IN3020/IN4020 – Database Systems Spring 2021, Week 16.2

Security in & with DBMS

(Elmasri & Navathe, Ch. 30 + slides)

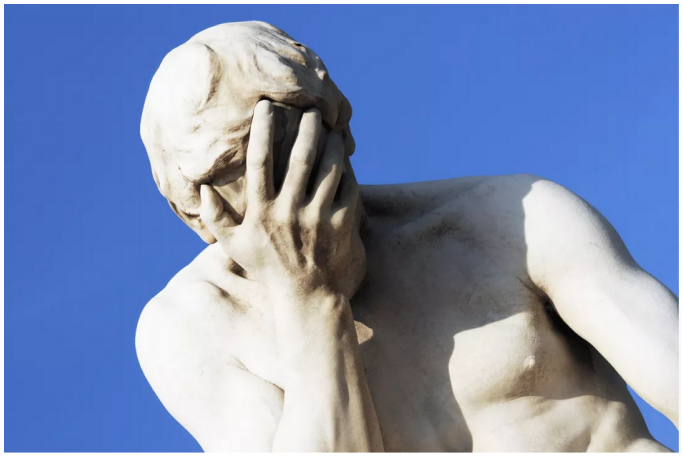
Dr. M. Naci Akkøk

CEO, In-Virtualis, Assoc. Prof. UiO/Ifi, Assoc. Prof. OsloMet/CEET

UiO : Institutt for informatikk
Det matematisk-naturvitenskapelige fakultet

While we are trying to …

- Ensure data consistency & durability …
- Avoid “wrong” reads and writes …
- Protect user accounts & info …
- We also have
  - The infamous data breach “hall of shame”
  - And the most recent one is the case of the Norwegian Parliament



https://www.cnet.com/news/2019-data-breach-hall-of-shame-these-were-the-biggest-data-breaches-of-the-year/

Goals vs. Cybercrime (examples)

Confidentiality (data disclosure)

- Unauthorized persons must not be able to see data they are not to have access to

Integrity (data change/trust)

- Data must be accurate and reliable. Therefore, data must be protected against changes by unauthorized “users”

Availability (data access/availability)

- Users must be able to view or modify their data

Data breach

- Data is compromised, stolen or altered

System hijacking

- Ransomware

Denial of Service

- Take a service down

Common concepts, regulations

- Data privacy laws, GDPR
- National security laws & related regulations

- Why do we store data?
- What is the purpose?
- Is processing inline with defined purpose?
- Legal base for processing?
- Proper RISK assessment…

- Who has accessed data, when & why, and how is the access used?

To protect the data, we need to protect more than the DBMS

Security is a comprehensive task because security can be compromised at all levels & in all components of a system [client(s), server(s), network components, etc.]

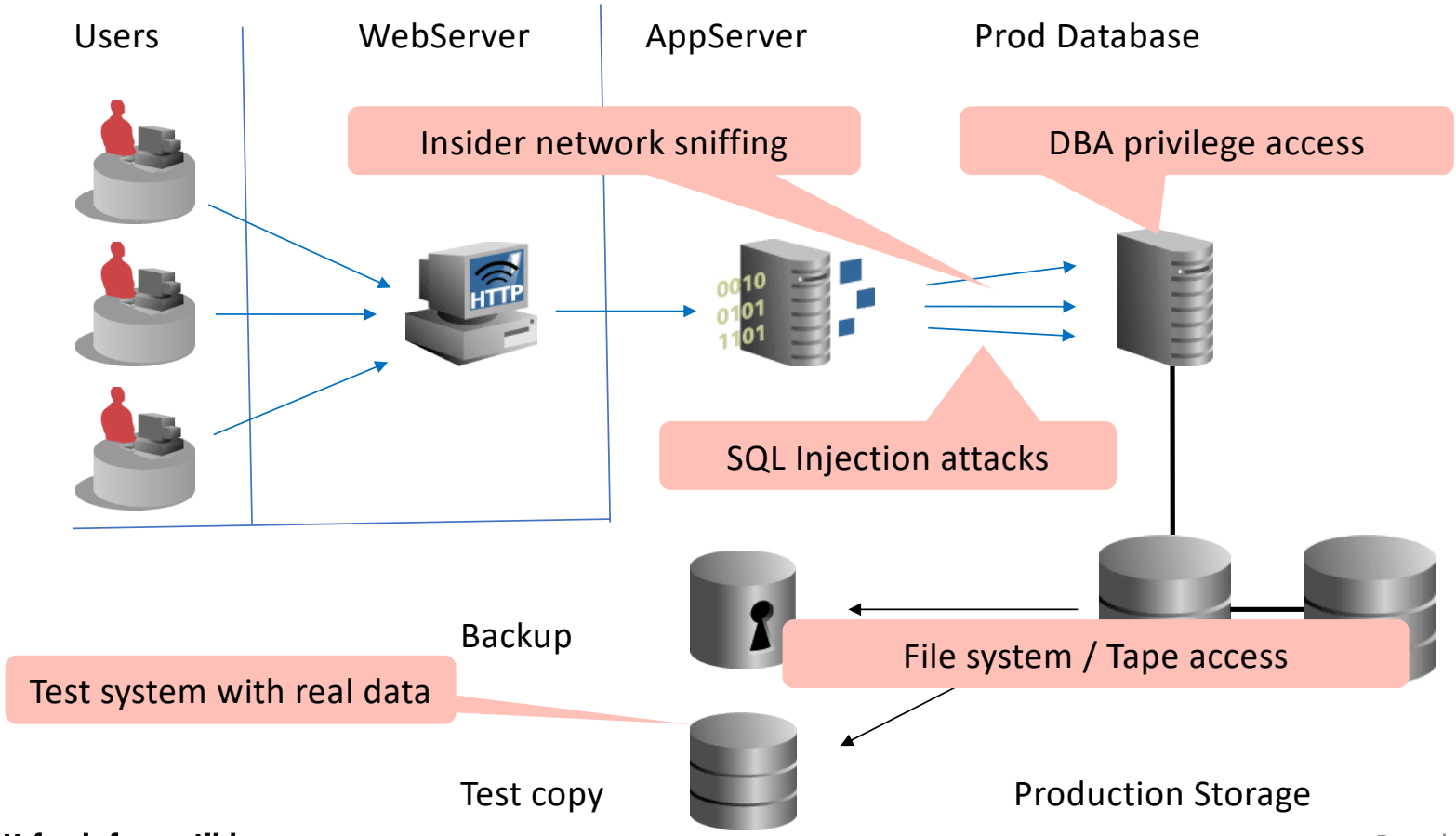
We must secure each individual component and the interaction between them.

Remember:
Data and the data store is almost always the goal!

Key concepts (and components) of security

- **Need-to-now:** You only have access to data required to fulfill your job role.
- **Least privilege:** You only have been granted the privileges required to fulfill a task.
- **Privilege creep:** As your job role changes over time, more privileges are granted. Privileges no longer needed is never revoked!
- **Governance and access control:** System and function that is responsible for granting/revoking access rights.
- **Role Based Access Control, RBAC:** Logical container that contains group of access rights. By granting the role and not the individual access rights, governance and administration is made simpler.
- **Attribute Based Access Control, ABAC:** Based on dynamic attributes like current time of day, current location, access rights or access roles are granted or revoked

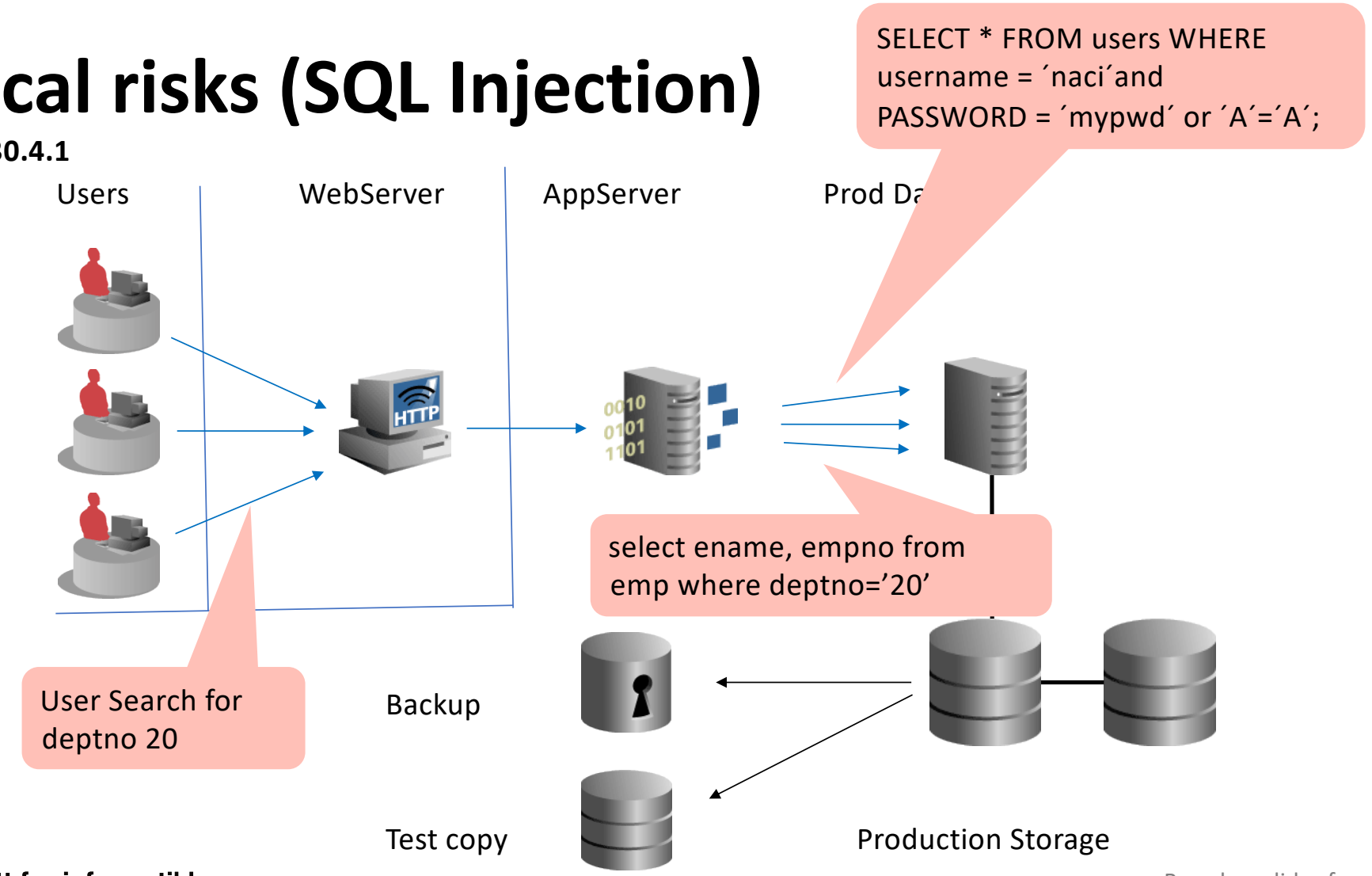
Typical risks



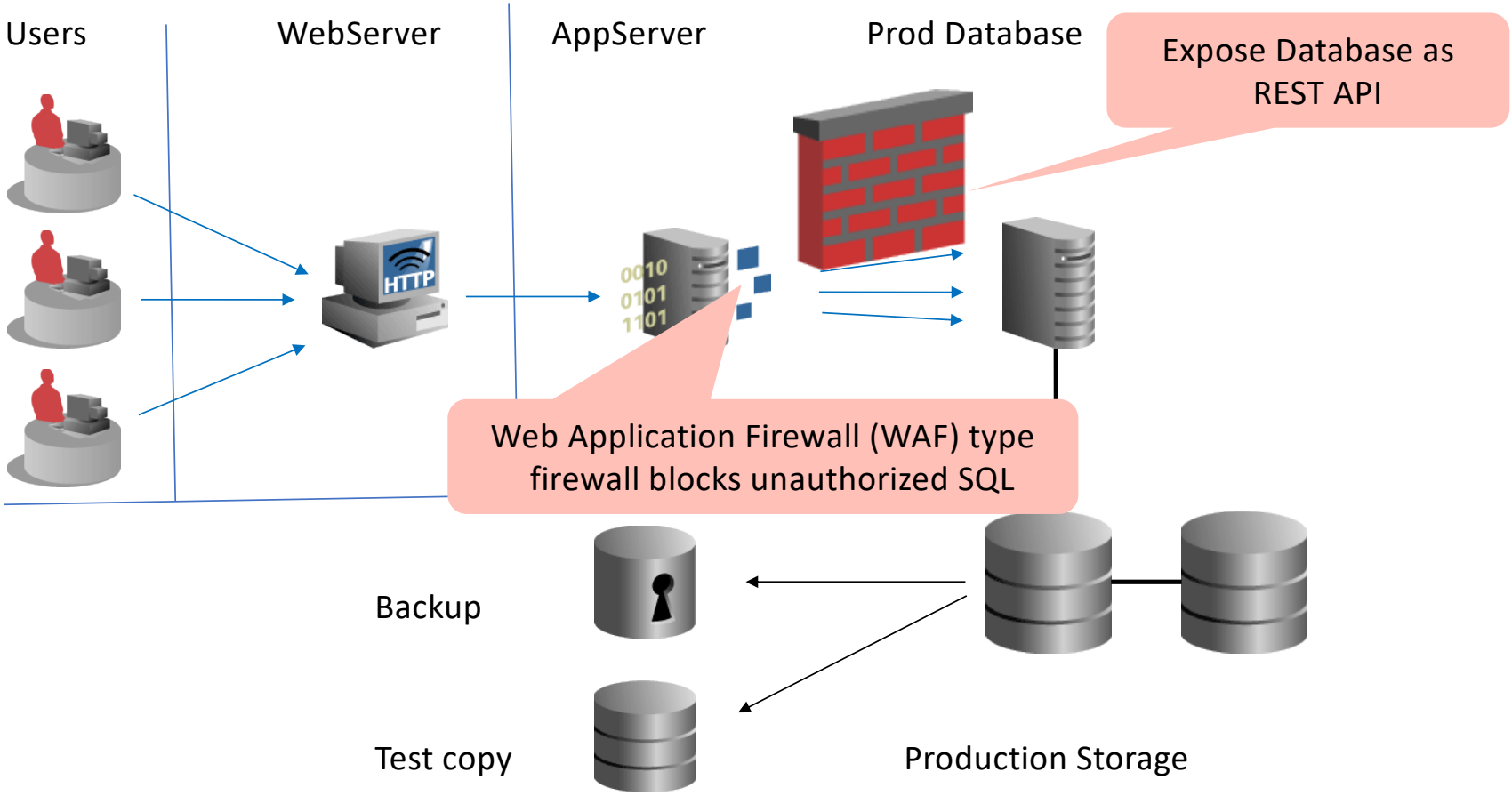
Based on slides from Inge Os
Oracle, 2020

Typical risks (SQL Injection)

See E&N 30.4.1

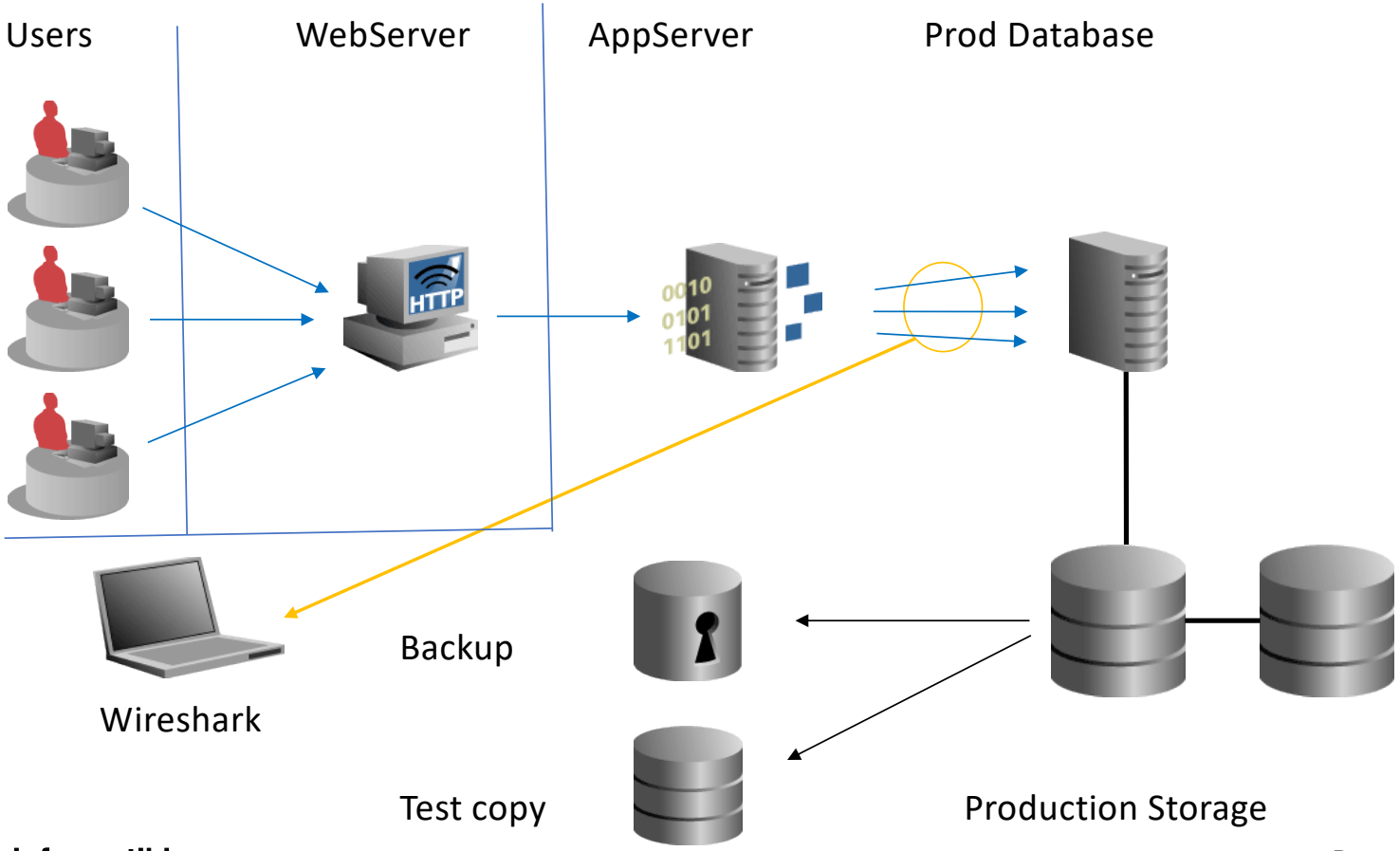


Typical risks (SQL Injection protection)



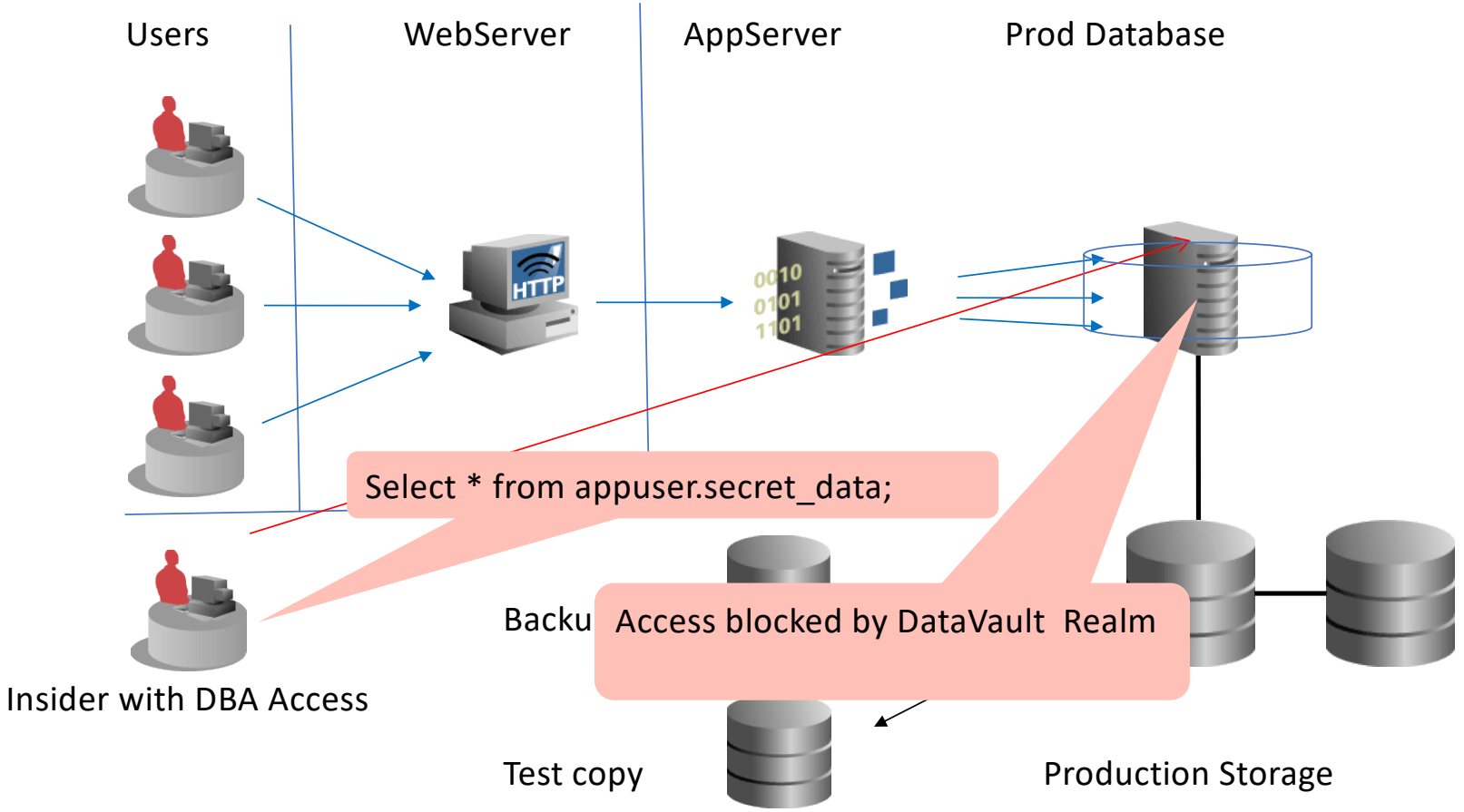
Based on slides from Inge Os
Oracle, 2020

Typical risks (DB traffic “sniffing”)



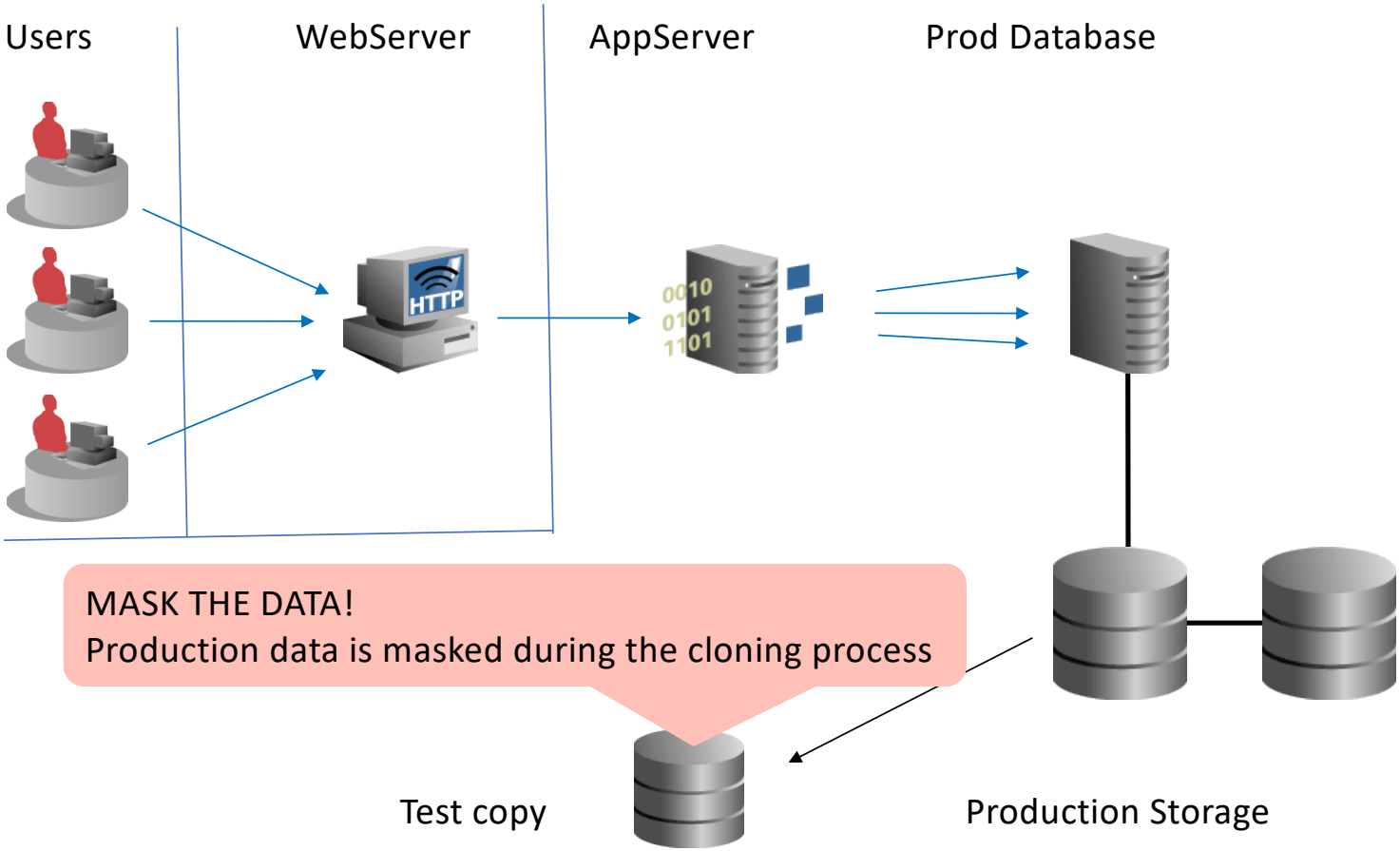
Based on slides from Inge Os
Oracle, 2020

Typical risks (Privileged account)



Based on slides from Inge Os
Oracle, 2020

Typical risks (Test systems, masking)



Based on slides from Inge Os
Oracle, 2020

Role of the DBA in DB Security

- Make data available at the right time to the right person/role, while maintaining SECURITY at all levels for all!

  (Not the easiest thing to do)

Role of the DBA in DB Security

- Keep track of security: I.e., keep track of
  - **accounts**,
  - **privileges**,
  - **security levels,**
  - **data sensitivity** (Navathe & Elmasri ch. 30.1)
- Authentication
- Role & identity management,
- Logs & Database audits

Information security vs. privacy

- **Information security**
  - Protecting data, information, and the whole system from unauthorized use, from **unauthorized access**
- **Information privacy**
  - More than security
  - Personal information is private!
  - How is personal data accessed? By whom? **How is it used or can be used?**

Access control

- **Privileges (E&N 30.2.1)**
  - Two levels:
    - Account level
    - Relation (table level)

    - There are other (finer) levels specific to some DBMS

Label based security & row-level access control

- Most major DBMS´ offer the possibility
- Fine grained as compared to account/table levels
- Each data row is given a label with info about its sensitivity, access restrictions etc.

Security classes

- Security is often “graded” using security classes
  - Top secret
  - secret
  - confidential
  - unclassified

(see E&N 30.3 mandatory access control and multilevel security)

Role/identity management

- Don´t forget that forgetting to revoke access and/or privileges from each DB and all levels & roles etc. is a security breach!
- There are tools (identity/role management tools, access control tools) that manage all access, roles & rights and make sure that everything or the correct ones are revoked

Many methods of protection

- Encryption, DES (Data Encryption Standard) – valid for data & communication and anything relevant
- Symmetric key algorithms. Same key for enc./dec. Fast.
- Public (asymmetric) key encryption. Must exchange the common key in a secure manner. Two keys (one public, one private, one for encryption, one for decryption)
- Digital signatures
- Digital certificates (requires a certification authority)

Challenges

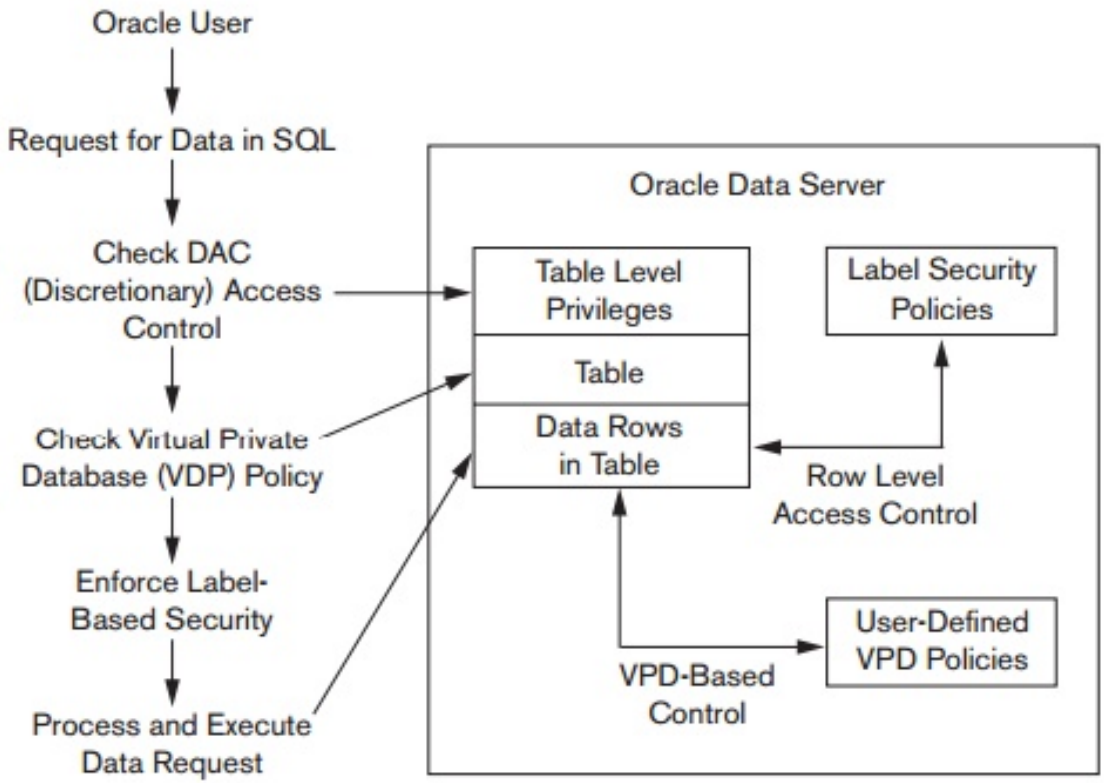
- Data quality, ETL / ELT
- IPR (Intellectual Property Rights), legal information
- DB survivability (E&N 30.9.3) – do the following:
  - Confinement
  - Damage assessment
  - Reconfiguration
  - Repair
  - Fault treatment

Oracle label-based security (E&N ch. 30.10)

- Unique to Oracle
- Restricting access to larger units of data (tables) and isolating data into separate databases are costly
- Oracle provides finer (row-level) access control

Oracle label-based security architecture

VPD: Virtual Private Database

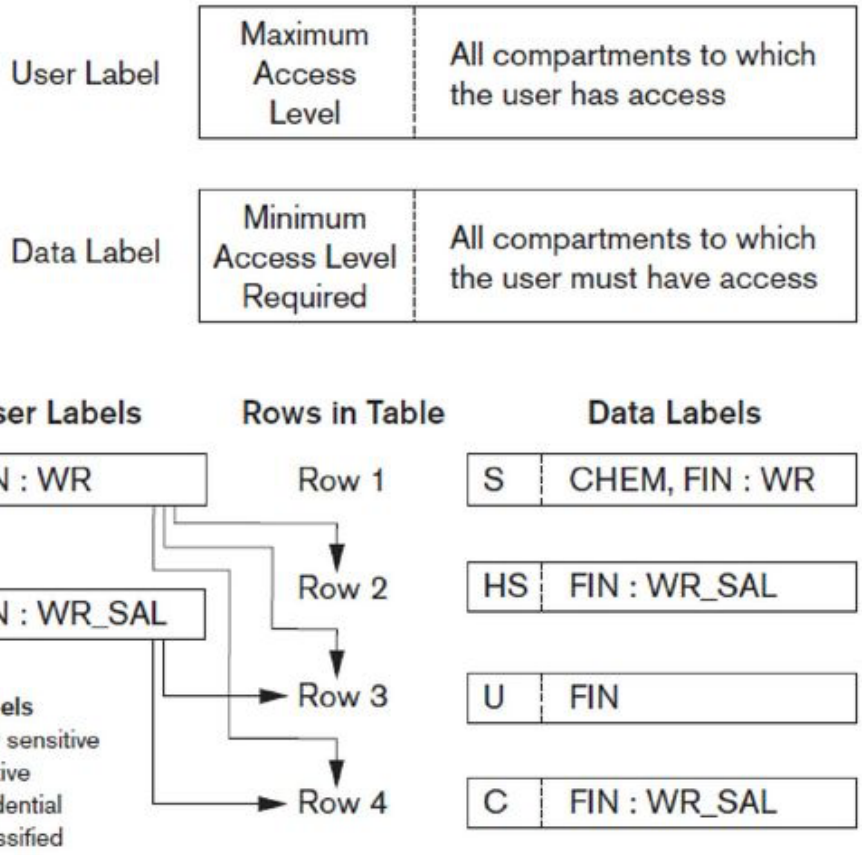


E&N Figure 30.4

Oracle Label Security architecture.

Source: Oracle (2007)

Oracle data labels & user labels



E&N Figure 30.5
Data labels and user labels in Oracle

Data from :Oracle (2007)

Reminder: Seminar, Friday 30. April 2021

- Data Science: The Bridge Between Data and Science
  - Intro to “data science” (including an understanding/memorizing technique through observing how most techniques relate to each other) – M. Naci Akkøk
  - Extensible AI: A new direction – Sagar Sen (SINTEF)
  - Oracle Machine Learning (OML) – Renée Wikestad, Oracle
  - What do data science and its “new” applications & directions require from the database management systems? – M. Naci Akkøk

Take care!

STAY SAFE, STAY HEALTHY!