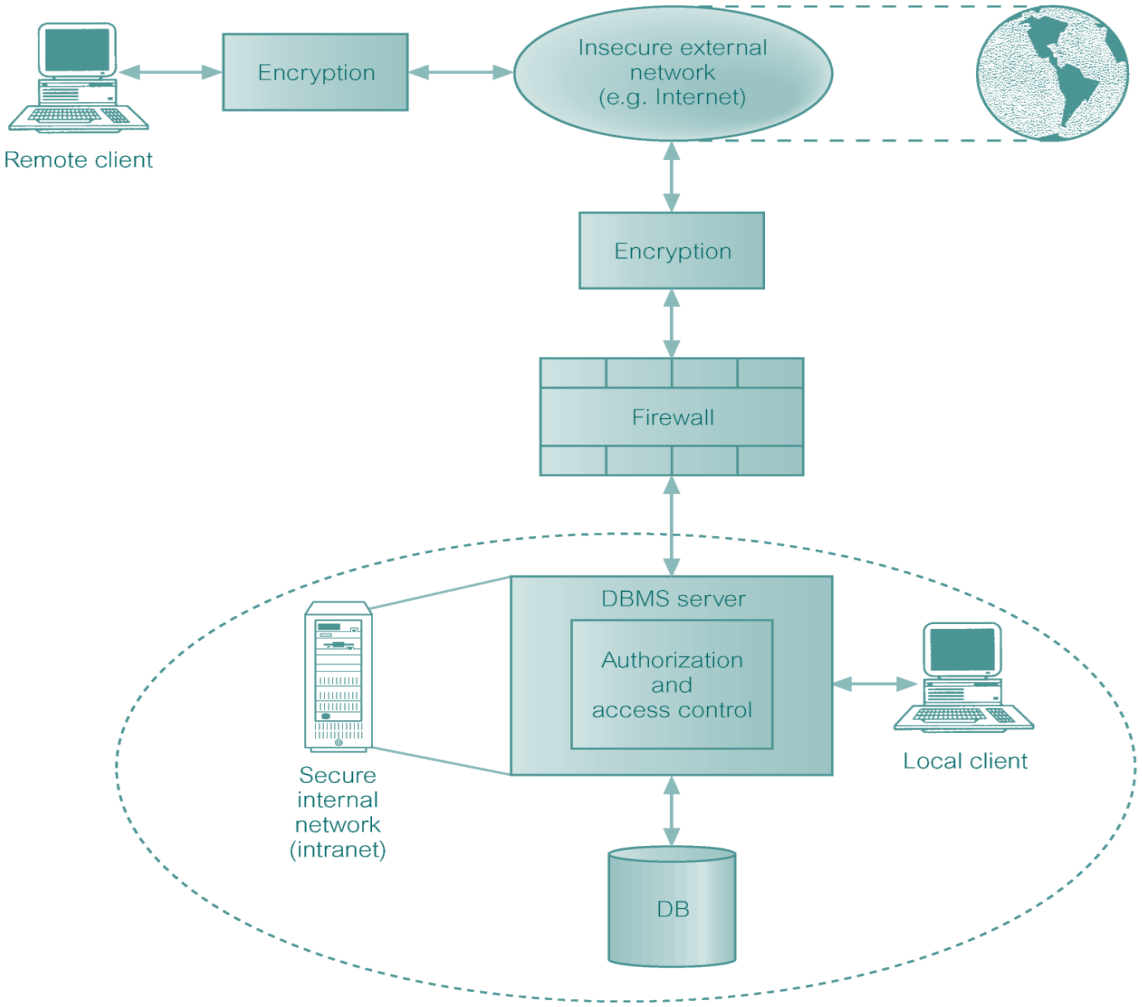


University of East London

Database Security: Privacy & Threats

- **Aspects of Security Problems**
  - **Legal/social**
  - **Levels of Security**
  - **Authentication Methods**
  - **Physical controls**
  - **Operational problems (how are the passwords protected)**
  - **Operating system Security (does the o/s protect/erase files when finished with?)**

Typical Multi-user Computer Environment



University of East London

Security Controls

University of East London

Countermeasures: Computer-Based Controls

- **Concerned with physical controls to administrative procedures and includes:**
  - **Authorization**
  - **Access controls**
  - **Views**
  - **Backup and recovery (Log files)**
  - **Integrity**
  - **Encryption**

University of East London

Countermeasures: Computer-Based Controls

- **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.
  - A given user will have authorisation to access different database objects and or individual data items
    - Records/rows
    - Files/tables
    - Database
  - A given user will also have different modes/levels of access to different objects.
    - SELECT
    - SELECT and UPDATE
    - READ or WRITE

University of East London

Countermeasures: Computer-Based Controls

- **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.
  - 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.
  - A privilege allows a user to create or access (that is read, write, or modify) some database object (such as a table, view, etc) or to run certain DBMS utilities.
  - Privileges are granted to users to accomplish the tasks required for their jobs.

University of East London

Countermeasures: Computer-Based Controls

- **Access control**
  - **In planning the access, the DBA often uses an access control matrix.**

Subject	Table 1	Table 2	Table 4	Table 5	Table 6
User 1001	Read	Read	All	All	All
User 1002	Update	Update	Read	Read	Read
User 1003	Read	Read	Write	Update	Read

University of East London

Countermeasures: Computer-Based Controls

- **Grant** command
  - A user may allow others access to data only if they themselves are allowed to access the data and give out the privileges

- Anyone who is an authoriser can revoke the privileges that they have granted
  - **Revoke** update **on** student **from** ‘mary’;

```
grant all
        on student
        to ‘mary’, ‘george’;
```

```
Grant select, update, insert
        on student
        to ‘george’;
```

University of East London

Countermeasures: Computer-Based Controls

Data Control Language - Grant & Revoke

GRANT *privilege* TO *the public or user*

(Allowing users to: select and update data from the ***Student*** *table)*

REVOKE *privilege* TO *user*

```
GRANT SELECT, UPDATE
ON STUDENT
TO PUBLIC;
        Or
GRANT SELECT, INSERT
ON STUDENT
TO JULIETTE;

REVOKE INSERT
ON STUDENT
FROM JULIETTE;
```

What PUBLIC means?

All Users

University of East London

Countermeasures: Computer-Based Controls

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

University of East London

Countermeasures: Computer-Based Controls

- **Integrity**
  - Prevents data from becoming invalid, and hence giving misleading or incorrect results.
- **Encryption**
  - The encoding of the data by a special algorithm that renders the data unreadable by any program without the decryption key.
- **Security Tools**
  - Security log
    - Records attempted security violations
  - Keep an audit trail
    - Records all access to the database
    - Operations
    - Terminal used
    - User details
  - Encrypt the data so that only the DBMS can access the information

University of East London

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.

- 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).**

University of East London

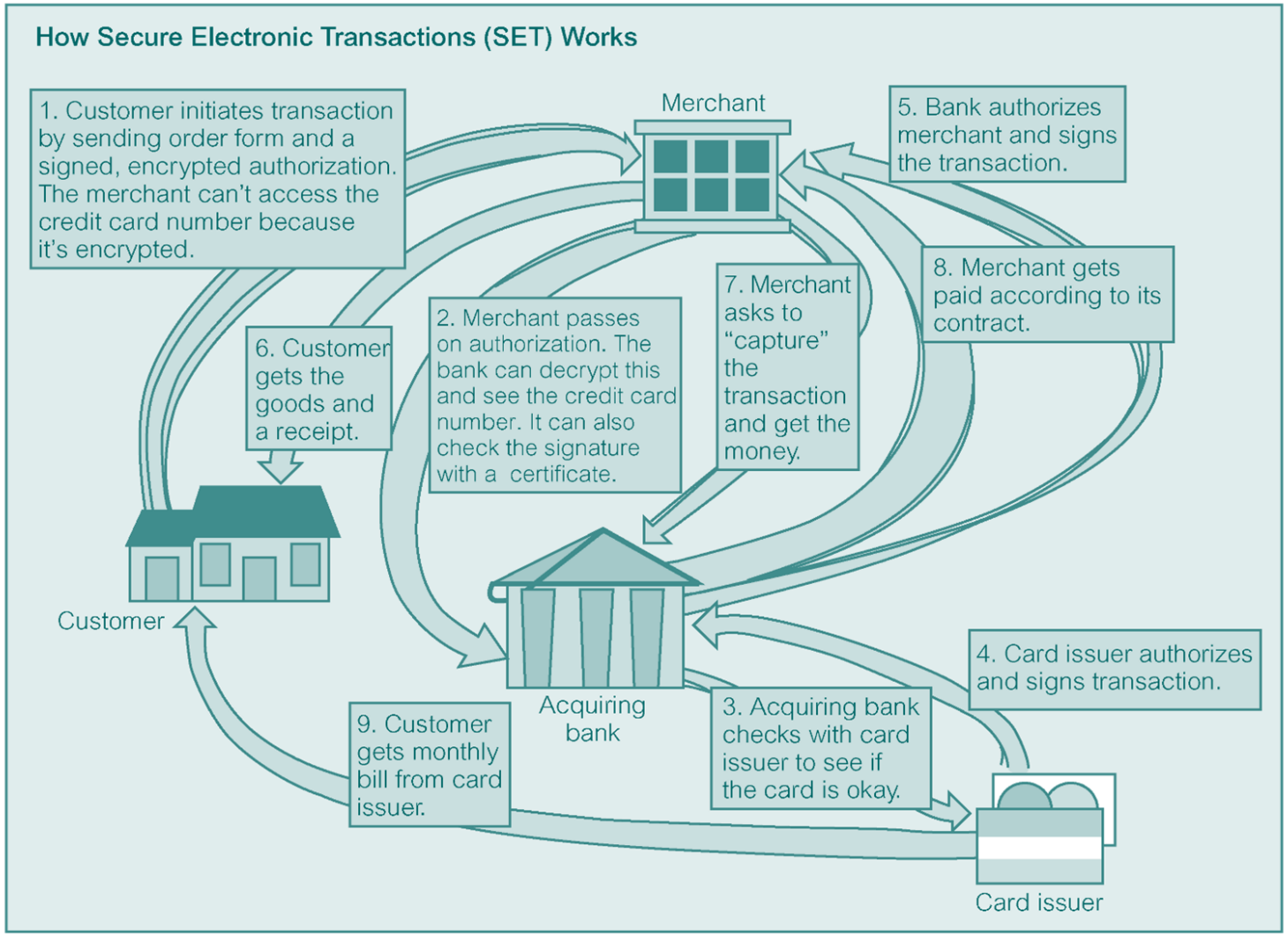
DBMSs and Web Security

- 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**

University of East London

DBMSs and Web Security

How Secure Electronic Transactions (SET) Works



University of East London

Summary

- **Security Vs. Integrity**
  - **Security :** ensuring that users only do what they are allowed to do
  - **Integrity:** ensuring that the users perform the correct actions
- **Security is an important aspect of DB design**
- **Privacy of users is crucial for trust**
- **SQL uses Data Control Language to Grant & Revoke user's access to different levels of data**
- **Standard security protocols should be in place for achieving better security of the resultant application**

University of East London

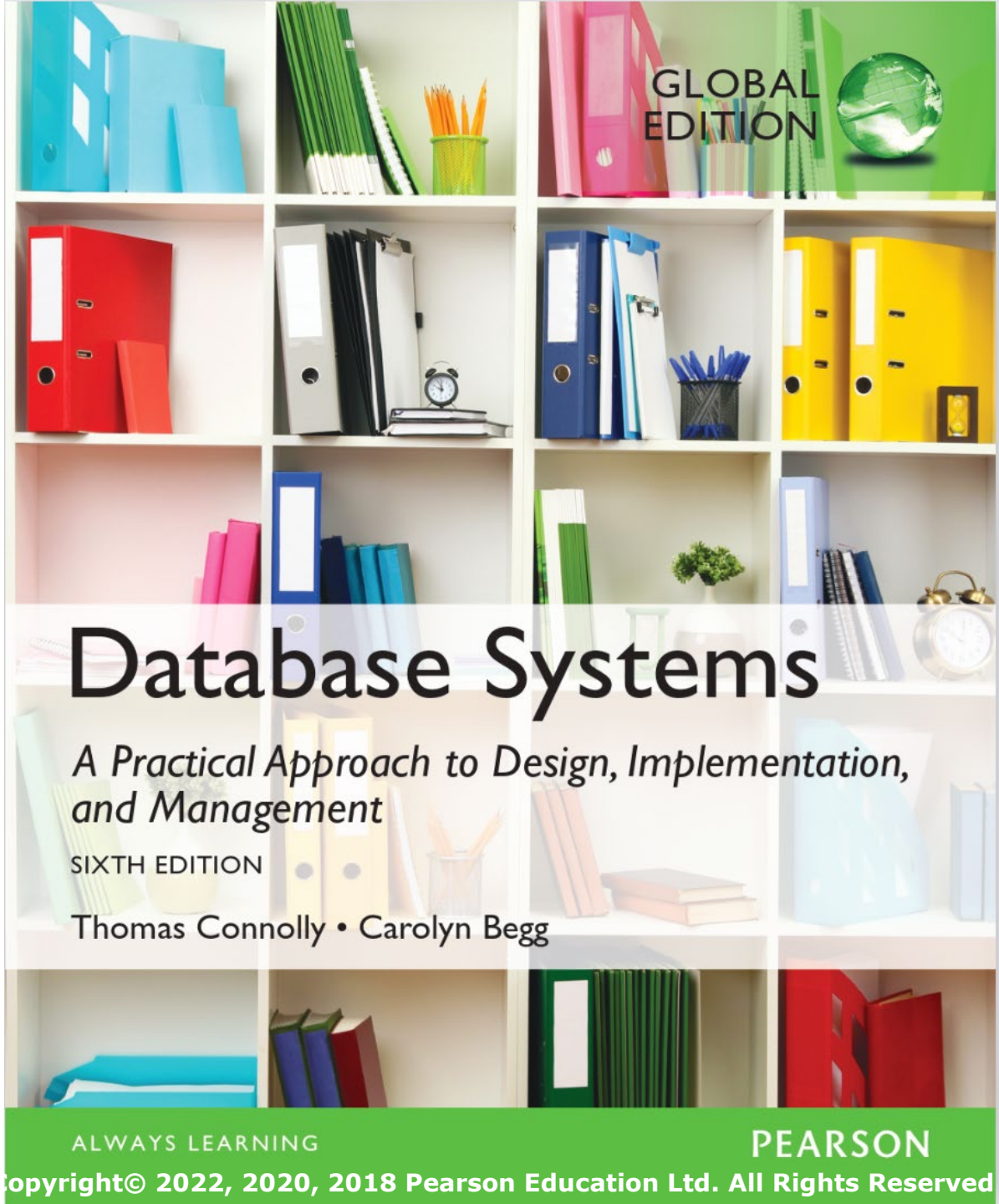
Independent Study

Database Systems
A Practical Approach to Design, Implementation, and Management

Sixth Edition, Global Edition

Chapter 20

Pearson



University of East London

Any Questions?

CN7028 – Database Systems

University of East London

Pioneering Futures Since 1898

Lecture #9

Database Security and Administration

Thank you for attending and participating

Module leader

Dr Hisham AbouGrad