OS and Database security

Dr Aftab Ali

COM398

Introduction

- Operating system security goals
- Operating system hardening
- Operating system encryption, logging and data backups and archives
- Linux/Unix and Windows security
- Virtualized and containerized infrastructure security
- Database security threats and vulnerabilities
- SQL injections
- and database access control

Operating System Security Goals

- Networked desktop computers
    - ensure secure operation in networked environment
- New threat?
    - Attackers coming from the network.
    - Network-facing programs on computers may be buggy.
    - Users may be hurt via online communication.
- Security mechanisms
    - Authentication; Access Control
    - Secure Communication (using cryptography)
    - Logging & Auditing
    - Intrusion Prevention and Detection

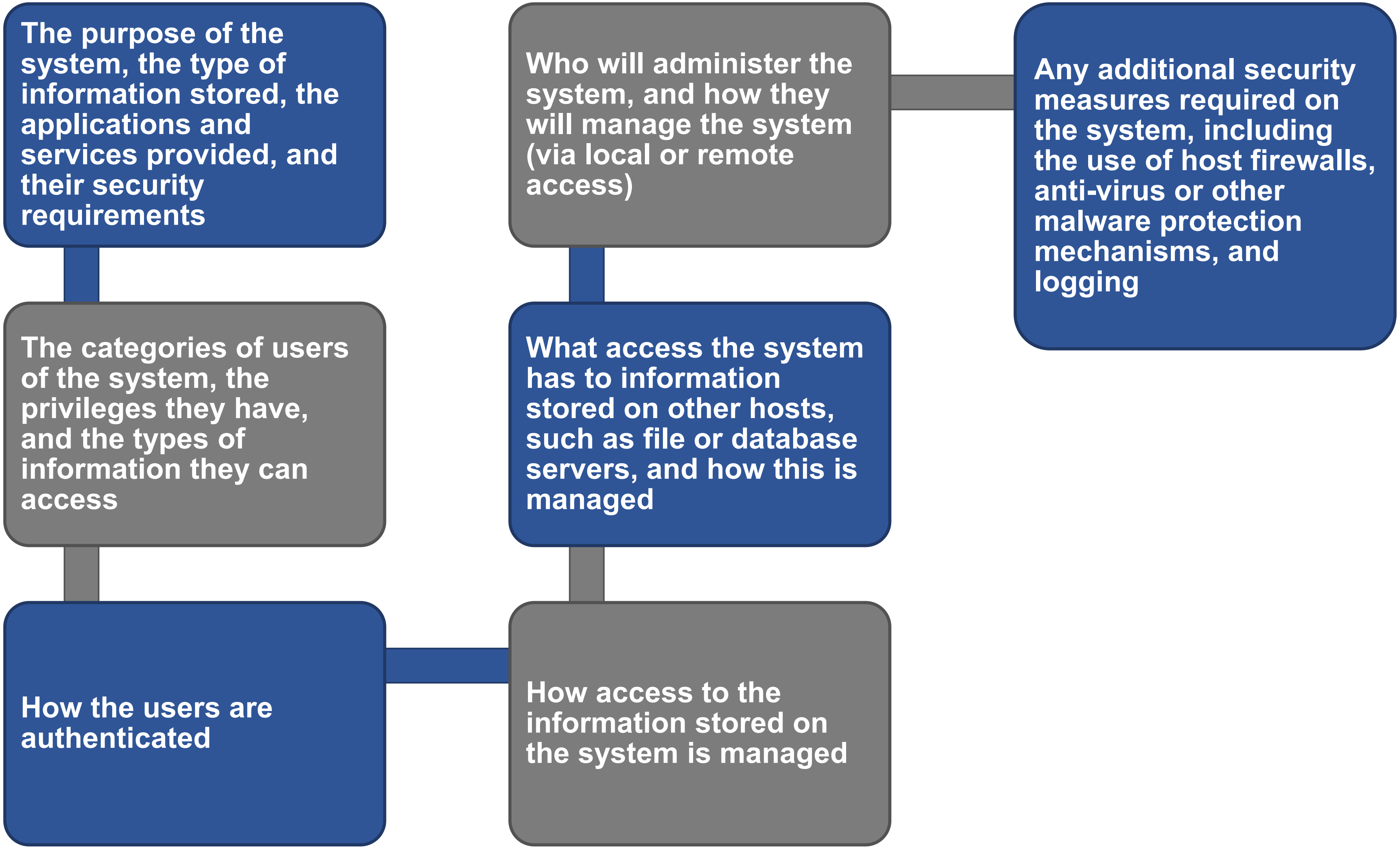
Operating System Security Goals

- Mobile computing devices:
- New threat?
  - Apps (programs) may be malicious.
  - More tightly connected with personal life of the owner.
- Security mechanisms?
  - Isolation of each app.
  - Users assess risks of apps.
  - Risk communication.

Operating Systems Hardening

- Basic steps
  - Install and patch the operating system
  - Harden and configure the operating system to adequately address the indentified security needs of the system by:
    - Removing unnecessary services, applications, and protocols
    - Configuring users, groups, and permissions
    - Configuring resource controls
  - Install and configure additional security controls, such as anti-virus, host-based firewalls, and intrusion detection system (IDS)
  - Test the security of the basic operating system to ensure that the steps taken adequately address its security needs

System Security Planning Process



The purpose of the system, the type of information stored, the applications and services provided, and their security requirements

The categories of users of the system, the privileges they have, and the types of information they can access

How the users are authenticated

How access to the information stored on the system is managed

What access the system has to information stored on other hosts, such as file or database servers, and how this is managed

Who will administer the system, and how they will manage the system (via local or remote access)

Any additional security measures required on the system, including the use of host firewalls, anti-virus or other malware protection mechanisms, and logging

Remove Unnecessary Services, Applications, Protocols

- If fewer software packages are available to run the risk is reduced
- System planning process should identify what is actually required for a given system

- When performing the initial installation the supplied defaults should not be used
  - Default configuration is set to maximize ease of use and functionality rather than security
  - If additional packages are needed later they can be installed when they are required

Configure Users, Groups, and Authentication

- Not all users with access to a system will have the same access to all data and resources on that system
- Elevated privileges should be restricted to only those users that require them, and then only when they are needed to perform a task

- System planning process should consider:
  - ○ Categories of users on the system
  - ○ Privileges they have
  - ○ Types of information they can access
  - ○ How and where they are defined and authenticated
- Default accounts included as part of the system installation should be secured
  - ○ Those that are not required should be either removed or disabled
  - ○ Policies that apply to authentication credentials configured

Configure Resource Controls

- Once the users and groups are defined, appropriate permissions can be set on data and resources
- Many of the security hardening guides provide lists of recommended changes to the default access configuration

Install Additional Security Controls

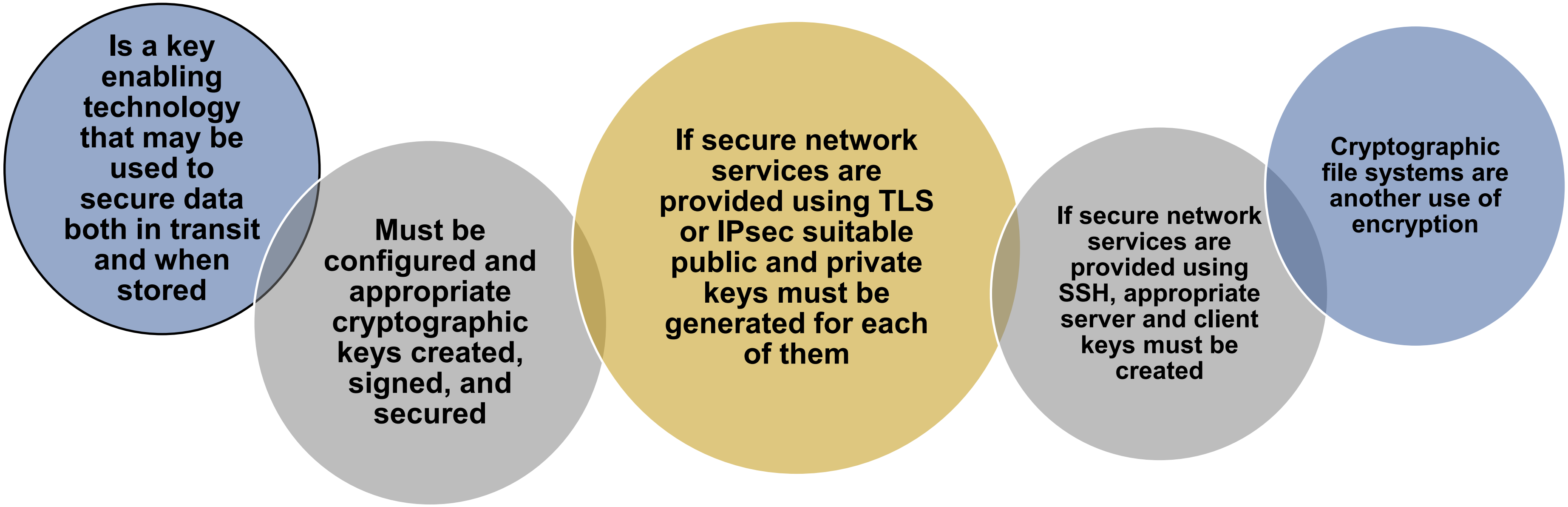
- Further security possible by installing and configuring additional security tools:
  - ○ Anti-virus software
  - ○ Host-based firewalls
  - ○ IDS or IPS software
  - ○ Application white-listing

Test the System Security

- Final step in the process of initially securing the base operating system is security testing
- Goal:
  - Ensure the previous security configuration steps are correctly implemented
  - Identify any possible vulnerabilities

- There are programs specifically designed to:
  - Review a system to ensure that a system meets the basic security requirements
  - Scan for known vulnerabilities and poor configuration practices
- Should be done following the initial hardening of the system
- Repeated periodically as part of the security maintenance process

Encryption Technology



Is a key enabling technology that may be used to secure data both in transit and when stored

Must be configured and appropriate cryptographic keys created, signed, and secured

If secure network services are provided using TLS or IPsec suitable public and private keys must be generated for each of them

If secure network services are provided using SSH, appropriate server and client keys must be created

Cryptographic file systems are another use of encryption

Security Maintenance

- Process of maintaining security is continuous
- Security maintenance includes:
  - Monitoring and analyzing logging information
  - Performing regular backups
  - Recovering from security compromises
  - Regularly testing system security
  - Using appropriate software maintenance processes to patch and update all critical software

Logging

Can only inform you about bad things that have already happened

In the event of a system breach or failure, system administrators can more quickly identify what happened

Key is to ensure you capture the correct data and then appropriately monitor and analyze this data

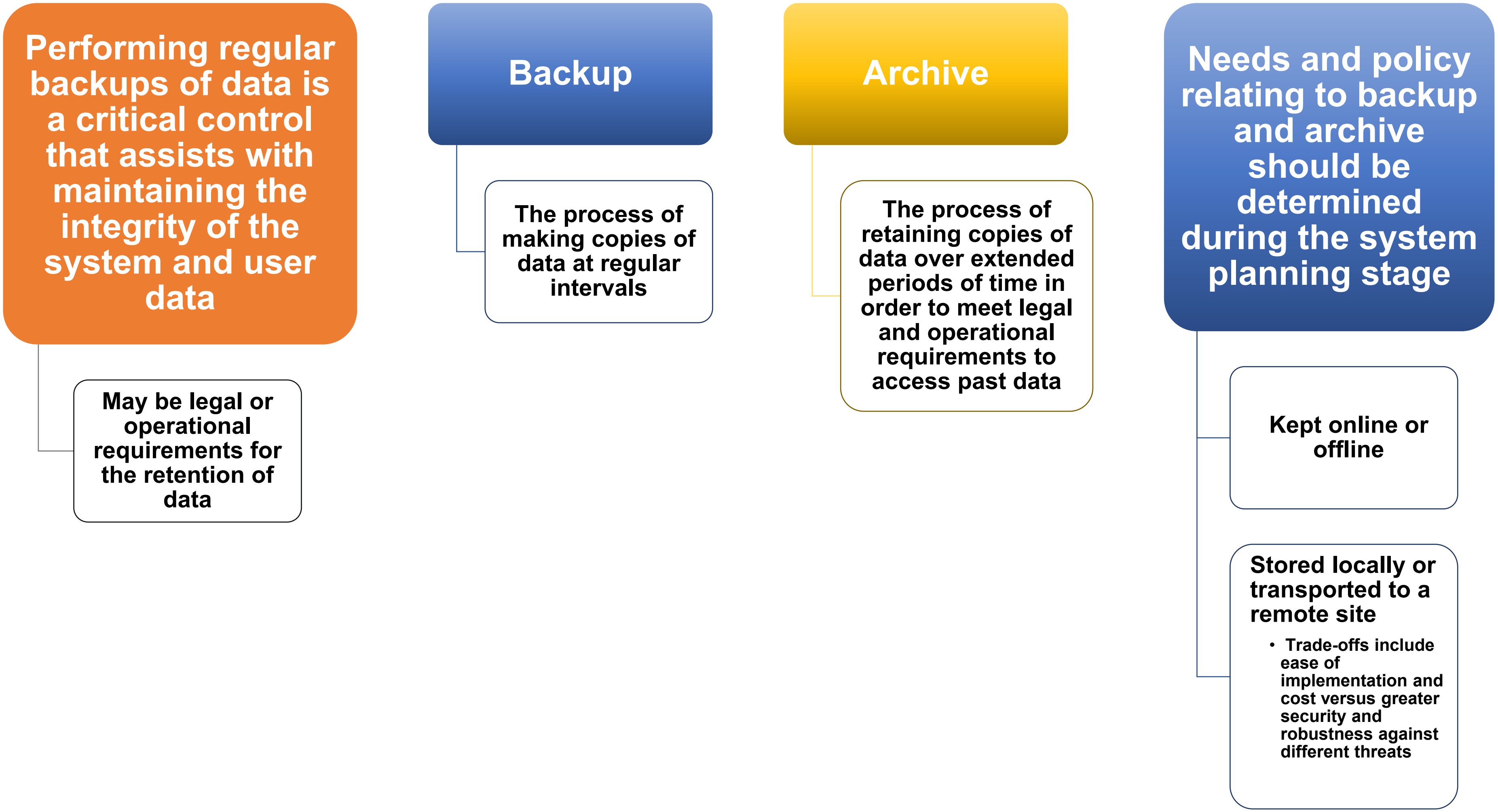
Information can be generated by the system, network and applications

Range of data acquired should be determined during the system planning stage

Generates significant volumes of information and it is important that sufficient space is allocated for them

Automated analysis is preferred

Data Backup and Archive



Performing regular backups of data is a critical control that assists with maintaining the integrity of the system and user data

May be legal or operational requirements for the retention of data

Backup

The process of making copies of data at regular intervals

Archive

The process of retaining copies of data over extended periods of time in order to meet legal and operational requirements to access past data

Needs and policy relating to backup and archive should be determined during the system planning stage

Kept online or offline

Stored locally or transported to a remote site

- Trade-offs include ease of implementation and cost versus greater security and robustness against different threats

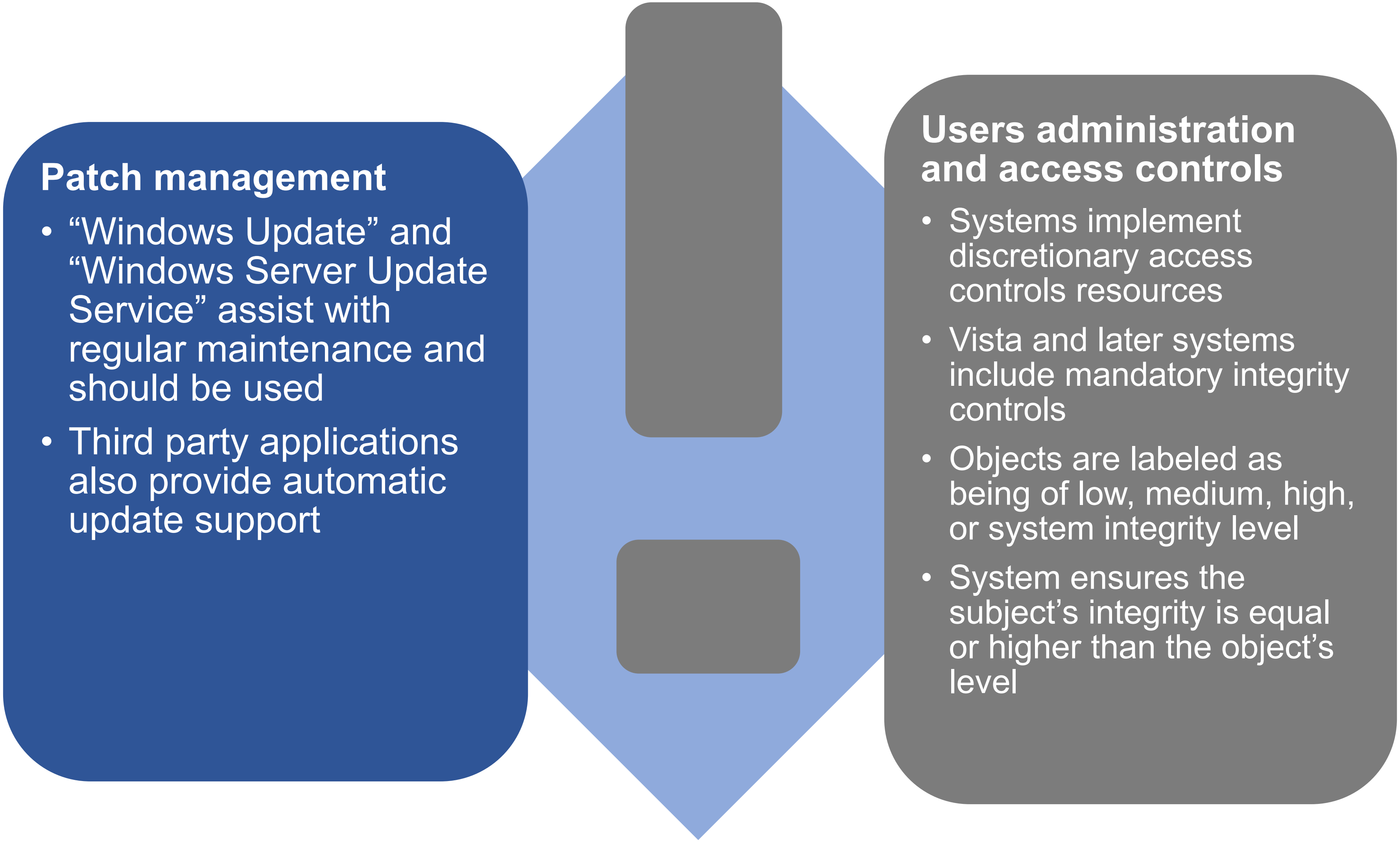
Linux/Unix Security

- Patch management
  - Keeping security patches up to date is a widely recognized and critical control for maintaining security
- Application and service configuration
  - Most commonly implemented using separate text files for each application and service
  - Generally located either in the /etc directory or in the installation tree for a specific application
  - Individual user configurations that can override the system defaults are located in hidden “dot” files in each user’s home directory
  - Most important changes needed to improve system security are to disable services and applications that are not required

Linux/Unix Security

- Users, groups, and permissions
  - Access is specified as granting read, write, and execute permissions to each of owner, group, and others for each resource
  - Guides recommend changing the access permissions for critical directories and files
  - Local exploit
    - Software vulnerability that can be exploited by an attacker to gain elevated privileges
  - Remote exploit
    - Software vulnerability in a network server that could be triggered by a remote attacker

Windows Security



Patch management

- “Windows Update” and “Windows Server Update Service” assist with regular maintenance and should be used
- Third party applications also provide automatic update support

Users administration and access controls

- Systems implement discretionary access controls resources
- Vista and later systems include mandatory integrity controls
- Objects are labeled as being of low, medium, high, or system integrity level
- System ensures the subject’s integrity is equal or higher than the object’s level

Windows Security
Users Administration and Access Controls

Windows systems also define privileges

- System wide and granted to user accounts

Combination of share and NTFS permissions may be used to provide additional security and granularity when accessing files on a shared resource

User Account Control (UAC)

- Provided in Vista and later systems
- Assists with ensuring users with administrative rights only use them when required, otherwise accesses the system as a normal user

Low Privilege Service Accounts

- Used for long-lived service processes such as file, print, and DNS services

Windows Security

Application and service configuration

- Much of the configuration information is centralized in the Registry
  - Forms a database of keys and values that may be queried and interpreted by applications
- Registry keys can be directly modified using the “Registry Editor”
  - More useful for making bulk changes

Windows Security

Other security controls

- Essential that anti-virus, anti-spyware, personal firewall, and other malware and attack detection and handling software packages are installed and configured
- Current generation Windows systems include basic firewall and malware countermeasure capabilities
- Important to ensure the set of products in use are compatible

Windows systems also support a range of cryptographic functions:

- Encrypting files and directories using the Encrypting File System (EFS)
- Full-disk encryption with AES using BitLocker

“Microsoft Baseline Security Analyzer”

- Free, easy to use tool that checks for compliance with Microsoft’s security recommendations

Virtualization

- A technology that provides an abstraction of the resources used by some software which runs in a simulated environment called a virtual machine (VM)
- Benefits include better efficiency in the use of the physical system resources
- Provides support for multiple distinct operating systems and associated applications on one physical system
- Raises additional security concerns

Hypervisor

- Software that sits between the hardware and the VMs
- Acts as a resource broker
- It allows multiple VMs to safely coexist on a single physical server host and share that host's resources
- Virtualizing software provides abstraction of all physical resources and thus enables multiple computing stacks, called virtual machines, to be run on a single physical host
- Each VM includes an OS, called the guest OS
    - This OS may be the same as the host OS, if present, or a different one

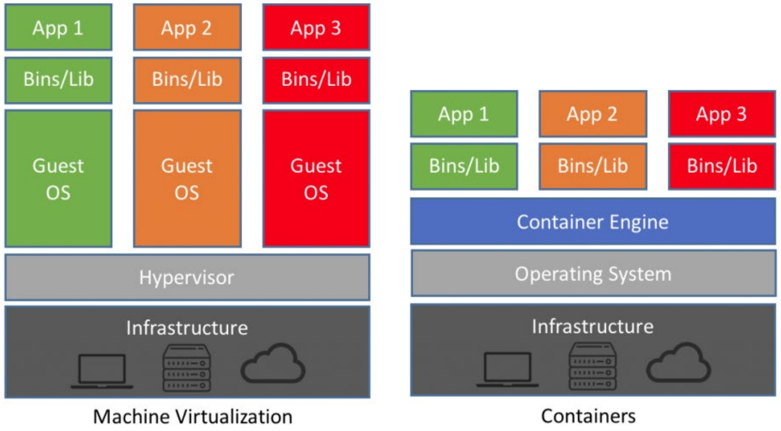
Hypervisor Functions

The principal functions performed by a hypervisor are:

- Execution management of VMs
- Devices emulation and access control
- Execution of privileged operations by hypervisor for guest VMs
- Management of VMs (also called VM lifecycle management)
- Administration of hypervisor platform and hypervisor software

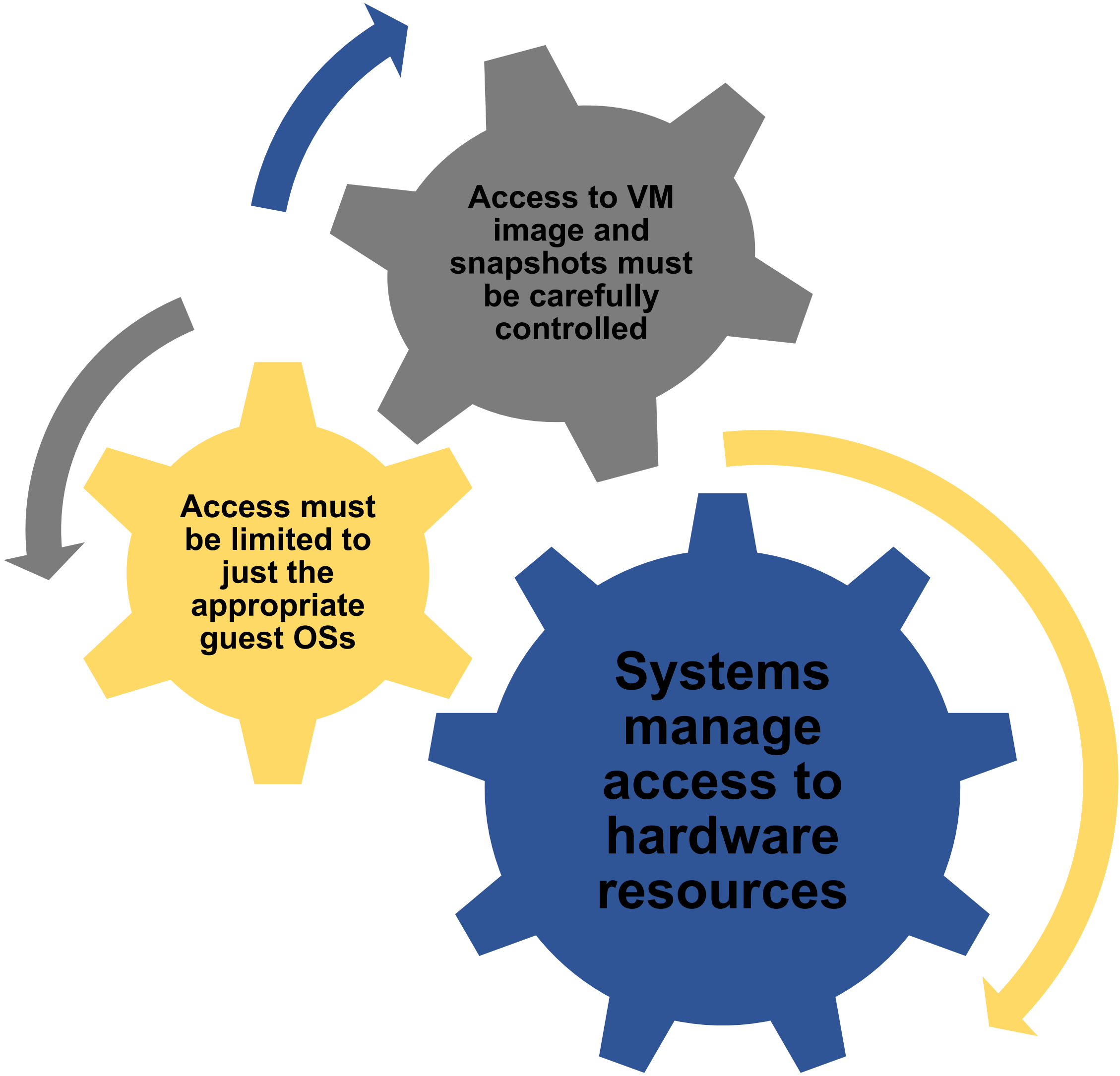
Containers

- A recent approach to virtualization is known as *container virtualization* or *application virtualization*
- In this approach, software known as a *virtualization container,* runs on top of the host OS kernel and provides an isolated execution environment for applications
- Unlike hypervisor-based VMs, containers do not aim to emulate physical servers
- All containerized applications on a host share a common OS kernel
- For containers, only a small container engine is required as support for the containers
- Containerization sits in between the OS and applications and incurs lower overhead, but potentially introduces greater security vulnerabilities



https://blog.netapp.com/blogs/containers-vs-vms/

Virtualized Infrastructure Security



Access to VM image and snapshots must be carefully controlled

Access must be limited to just the appropriate guest OSs

Systems manage access to hardware resources

Database Security

Database

- Structured collection of data stored for use by one or more applications
- Contains the relationships between data items and groups of data items
- Can sometimes contain sensitive data that needs to be secured
- Query language
  - Provides a uniform interface to the database for users and applications

Database management system (DBMS)

- Suite of programs for constructing and maintaining the database
- Offers ad hoc query facilities to multiple users and applications

Relational Databases

- Table of data consisting of rows and columns
    - Each column holds a particular type of data
    - Each row contains a specific value for each column
    - Ideally has one column where all values are unique, forming an identifier/key for that row
- Enables the creation of multiple tables linked together by a unique identifier that is present in all tables
- Use a relational query language to access the database
    - Allows the user to request data that fit a given set of criteria

Relational Database Elements

- Relation
  - ○ Table/file
- Tuple
  - ○ Row/record
- Attribute
  - ○ Column/field

Primary key

- Uniquely identifies a row
- Consists of one or more column names

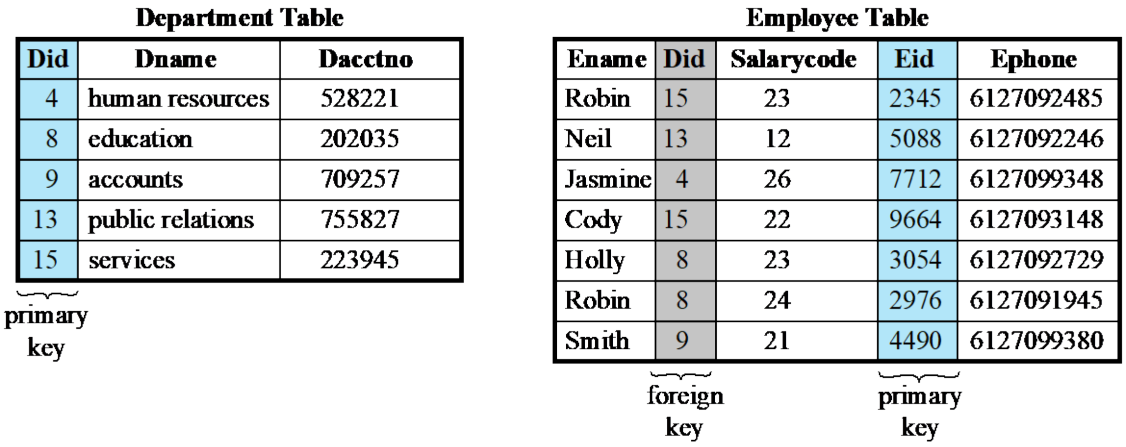
Foreign key

- Links one table to attributes in another

View/virtual table

- Result of a query that returns selected rows and columns from one or more tables
- Views are often used for security purposes

Relational Database Example



Department Table

Did	Dname	Dacctno
4	human resources	528221
8	education	202035
9	accounts	709257
13	public relations	755827
15	services	223945

primary key

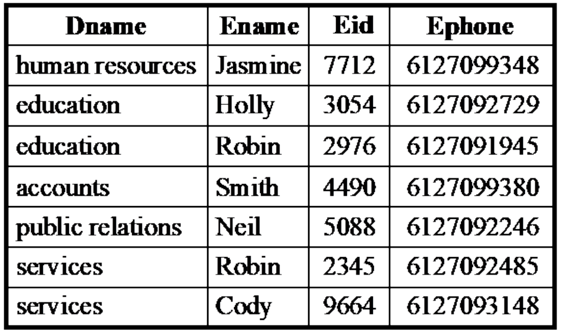
Employee Table

Ename	Did	Salarycode	Eid	Ephone
Robin	15	23	2345	6127092485
Neil	13	12	5088	6127092246
Jasmine	4	26	7712	6127099348
Cody	15	22	9664	6127093148
Holly	8	23	3054	6127092729
Robin	8	24	2976	6127091945
Smith	9	21	4490	6127099380

foreign key

primary key

(a) Two tables in a relational database



Dname	Ename	Eid	Ephone
human resources	Jasmine	7712	6127099348
education	Holly	3054	6127092729
education	Robin	2976	6127091945
accounts	Smith	4490	6127099380
public relations	Neil	5088	6127092246
services	Robin	2345	6127092485
services	Cody	9664	6127093148

(b) A view derived from the database

Structured Query Language (SQL)

- Standardized language to define schema, manipulate, and query data in a relational database
- Several similar versions of ANSI/ISO standard
- All follow the same basic syntax and semantics

SQL statements can be used to:

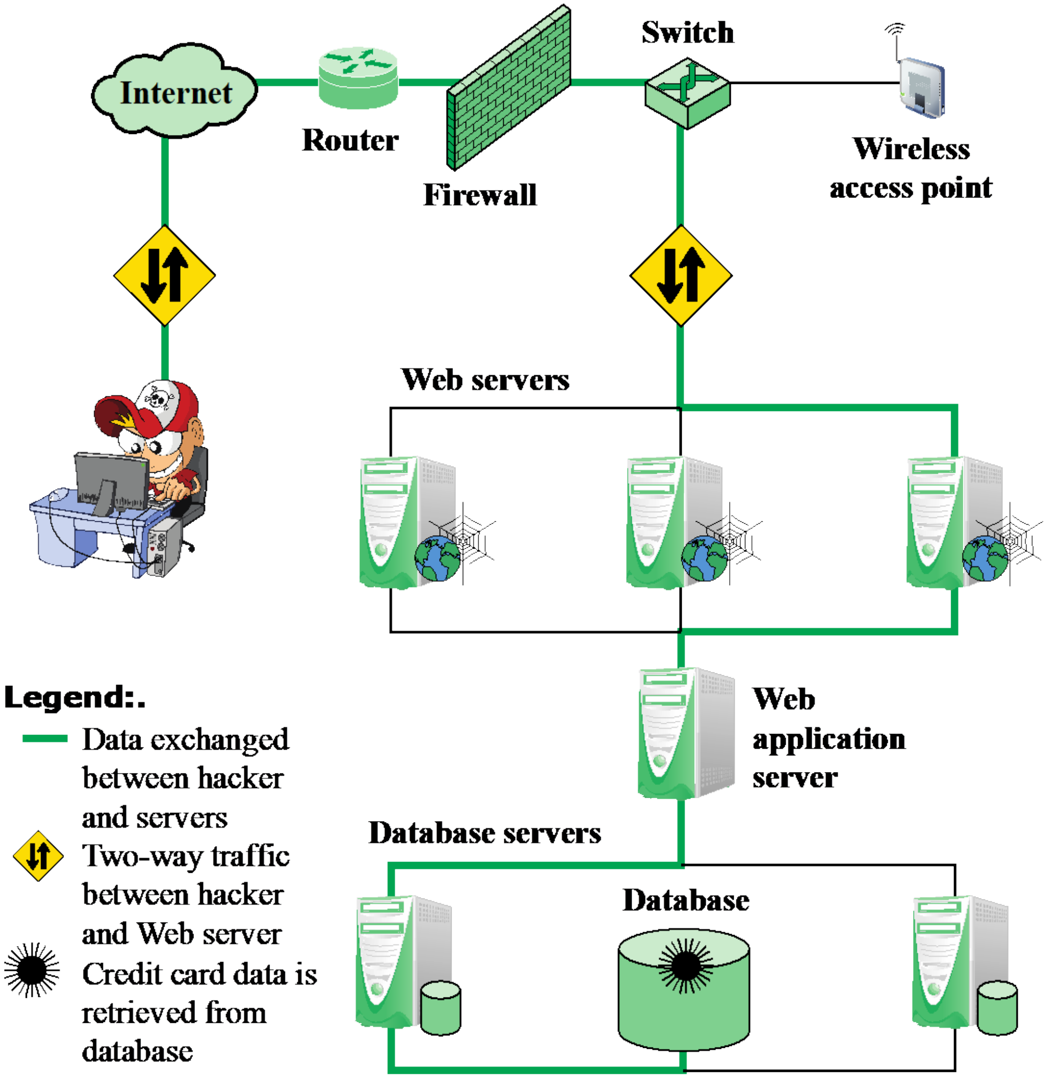
- Create tables
- Insert and delete data in tables
- Create views
- Retrieve data with query statements

SQL Injection Attacks (SQLi)

- One of the most prevalent and dangerous network-based security threats
- Designed to exploit the nature of Web application pages
- Send malicious SQL commands to the database server

- Most common attack goal is bulk extraction of data
- Depending on the environment SQL injection can also be exploited to:
  - ○ Modify or delete data
  - ○ Execute arbitrary operating system commands
  - ○ Launch denial-of-service (DoS) attacks

SQL Injection Attack


Internet
Router
Firewall
Switch
Wireless access point
Web servers
Web application server
Database servers
Database
Legend:.
🟩 Data exchanged between hacker and servers
⇅ Two-way traffic between hacker and Web server
✹ Credit card data is retrieved from database

SQLi Attack Avenues

User input

- Attackers inject SQL commands by providing suitable crafted user input

Server variables

- Attackers can forge the values that are placed in HTTP and network headers and exploit this vulnerability by placing data directly into the headers

Second-order injection

- A malicious user could rely on data already present in the system or database to trigger an SQL injection attack, so when the attack occurs, the input that modifies the query to cause an attack does not come from the user, but from within the system itself

Cookies

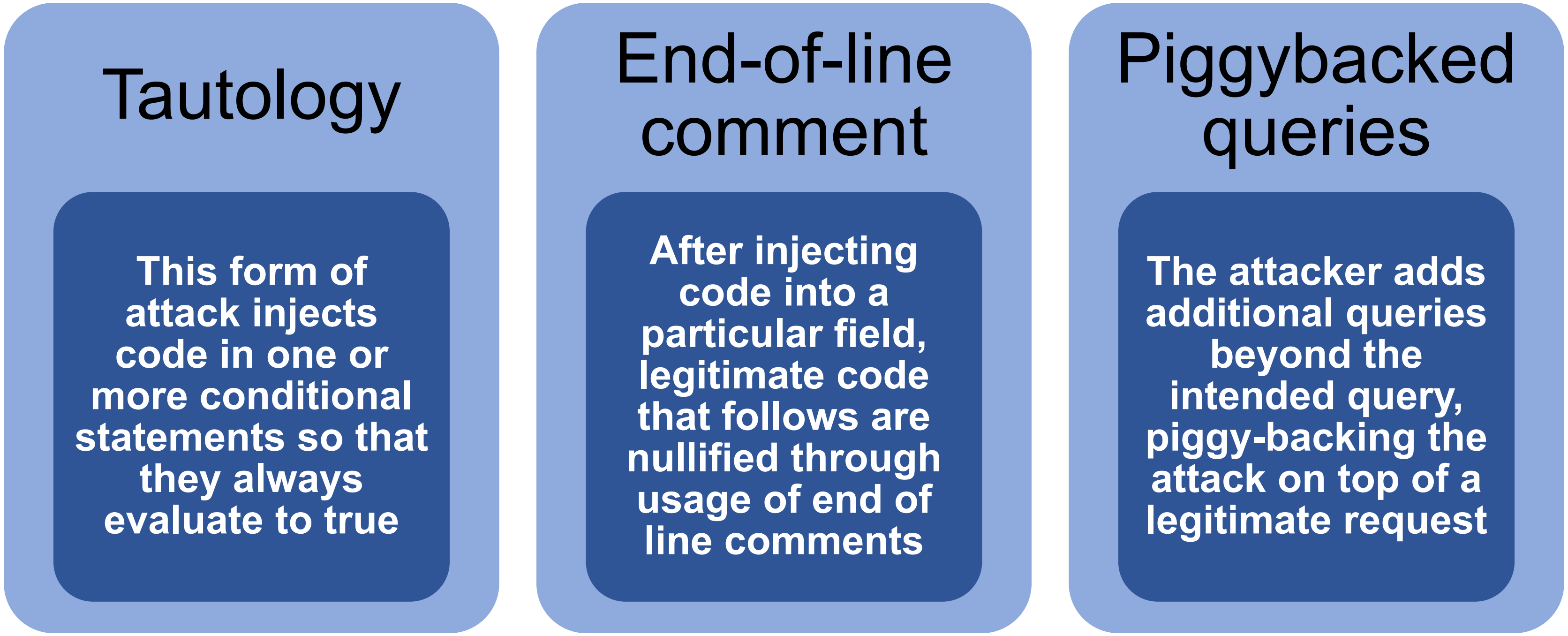
- An attacker could alter cookies such that when the application server builds an SQL query based on the cookie’s content, the structure and function of the query is modified

Physical user input

- Applying user input that constructs an attack outside the realm of web requests

Inband Attacks

- Uses the same communication channel for injecting SQL code and retrieving results
- The retrieved data are presented directly in application Web page
- Include:



Tautology

This form of attack injects code in one or more conditional statements so that they always evaluate to true

End-of-line comment

After injecting code into a particular field, legitimate code that follows are nullified through usage of end of line comments

Piggybacked queries

The attacker adds additional queries beyond the intended query, piggy-backing the attack on top of a legitimate request

Inferential Attack

- There is no actual transfer of data, but the attacker is able to reconstruct the information by sending particular requests and observing the resulting behavior of the Website/database server

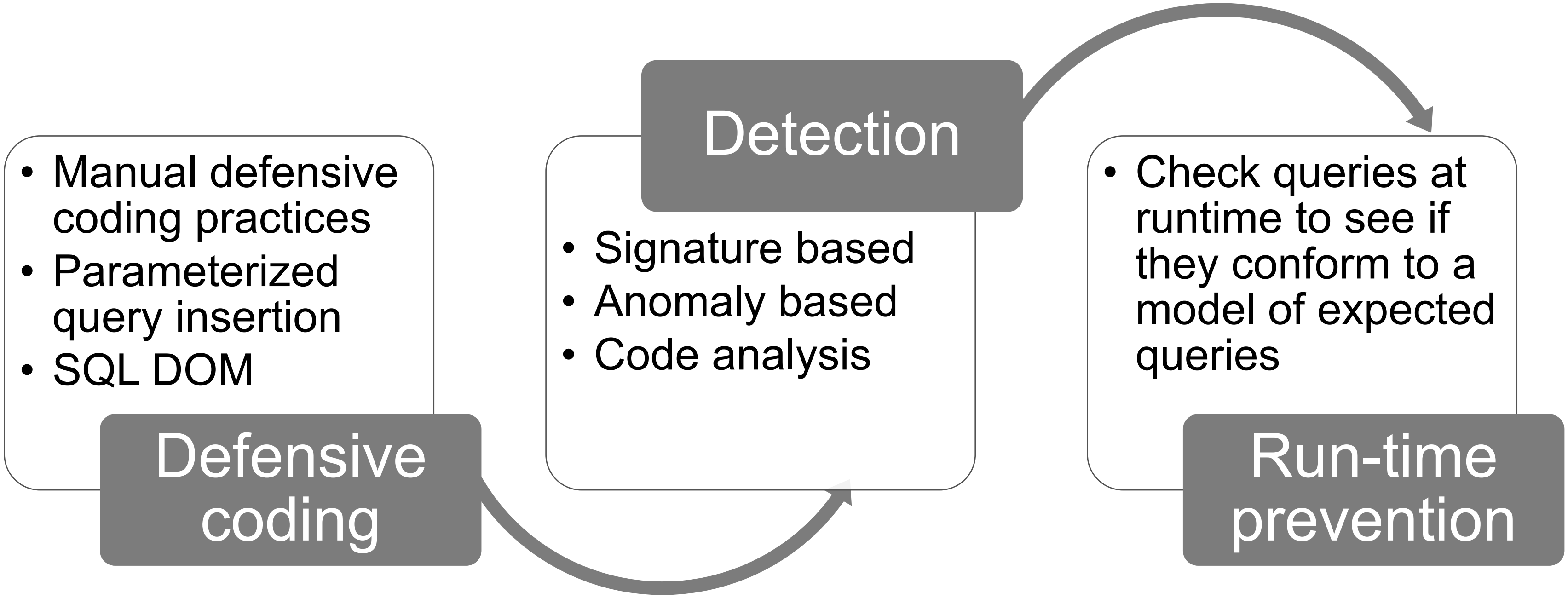
- Include:
    - Illegal/logically incorrect queries
        - This attack lets an attacker gather important information about the type and structure of the backend database of a Web application
        - The attack is considered a preliminary, information-gathering step for other attacks
    - Blind SQL injection
        - Allows attackers to infer the data present in a database system even when the system is sufficiently secure to not display any erroneous information back to the attacker

Out-of-Band Attack

- Data are retrieved using a different channel
- This can be used when there are limitations on information retrieval, but outbound connectivity from the database server is relaxed or not strict

SQLi Countermeasures

- Three types:



Defensive coding

- Manual defensive coding practices
- Parameterized query insertion
- SQL DOM

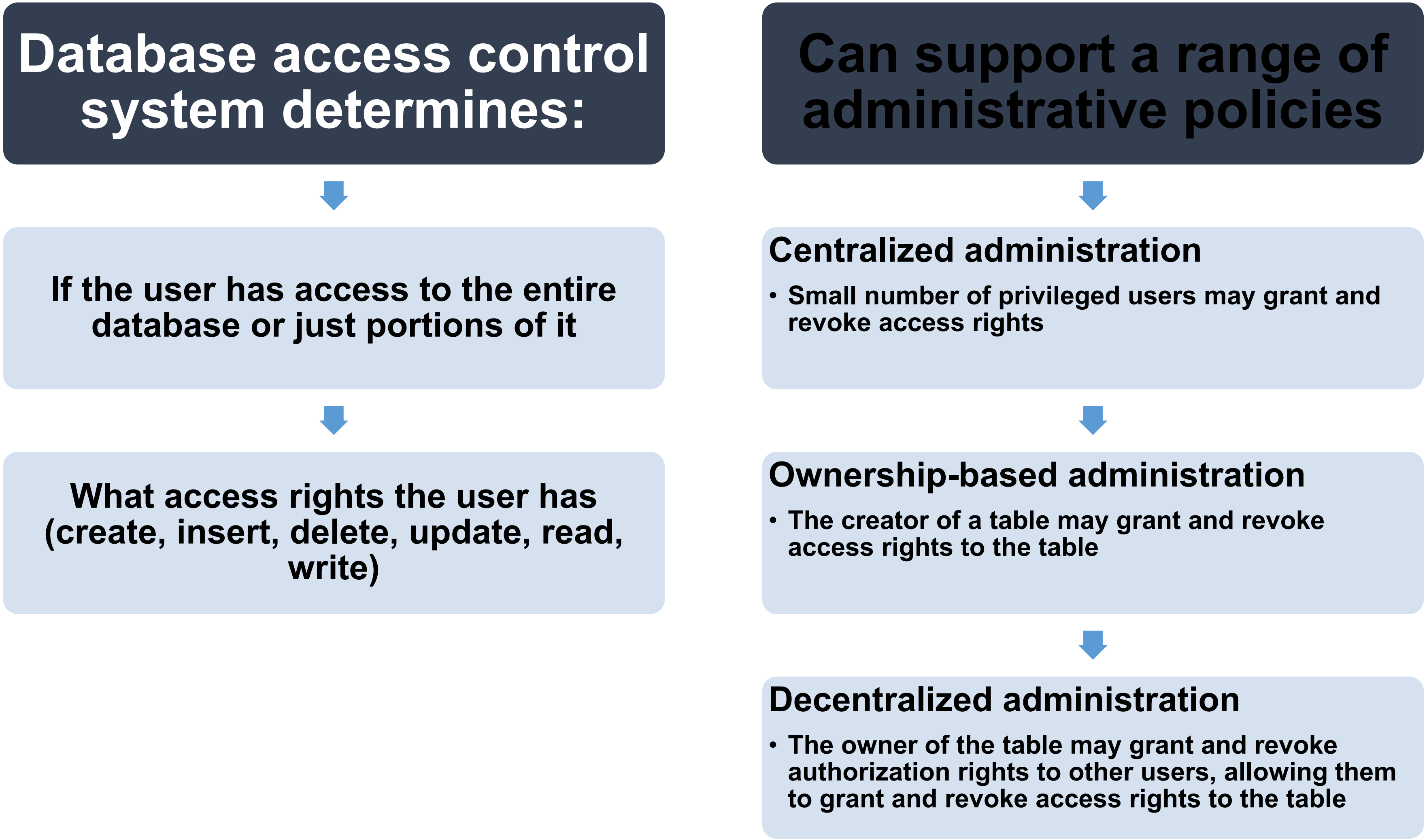
Detection

- Signature based
- Anomaly based
- Code analysis

Run-time prevention

- Check queries at runtime to see if they conform to a model of expected queries

Database Access Control



Database access control system determines:

If the user has access to the entire database or just portions of it

What access rights the user has (create, insert, delete, update, read, write)

Can support a range of administrative policies

Centralized administration

- Small number of privileged users may grant and revoke access rights

Ownership-based administration

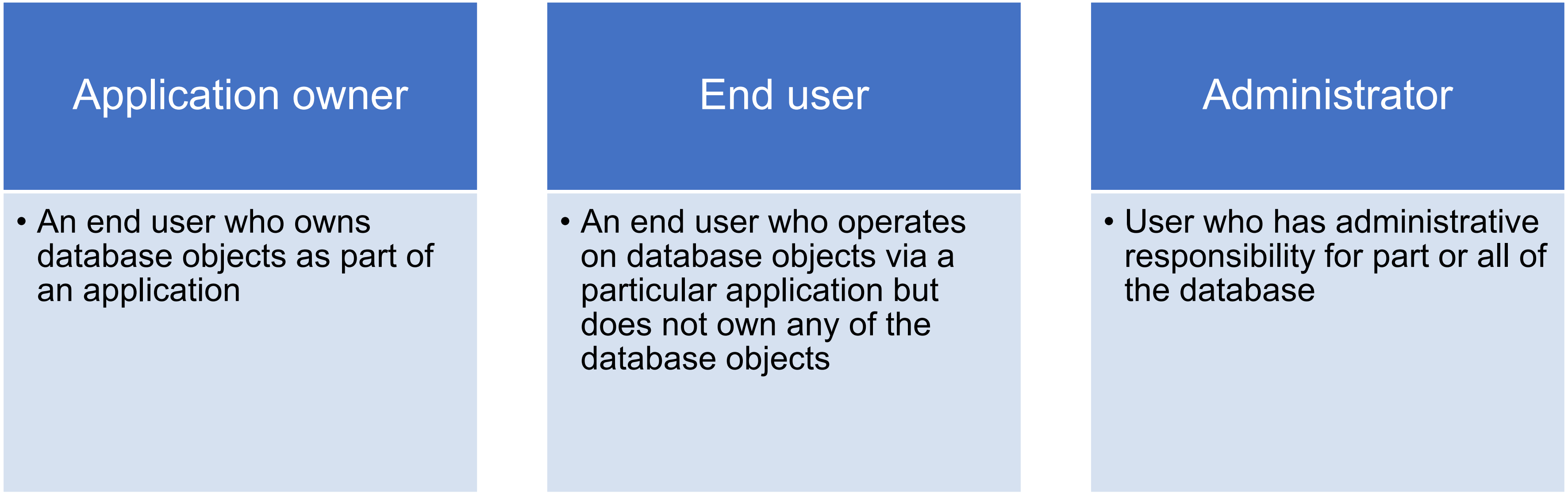
- The creator of a table may grant and revoke access rights to the table

Decentralized administration

- The owner of the table may grant and revoke authorization rights to other users, allowing them to grant and revoke access rights to the table

Role-Based Access Control (RBAC)

- Role-based access control eases administrative burden and improves security
- A database RBAC needs to provide the following capabilities:
  - Create and delete roles
  - Define permissions for a role
  - Assign and cancel assignment of users to roles



Application owner

- An end user who owns database objects as part of an application

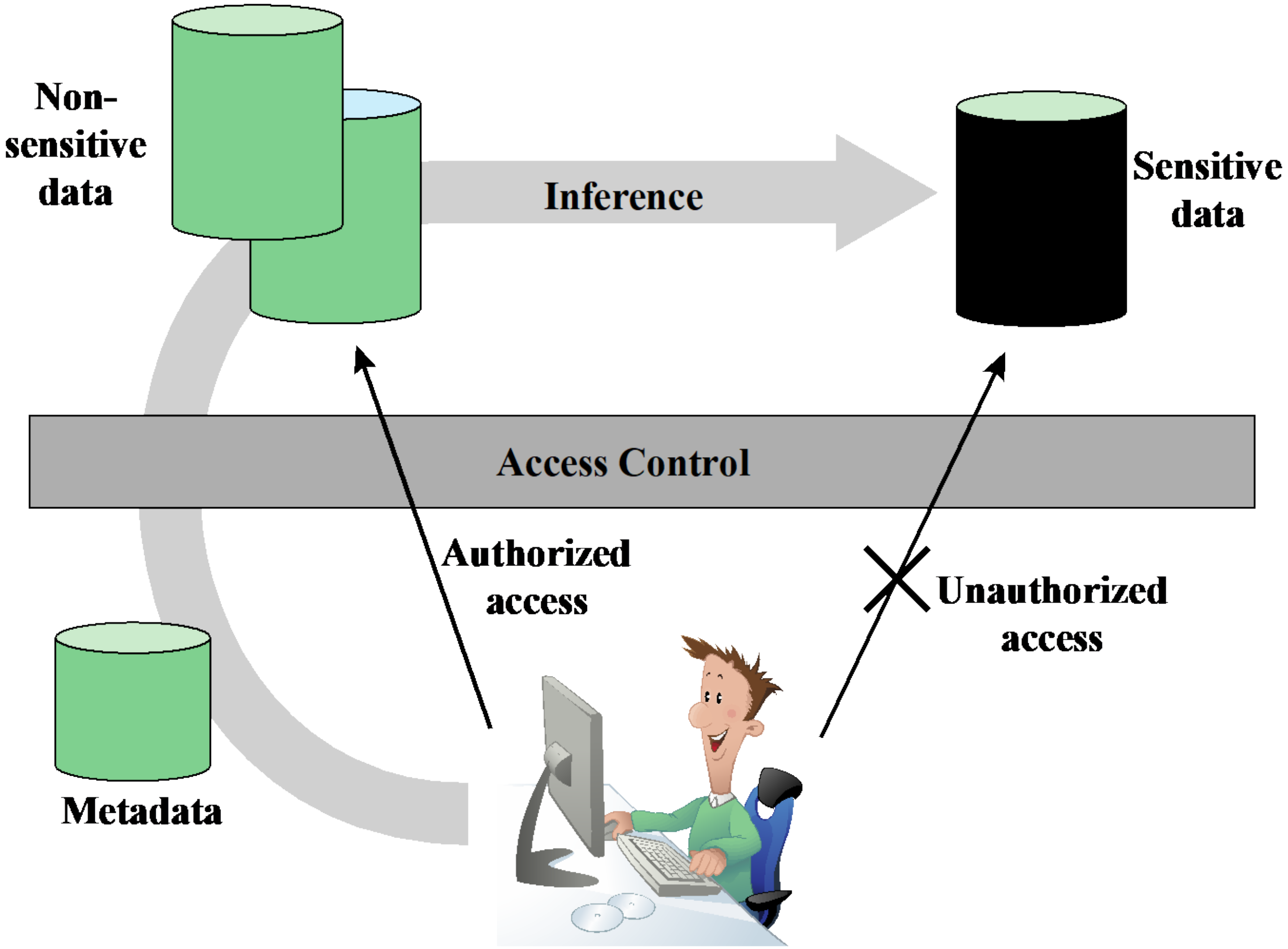
End user

- An end user who operates on database objects via a particular application but does not any of the database objects

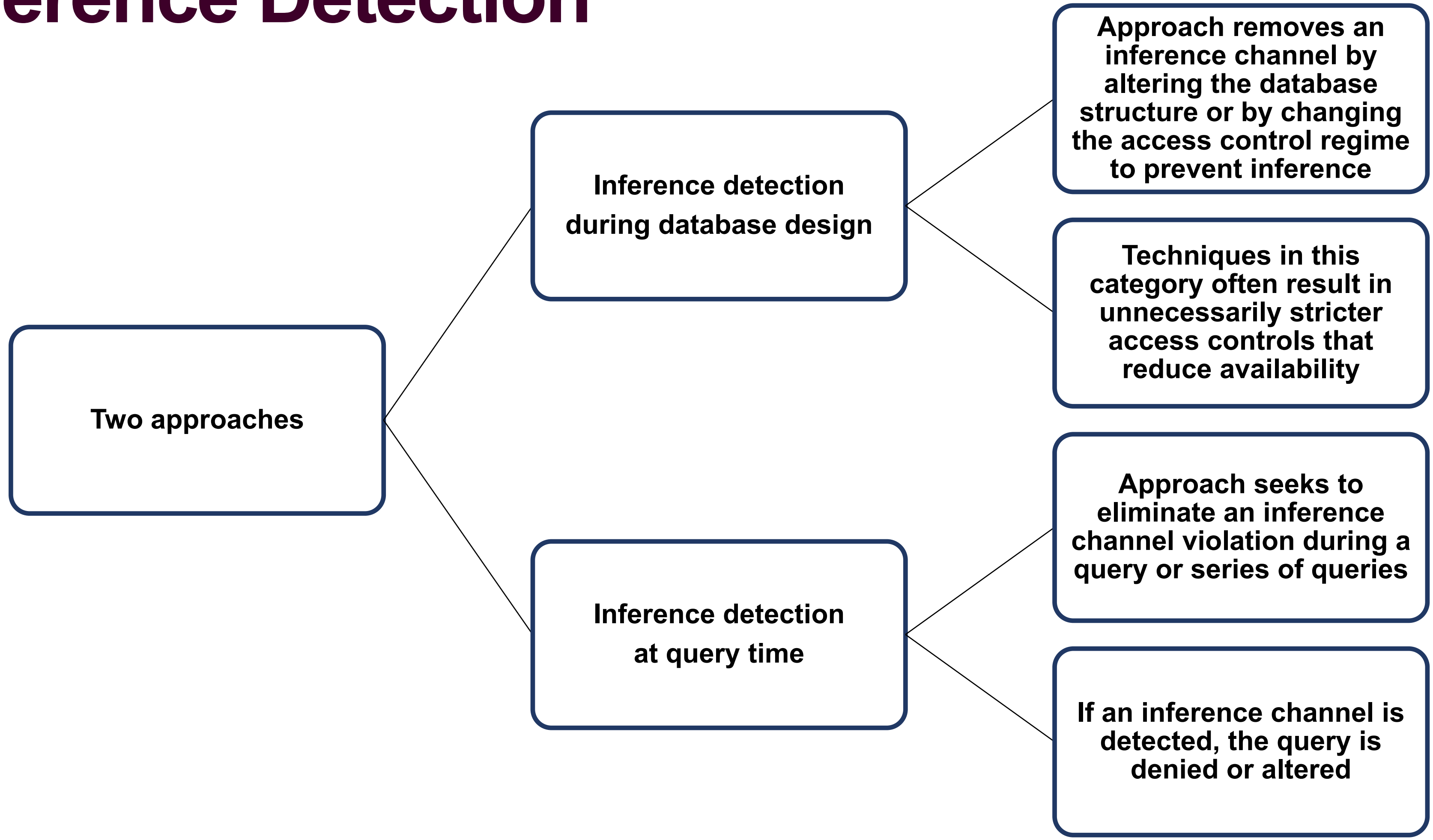
Administrator

- User who has administrative responsibility for part or all of the database

Indirect Information Access Via Inference Channel



Inference Detection



Two approaches

Inference detection during database design

Approach removes an inference channel by altering the database structure or by changing the access control regime to prevent inference

Techniques in this category often result in unnecessarily stricter access controls that reduce availability

Inference detection at query time

Approach seeks to eliminate an inference channel violation during a query or series of queries

If an inference channel is detected, the query is denied or altered

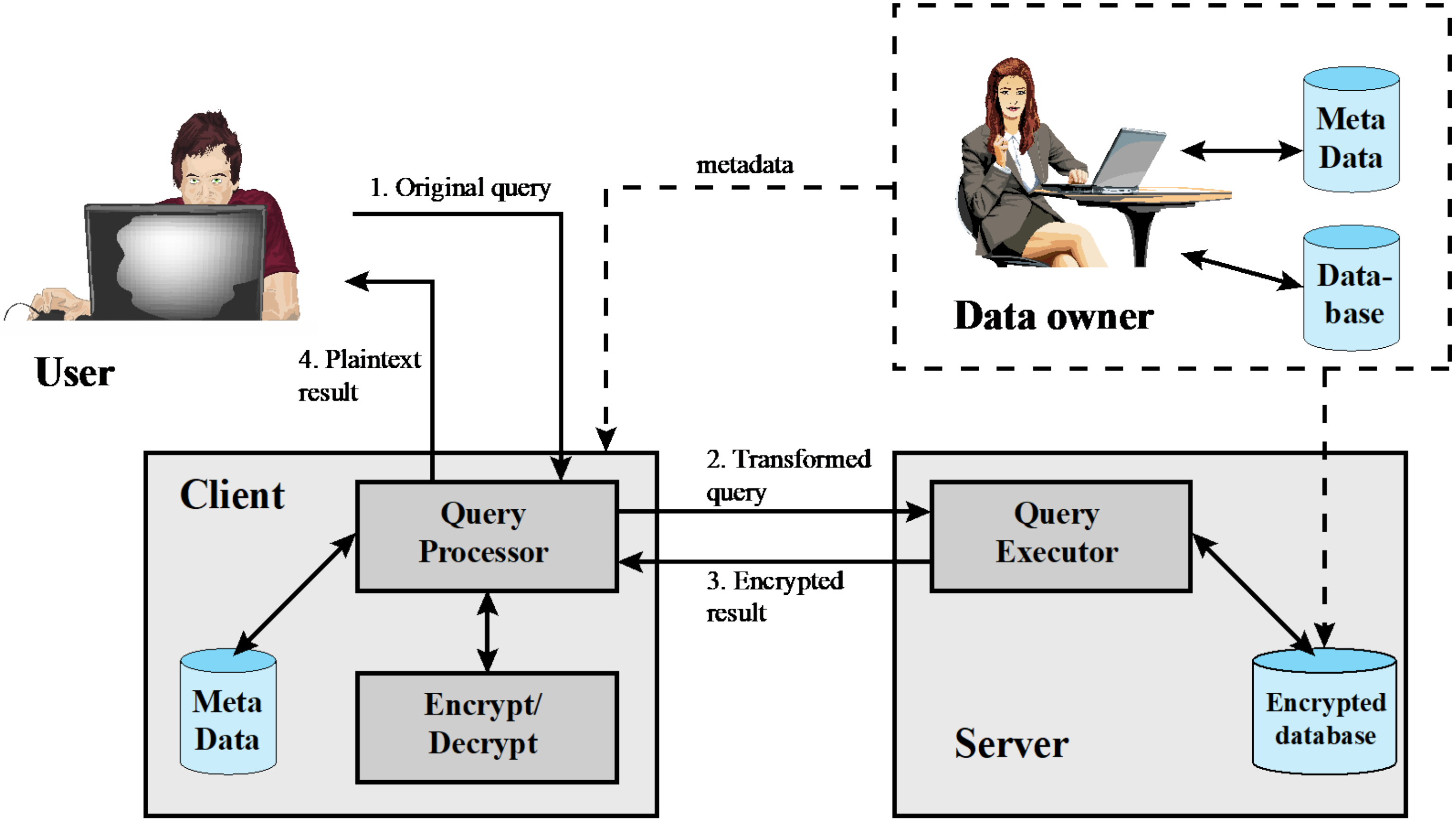
- Some inference detection algorithm is needed for either of these approaches
- Progress has been made in devising specific inference detection techniques for multilevel secure databases and statistical databases

Database Encryption

- The database is typically the most valuable information resource for any organization
    - Protected by multiple layers of security
        - Firewalls, authentication, general access control systems, DB access control systems, database encryption
        - Encryption becomes the last line of defense in database security
    - Can be applied to the entire database, at the record level, the attribute level, or level of the individual field

- Disadvantages to encryption:
    - Key management
        - Authorized users must have access to the decryption key for the data for which they have access
    - Inflexibility
        - When part or all of the database is encrypted it becomes more difficult to perform record searching

A Database Encryption Scheme



Data Center Security

- Data center:
  - An enterprise facility that houses a large number of servers, storage devices, and network switches and equipment
  - The number of servers and storage devices can run into the tens of thousands in one facility
  - Generally includes redundant or backup power supplies, redundant network connections, environmental controls, and various security devices
  - Can occupy one room of a building, one or more floors, or an entire building
- Examples of uses include:
  - Cloud service providers
  - Search engines
  - Large scientific research facilities
  - IT facilities for large enterprises