Introduction to Database Security

Assoc. Prof. Dr. Dang Tran Khanh

khanh@hcmut.edu.vn

Outline

- Introduction to DB Security
  - Oracle as an example
- Basic Countermeasures
  - Access Control:
    - DAC (Discretionary Access Control)
    - MAC (Mandatory Access Control)
    - RBAC (Role based Access Control)
  - Flow Control
  - Inference Problem
  - Encryption
- Reading Suggestion
  - [1]: Chapter 30
  - www.oracle.com

Introduction to DB Security

Three Basic Concepts

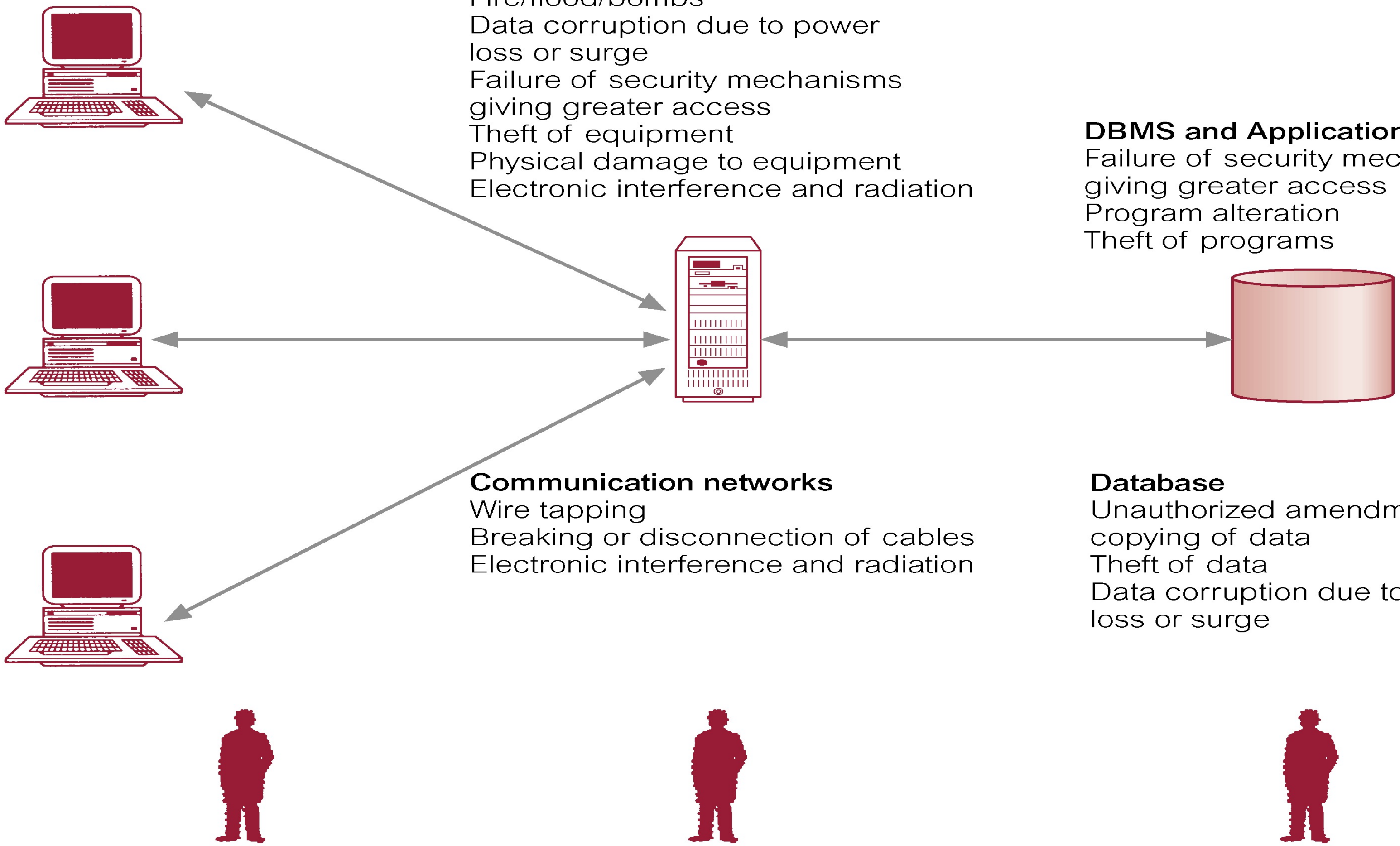
- Authentication: a mechanism that determines whether a user is who he or she claims to be
- Authorization: the granting of a right or privilege, which enables a subject to legitimately have access to a system or a system's objects
- Access Control: a security mechanism (of a DBMS) for restricting access to a system's objects (the database) as a whole

Introduction to DB Security

Threats

- Any situation or event, whether intentional or unintentional, that will adversely affect a system and consequently an organization
- Threats to:
  - Computer systems
  - Databases

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

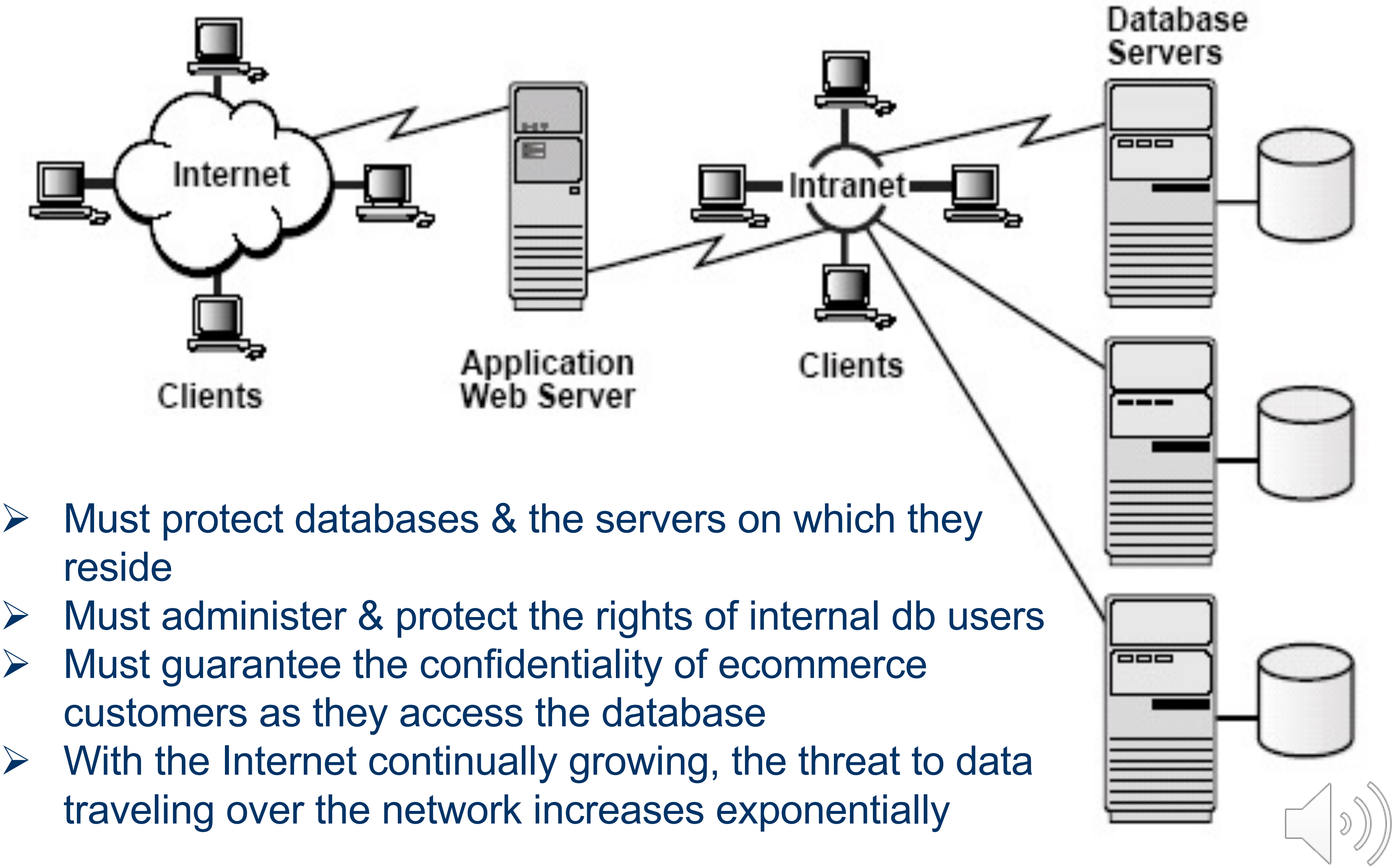
Database
Unauthorized amendment or copying of data
Theft of data
Data corruption due to power loss or surge

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

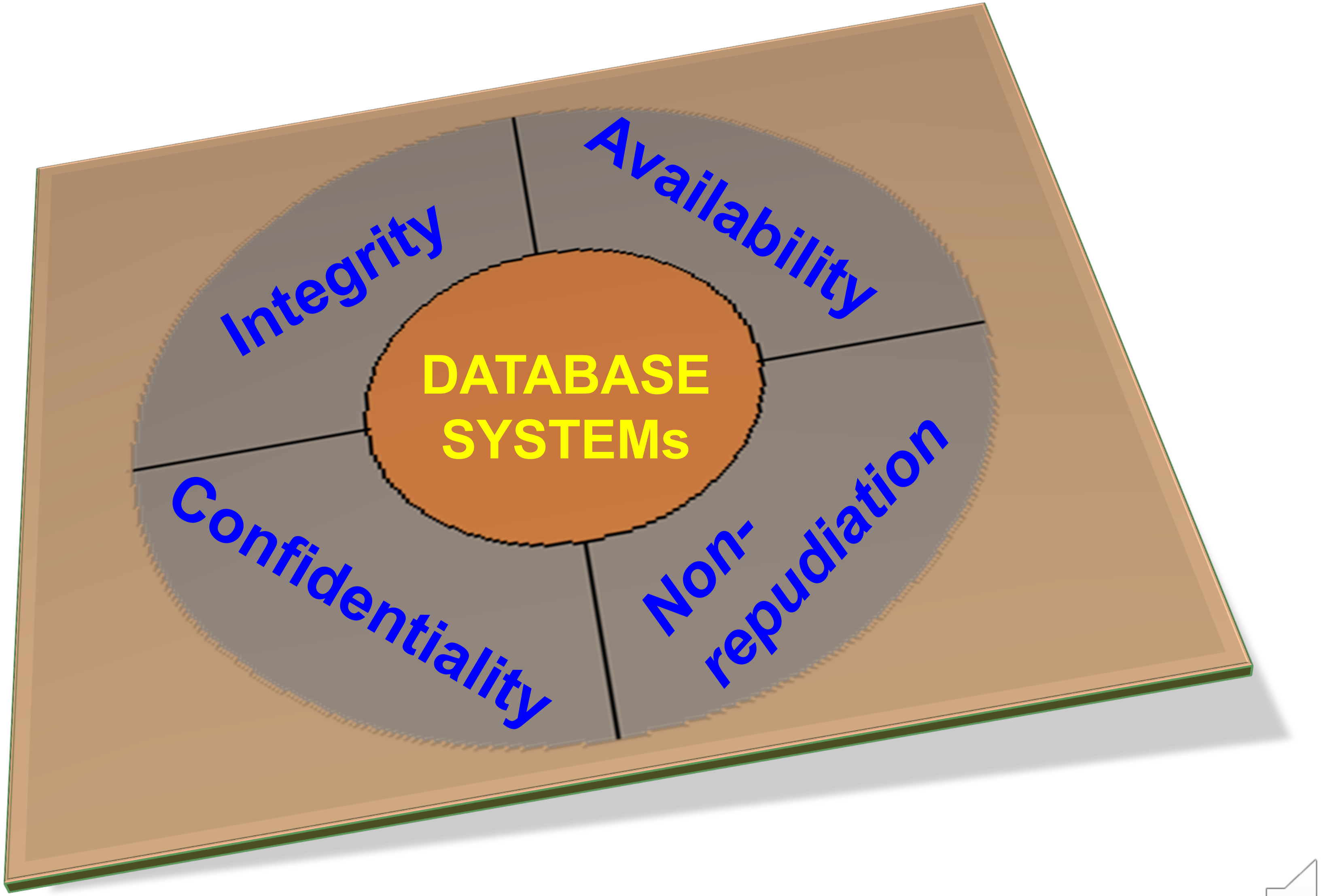
Data/Database Administrator
Inadequate security policies and procedures

Scope of Data Security Needs



- Must protect databases & the servers on which they reside
- Must administer & protect the rights of internal db users
- Must guarantee the confidentiality of ecommerce customers as they access the database
- With the Internet continually growing, the threat to data traveling over the network increases exponentially

Data security requirements



Introduction to DB Security

Fundamental Data Security Requirements

- **Confidentiality**: A secure system ensures the confidentiality of data. This means that it allows individuals to see only the data that they are supposed to see. Confidentiality has several different aspects:
  - Privacy of Communications
  - Secure Storage of Sensitive Data
  - Authenticated Users
  - Granular Access Control

Introduction to DB Security

Fundamental Data Security Requirements

- **Integrity**: A secure system ensures that the data it contains is valid. Data integrity means that data is protected from deletion and corruption, both while it resides within the database, and while it is being transmitted over the network. Integrity has several aspects:
  - System and object privileges control access to application tables and system commands, so that only authorized users can change data
  - Referential integrity is the ability to maintain valid relationships between values in the database, according to rules that have been defined
  - A database must be protected against viruses designed to corrupt the data
  - The network traffic must be protected from deletion, corruption, and eavesdropping

Introduction to DB Security

Fundamental Data Security Requirements

- **Availability:** A secure system makes data available to authorized users, without delay. Denial-of-service attacks are attempts to block authorized users' ability to access and use the system when needed
- **Non-repudiation:** cannot deny what s/he did

Introduction to DB Security

Threats to databases

- Loss of confidentiality: -> must maintain secrecy over data
  - Note: privacy refers to the need to protect data about individuals
- Loss of integrity: -> must prevent the improper modification of information
- Loss of availability: -> must avoid *denial of service* (objective: 24/7 availability)
- Loss of non-repudiation -> auditing & accountability

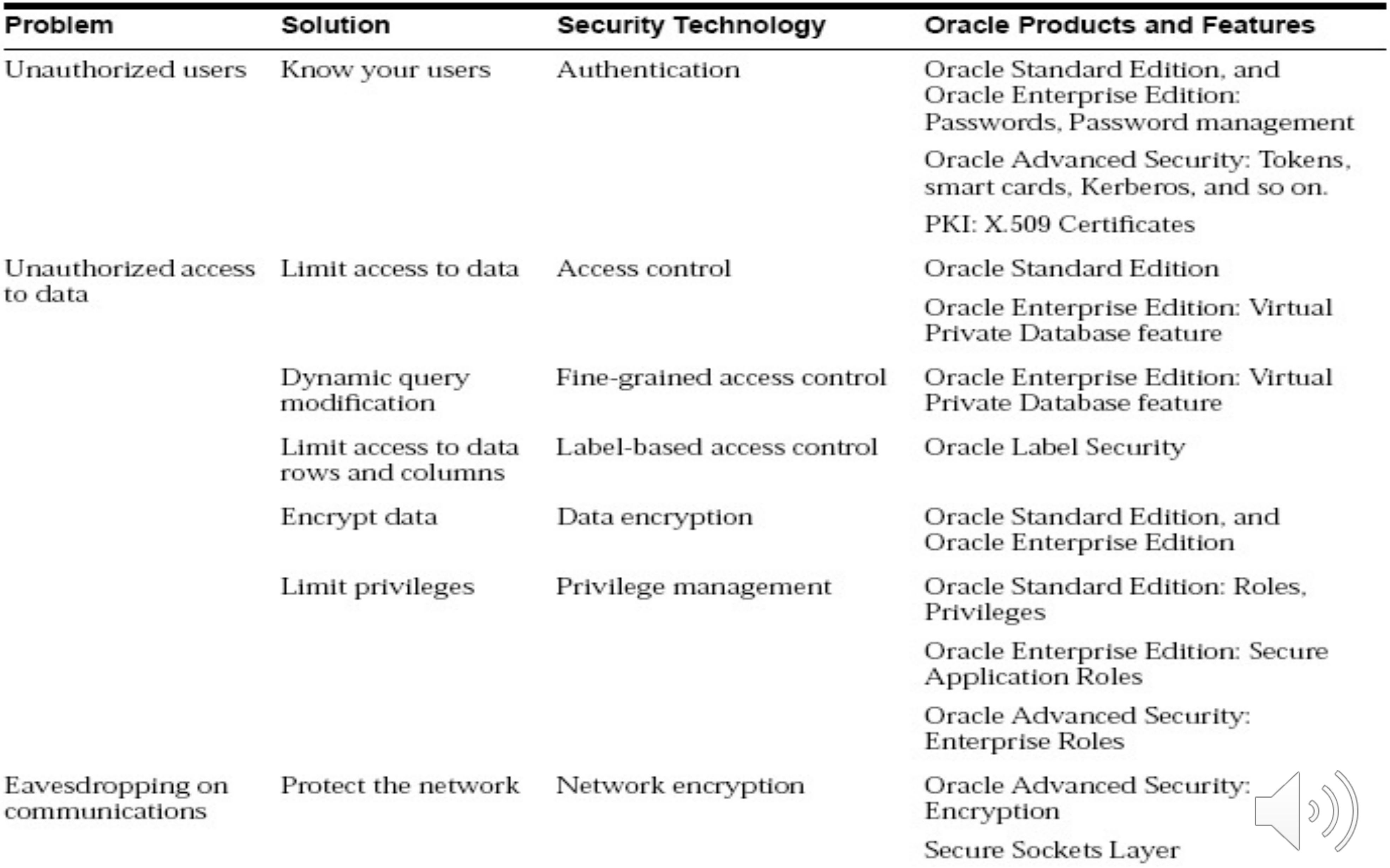
Introduction to DB Security

Countermeasures

- To protect databases against these types of threats five kinds of countermeasures can be implemented:
  - *Access control*
  - *Inference control*
  - *Flow control*
  - *Encryption*
  - *Auditing*

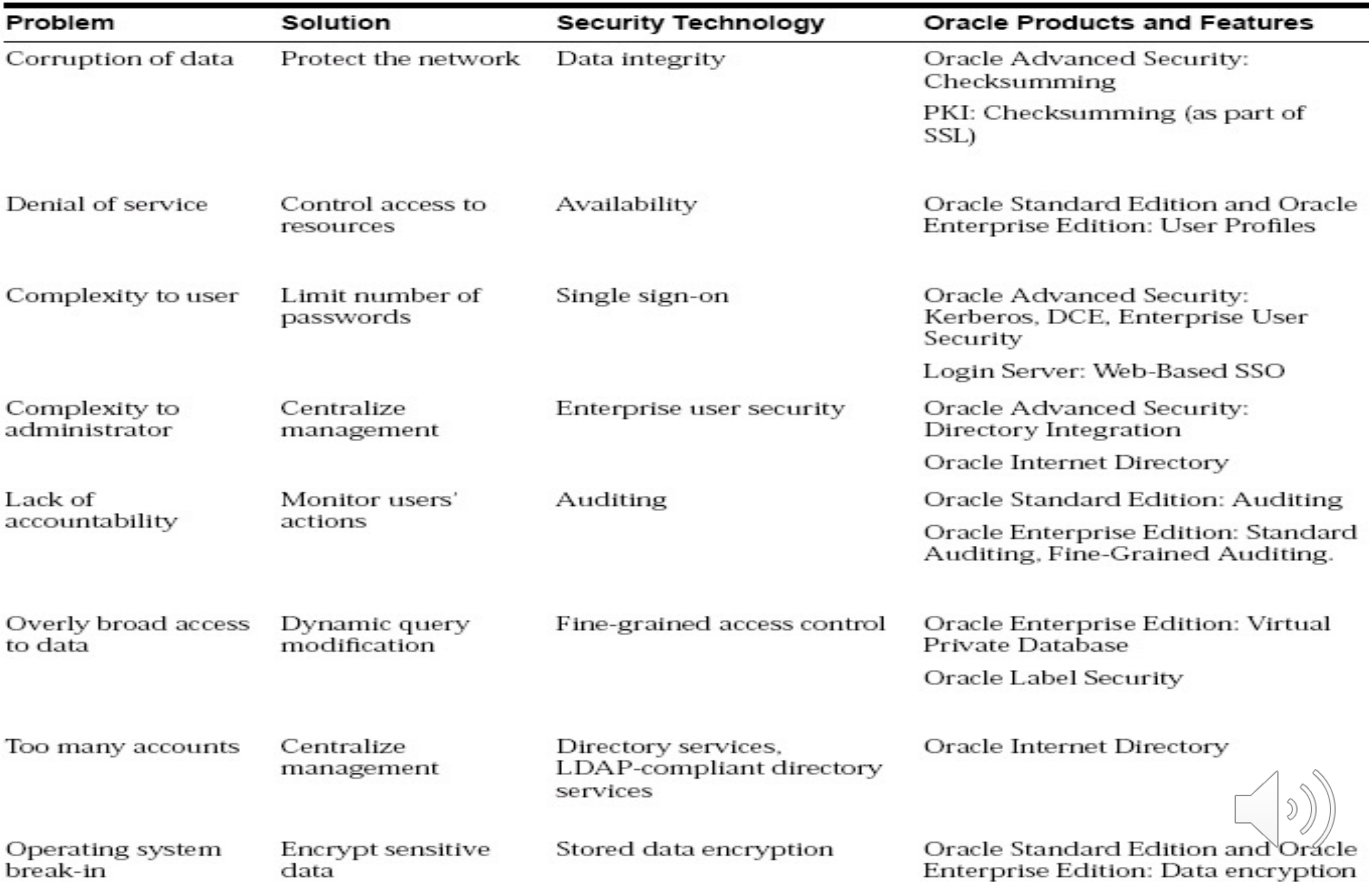
Introduction to DB Security

Oracle as an example (1)



Problem	Solution	Security Technology	Oracle Products and Features
Unauthorized users	Know your users	Authentication	Oracle Standard Edition, and Oracle Enterprise Edition: Passwords, Password management Oracle Advanced Security: Tokens, smart cards, Kerberos, and so on. PKI: X.509 Certificates
Unauthorized access to data	Limit access to data	Access control	Oracle Standard Edition Oracle Enterprise Edition: Virtual Private Database feature
	Dynamic query modification	Fine-grained access control	Oracle Enterprise Edition: Virtual Private Database feature
	Limit access to data rows and columns	Label-based access control	Oracle Label Security
	Encrypt data	Data encryption	Oracle Standard Edition, and Oracle Enterprise Edition
	Limit privileges	Privilege management	Oracle Standard Edition: Roles, Privileges Oracle Enterprise Edition: Secure Application Roles Oracle Advanced Security: Enterprise Roles
Eavesdropping on communications	Protect the network	Network encryption	Oracle Advanced Security: Encryption Secure Sockets Layer

Introduction to DB Security
Oracle as an example (2)



Problem	Solution	Security Technology	Oracle Products and Features
Corruption of data	Protect the network	Data integrity	Oracle Advanced Security: Checksumming PKI: Checksumming (as part of SSL)
Denial of service	Control access to resources	Availability	Oracle Standard Edition and Oracle Enterprise Edition: User Profiles
Complexity to user	Limit number of passwords	Single sign-on	Oracle Advanced Security: Kerberos, DCE, Enterprise User Security Login Server: Web-Based SSO
Complexity to administrator	Centralize management	Enterprise user security	Oracle Advanced Security: Directory Integration Oracle Internet Directory
Lack of accountability	Monitor users' actions	Auditing	Oracle Standard Edition: Auditing Oracle Enterprise Edition: Standard Auditing, Fine-Grained Auditing.
Overly broad access to data	Dynamic query modification	Fine-grained access control	Oracle Enterprise Edition: Virtual Private Database Oracle Label Security
Too many accounts	Centralize management	Directory services, LDAP-compliant directory services	Oracle Internet Directory
Operating system break-in	Encrypt sensitive data	Stored data encryption	Oracle Standard Edition and Oracle Enterprise Edition: Data encryption

Outline

- Introduction to DB Security
  - Oracle as an example
- Basic Countermeasures
  - Access Control:
    - DAC (Discretionary Access Control)
    - MAC (Mandatory Access Control)
    - RBAC (Role based Access Control)
  - Flow Control
  - Inference Problem
  - Encryption
- Reading Suggestion
  - [1]: Chapter 30
  - www.oracle.com

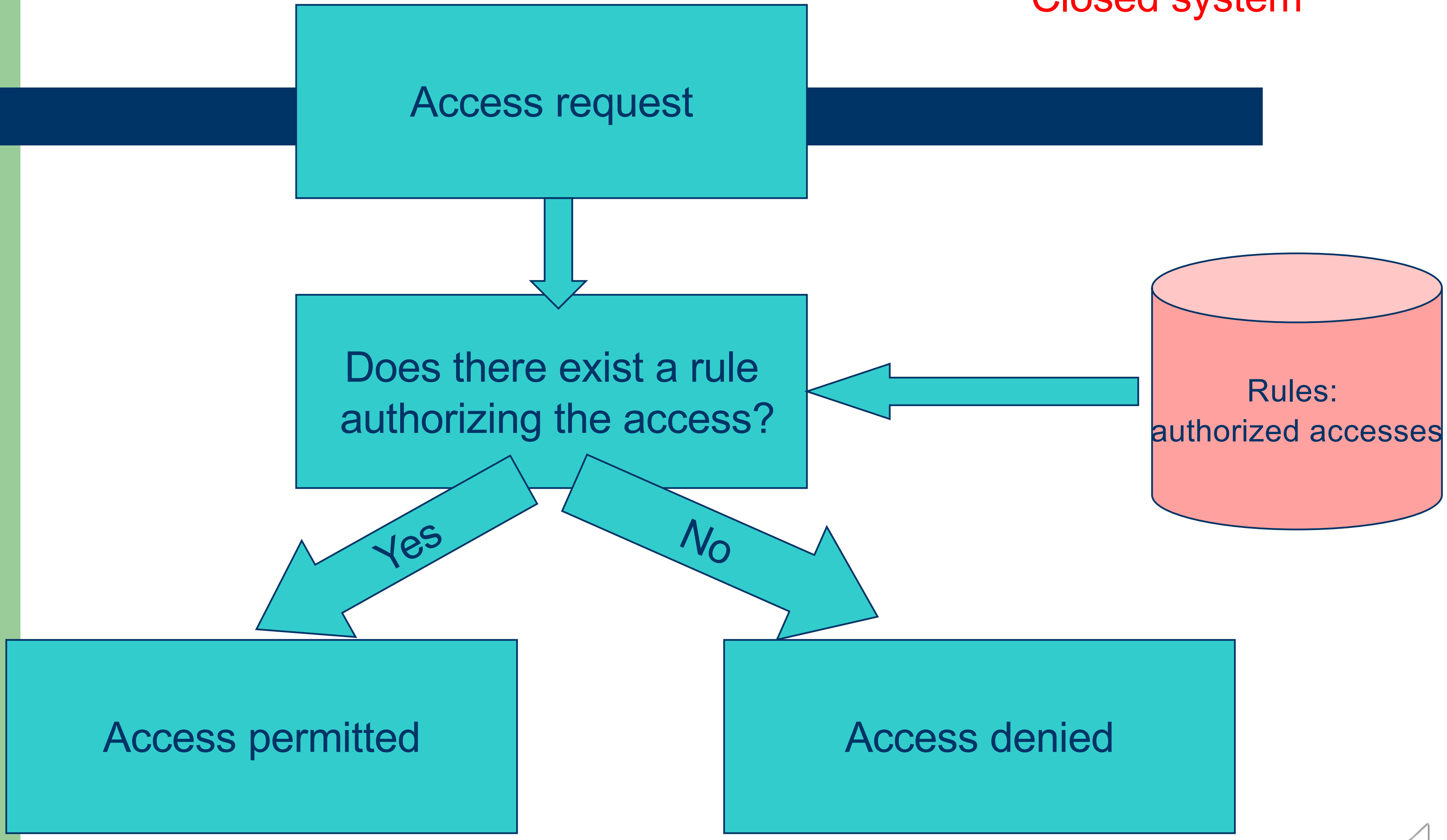
Access Control Systems

- Close systems
- Open systems
- What are the differences between the two?

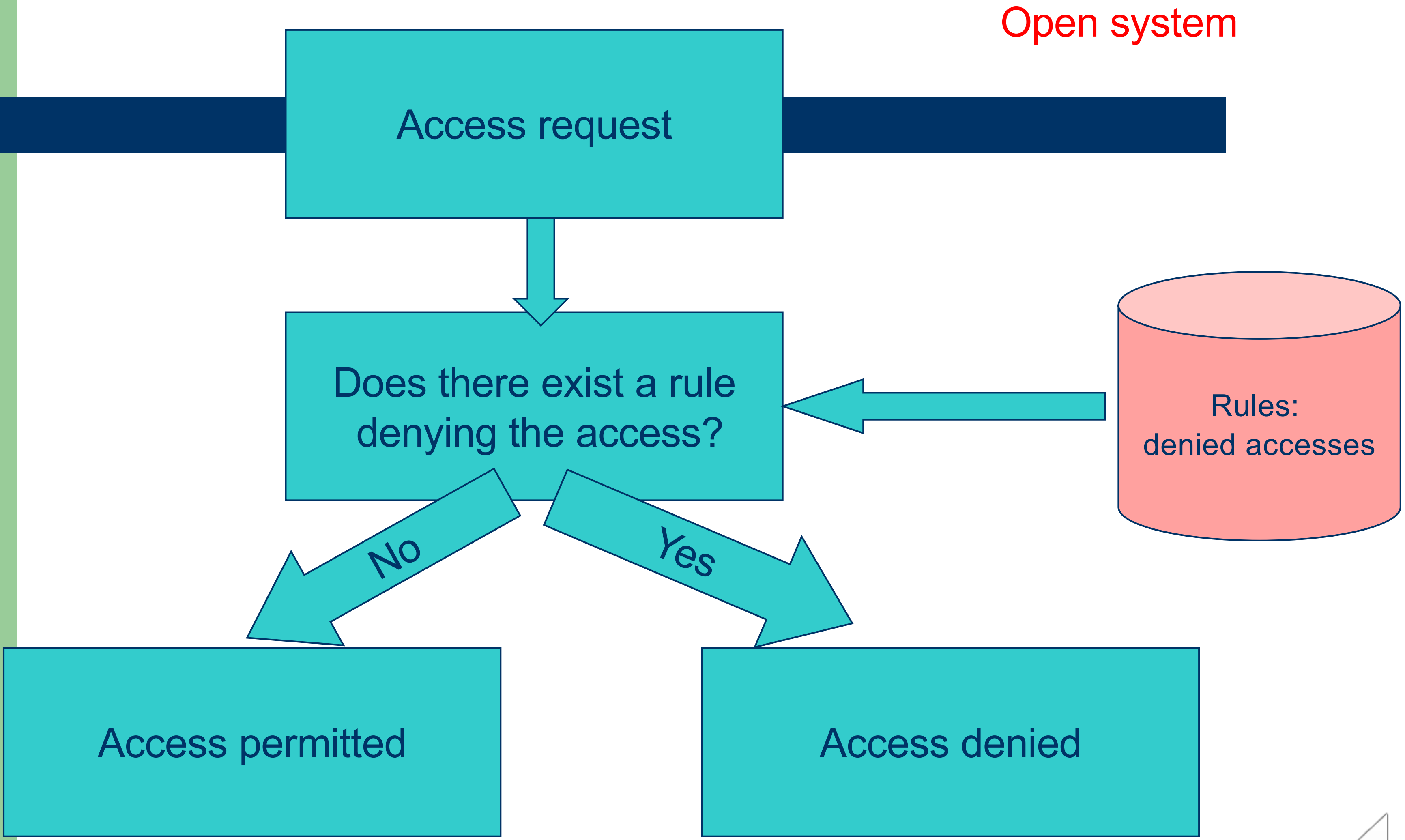
16

Exercise: Open & Close AC systems

Closed system


Access request
Does there exist a rule authorizing the access?
Rules: authorized accesses
Yes
No
Access permitted
Access denied

Exercise:
Open & Close AC systems



18

Countermeasures
Access Control & Flow Control

- **DAC**: granting access to the data on the basis of users' identity and of rules that specify the types of access each user is allowed for each object in the system
- Identification & authentication: 1st procedure
  - Identification: a user claims who s/he is
  - Authentication: establishing the validity of this claim
    - something the user *knows* (e.g., a password, PIN)
    - something the user *possesses* (e.g., an ATM card)
    - something the user *is* (e.g., a voice pattern, a fingerprint)

DAC - Access matrix model

- Authorization state: Q=(S,O,A)
- For DBs, A[s,o] also includes conditions that must be satisfied in order for s to exercise the access modes
- Possible conditions: data-dependent (sal<1000), time-dependent (8:00am-5:00pm), context-dependent ("name-salary" pair is prohibited), history-dependent, …

	O1	…	Oi	…	Om
S1	A[s1,o1]		A[s1,oi]		A[s1,om]
…					
Si	A[si,o1]		A[si,oi]		A[si,om]
…					
Sn	A[sn,o1]		A[sn,oi]		A[sn,om]

DAC - Access matrix model

	asset 1	asset 2	file	device
Alice	read, write, execute, own	execute	read	write
Bob	read	read, write, execute, own		

DAC - Access matrix model

- Model implementation:
  - S→ {(O,A)}: capability list
  - O→{(S,A)}: ACL (access control list)
    - each entry in the list specifies a subject and operation(s): for example, the entry (Alice, delete) on the ACL for file X gives Alice permission to delete file X
- Advantages & disadvantages of the two above & the model?
  - Capability list: compute a set of subjects granted access on a given object → all lists must be gone through
  - ACL: find all objects a subject can access
  - The model’s pros & cons: homework

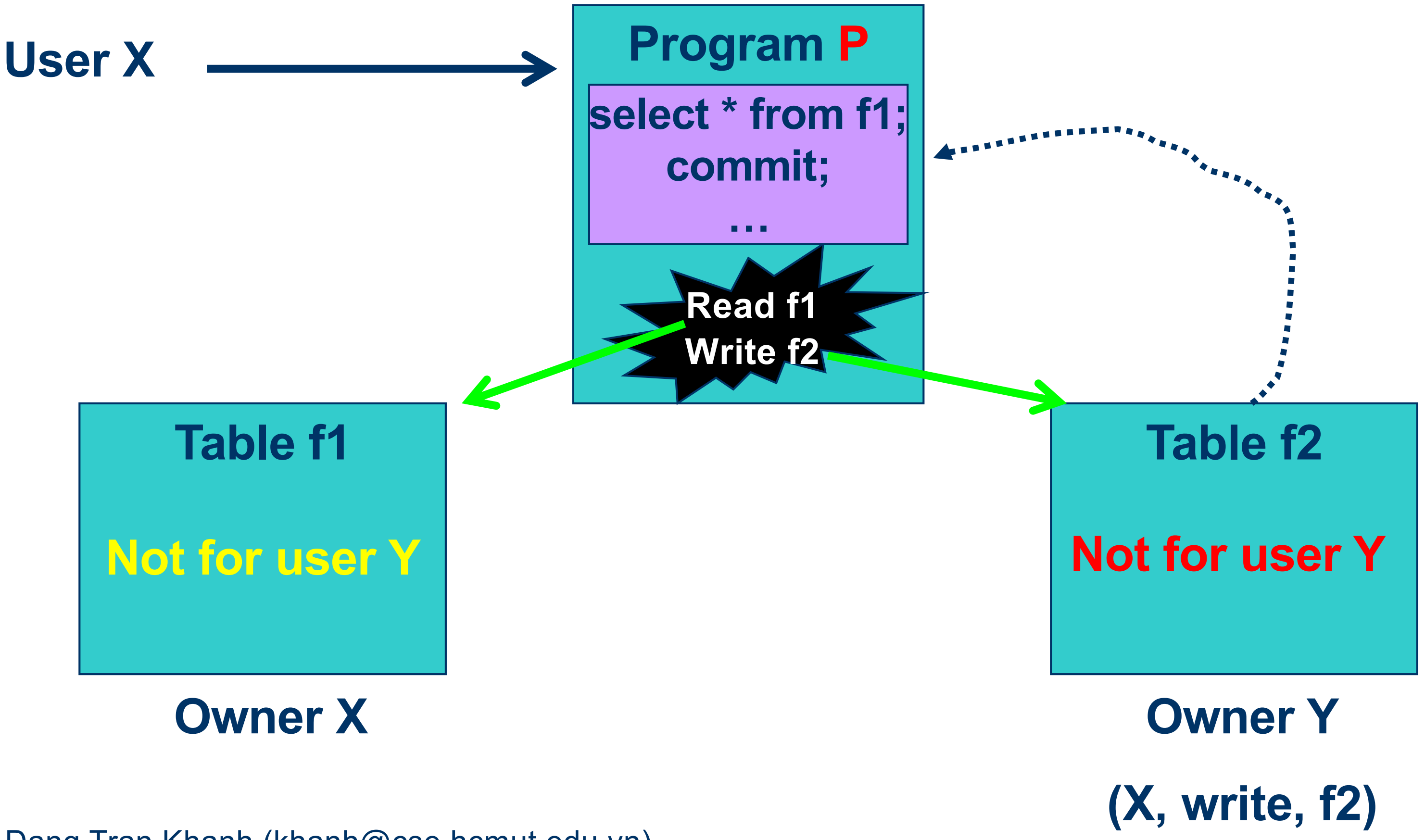
Countermeasures

Access Control & Flow Control

- DAC weakness: dissemination of information is not controlled → vulnerable to Trojan Horses

DAC (Discretionary Access Control)

Example of a Trojan Horse



Dr. Dang Tran Khanh (khanh@cse.hcmut.edu.vn)

DAC (cont.)

- The typical method of enforcing DAC in a database system is based on the granting and revoking privileges
- SQL standard supports DAC through the GRANT and REVOKE commands: The GRANT command gives privileges to users, and the REVOKE command takes away privileges
- Details: see chapter 30 [1] and the Web

SQL for Data Control

- Commands:
  - GRANT
  - REVOKE
- Based on three central objects:
  - Users
  - Database objects
  - Privileges: select, insert, update, delete, reference

GRANT

- Function: to specify privileges for users on database objects

```
GRANT <privilege list>
ON        <relation or view>
TO        <user list>
```

```
GRANT     SELECT, INSERT
ON        Employee
TO        khanh
```

```
GRANT     UPDATE(Designation)
ON        Employee
TO        khanh, someone
```

GRANT

- The SQL references privilege is granted on specific attributes (as for update). This allows a user to create relations that reference an attribute (key) of a relation as foreign key

```
GRANT  REFERENCES(Emp_No)
ON     Employee
TO     khanh
```

REVOKE

- Function: Remove privileges from users on database objects

```
REVOKE <privilege list>
ON       <relation or view>
FROM     <user list>
```

```
REVOKE  SELECT, UPDATE(Designation)
ON      Employee
FROM    khanh
```

Outline

- Introduction to DB Security
  - Oracle as an example
- Basic Countermeasures
  - Access Control:
    - DAC (Discretionary Access Control)
    - MAC (Mandatory Access Control)
    - RBAC (Role based Access Control)
  - Flow Control
  - Inference Problem
  - Encryption
- Reading Suggestion
  - [1]: Chapter 30
  - www.oracle.com

MAC (Mandatory Access Control)

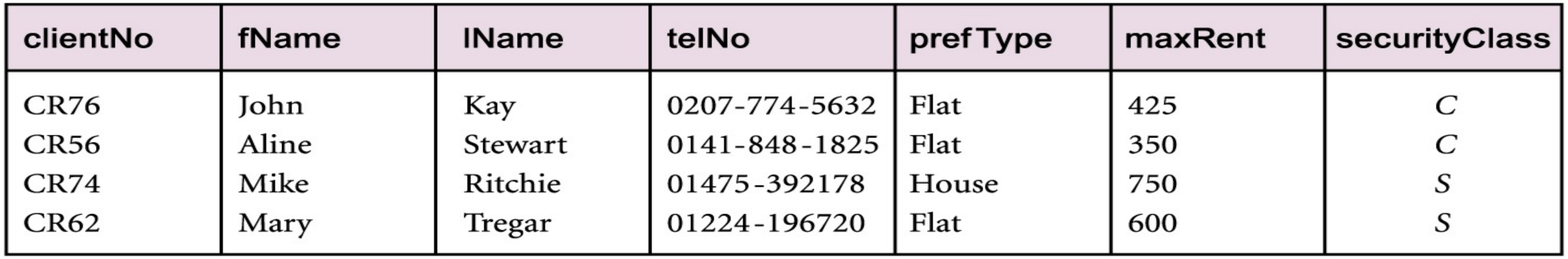
- Granting access to the data on the basis of users' clearance level and the sensitivity level of the data
- Bell-LaPadula's two principles: no read-up & no write-down secrecy
  - Data confidentiality, but Integrity

Bell-LaPudula Model

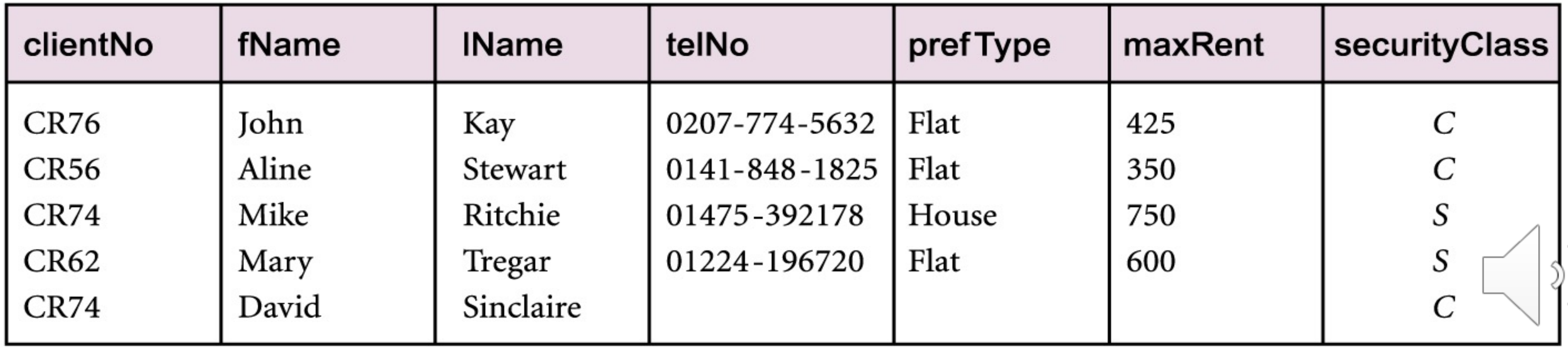
- Typical **security classes** are top secret (TS), secret (S), confidential (C), and unclassified (U), where TS is the highest level and U is the lowest one: TS ≥ S ≥ C ≥ U
- Two restrictions are enforced on data access based on the subject/object classifications:

  A subject S is not allowed read access to an object O unless class(S) ≥ class(O). This is known as the **simple security property**

  A subject S is not allowed to write an object O unless class(S) ≤ class(O). This known as the **star property** (or * property)



clientNo	fName	lName	telNo	prefType	maxRent	securityClass
CR76	John	Kay	0207-774-5632	Flat	425	*C*
CR56	Aline	Stewart	0141-848-1825	Flat	350	*C*
CR74	Mike	Ritchie	01475-392178	House	750	*S*
CR62	Mary	Tregar	01224-196720	Flat	600	*S*



clientNo	fName	lName	telNo	prefType	maxRent	securityClass
CR76	John	Kay	0207-774-5632	Flat	425	*C*
CR56	Aline	Stewart	0141-848-1825	Flat	350	*C*
CR74	Mike	Ritchie	01475-392178	House	750	*S*
CR62	Mary	Tregar	01224-196720	Flat	600	*S*
CR74	David	Sinclaire				*C*

MAC (cont.)

- In general, each attribute A is associated with a **classification attribute** C in the schema
- In addition, in some models, a **tuple classification** attribute TC is added to the relation attributes to provide a classification for each tuple as a whole. Hence, a **multilevel relation** schema R with n attributes would be represented as

  $R(A_1,C_1,A_2,C_2, \ldots, A_n,C_n,TC)$

  where each C_i represents the classification attribute associated with attribute A_i
- An interesting issue: covert channel
- More details: see references

MAC (Mandatory Access Control)

- Just a few number of efforts reported on investigating mandatory security for emerging DMSs: why??
  - Strict
  - The SQL standard does not include support for MAC
- www.oracle.com

Outline

- Introduction to DB Security
  - Oracle as an example
- Basic Countermeasures
  - Access Control:
    - DAC (Discretionary Access Control)
    - MAC (Mandatory Access Control)
    - RBAC (Role based Access Control)
  - Flow Control
  - Inference Problem
  - Encryption
- Reading Suggestion
  - [1]: Chapter 30
  - www.oracle.com

RBAC (Role-Based Access Control)

- RBAC emerged rapidly in the 1990s as a proven technology for managing and enforcing security in large-scale enterprise systems
- Its basic notion is that permissions are associated with roles, and users are assigned to appropriate roles
- Roles can be created using the CREATE ROLE and DESTROY ROLE commands. Similarly to DAC, the GRANT and REVOKE commands can then be used to assign and revoke privileges from roles

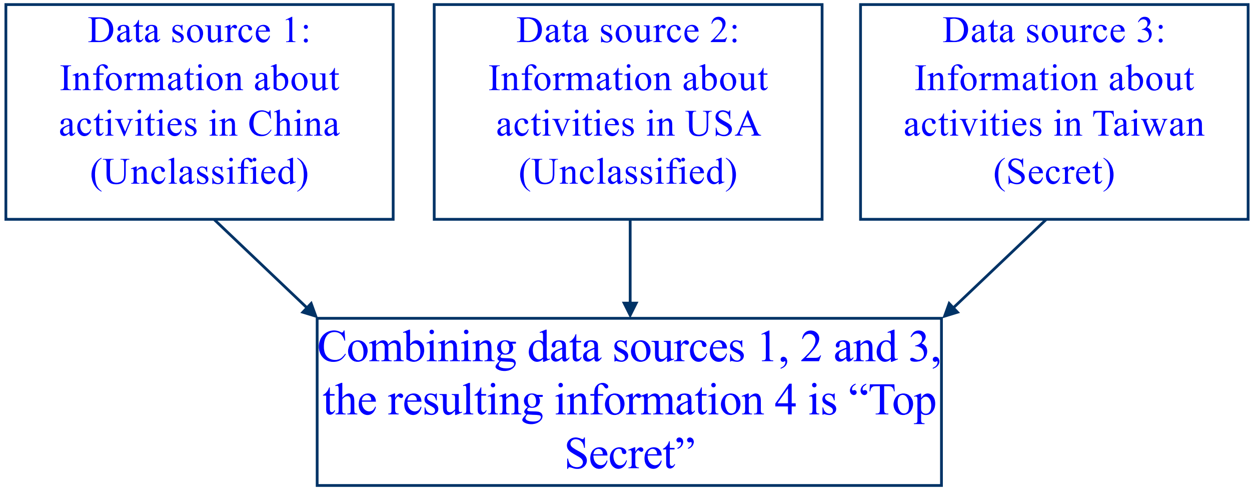
Outline

- Introduction to DB Security
  - Oracle as an example
- Basic Countermeasures
  - Access Control:
    - DAC (Discretionary Access Control)
    - MAC (Mandatory Access Control)
    - RBAC (Role based Access Control)
  - Flow Control
  - Inference Problem
  - Encryption
- Reading Suggestion
  - [1]: Chapter 30
  - www.oracle.com

Countermeasures

Inference Problem

- Inference problem:
  - Inference is the process of posing queries and deducing new information from the returned results
  - **Statistical DBs**: aggregate query results do not divulge individual's information
  - MLS/DBMSs: multilevel/mandatory security DBMSs



Data source 1: Information about activities in China (Unclassified)

Data source 2: Information about activities in USA (Unclassified)

Data source 3: Information about activities in Taiwan (Secret)

Combining data sources 1, 2 and 3, the resulting information 4 is "Top Secret"

  - Two main approaches: based on security constraints and conceptual structures

Countermeasures

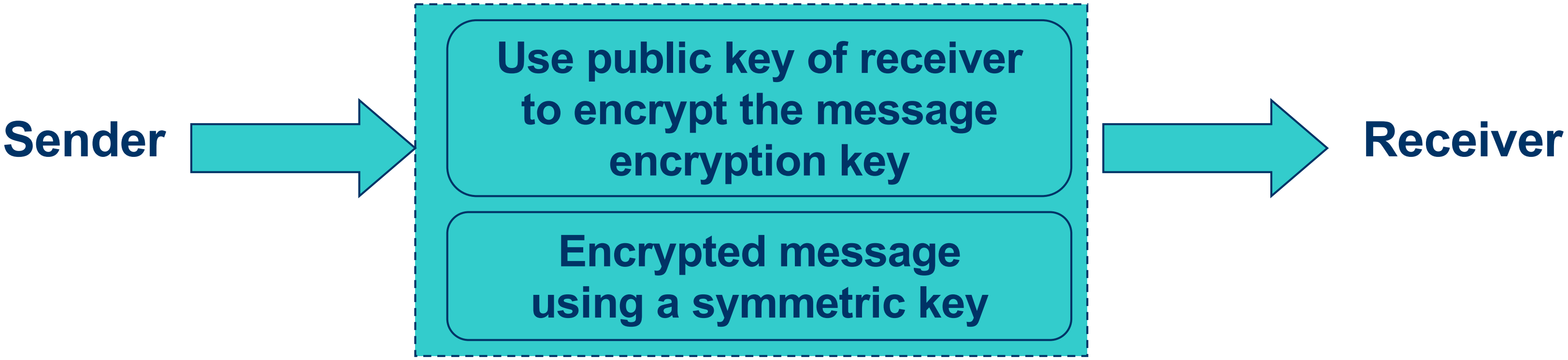
Encryption

- The encoding of the data by a special algorithm that renders the data unreadable by any program without the decryption key
- Symmetric cryptography: sender and receiver use the same key
- Asymmetric cryptography: encryption & decryption keys
- Oracle: TDE-transparent data encryption

Countermeasures

Encryption

- Encryption key: public key
- Decryption key: private key
- Asymmetric techniques: more secure but expensive in terms of computational costs

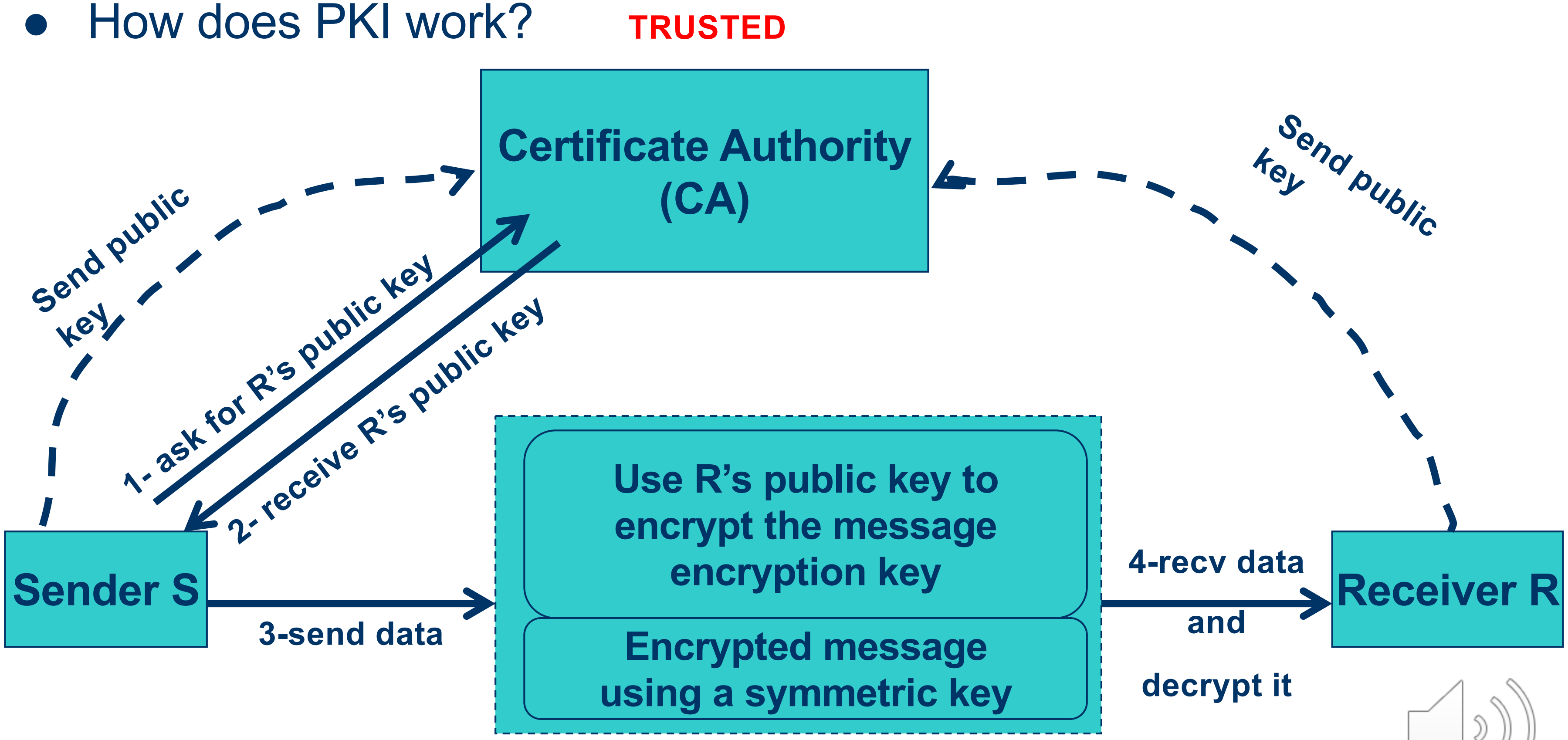

Sender
Use public key of receiver to encrypt the message encryption key
Encrypted message using a symmetric key
Receiver

→ How to obtain receiver's public key?

→ How to ensure that the message has not been tampered with by someone else?

Encryption & PKI (Public Key Infrastructure)

- How does PKI work?



TRUSTED
Certificate Authority (CA)
Send public key
Send public key
1- ask for R's public key
2- receive R's public key
Sender S
3-send data
Use R's public key to encrypt the message encryption key
Encrypted message using a symmetric key
4-recv data and decrypt it
Receiver R

Outline

- Introduction to DB Security
  - Oracle as an example
- Basic Countermeasures
  - Access Control:
    - DAC (Discretionary Access Control)
    - MAC (Mandatory Access Control)
    - RBAC (Role based Access Control)
  - Flow Control
  - Inference Problem
  - Encryption
- Reading Suggestion
  - [1]: Chapter 30
  - www.oracle.com

Summary

- Introduction to DB Security
  - Oracle as an example
- Basic Countermeasures
  - Access Control: DAC, MAC, RBAC
  - Flow Control
  - Inference Problem
  - Encryption

Q&A

Questions ??