UNIVERSITY OF WESTMINSTER

Security in various environments

6COSC019W- Cyber Security

Dr Ayman El Hajjar

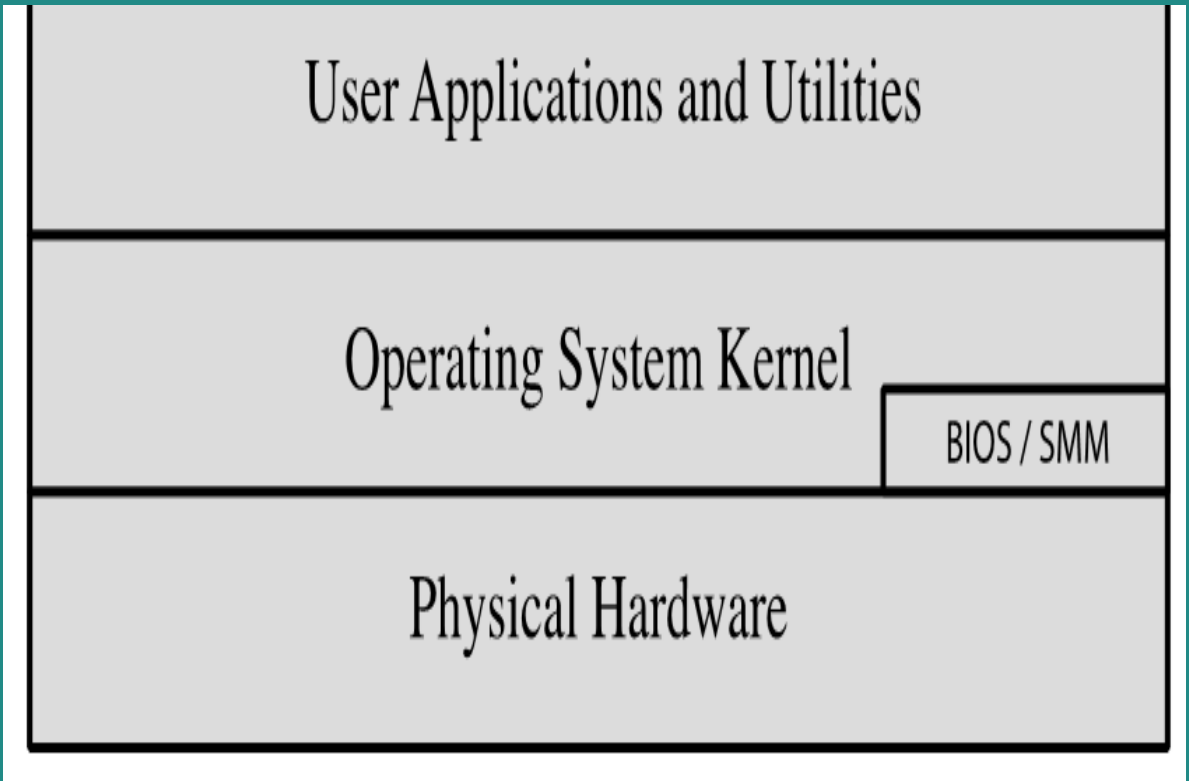
April 03, 2023

School of Computer Science and Engineering
University of Westminster

OUTLINE

Operating system security

OPERATING SYSTEM SECURITY LAYERS



OPERATING SYSTEM SECURITY

- Possible for a system to be compromised during the installation process before it can install the latest patches
- Building and deploying a system should be a planned process designed to counter this threat
- Process must:
  - Assess risks and plan the system deployment
  - Secure the underlying operating system and then the key applications
  - Ensure any critical content is secured
  - Ensure appropriate network protection mechanisms are used
  - Ensure appropriate processes are used to maintain security

System Security Planning

The first step in deploying a new system is planning

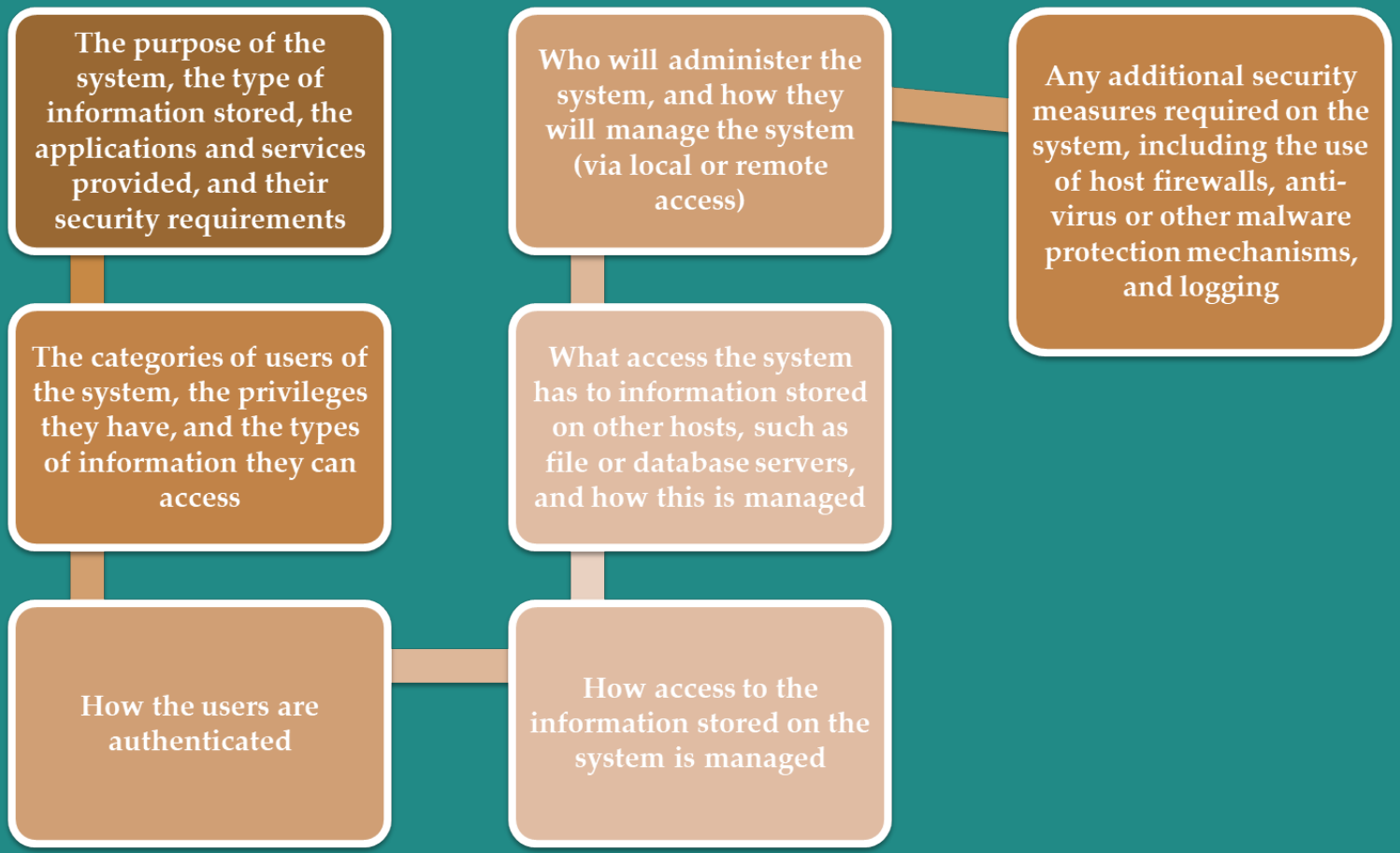
Plan needs to identify appropriate personnel and training to install and manage the system

Planning should include a wide security assessment of the organization

Planning process needs to determine security requirements for the system, applications, data, and users

Aim is to maximize security while minimizing costs

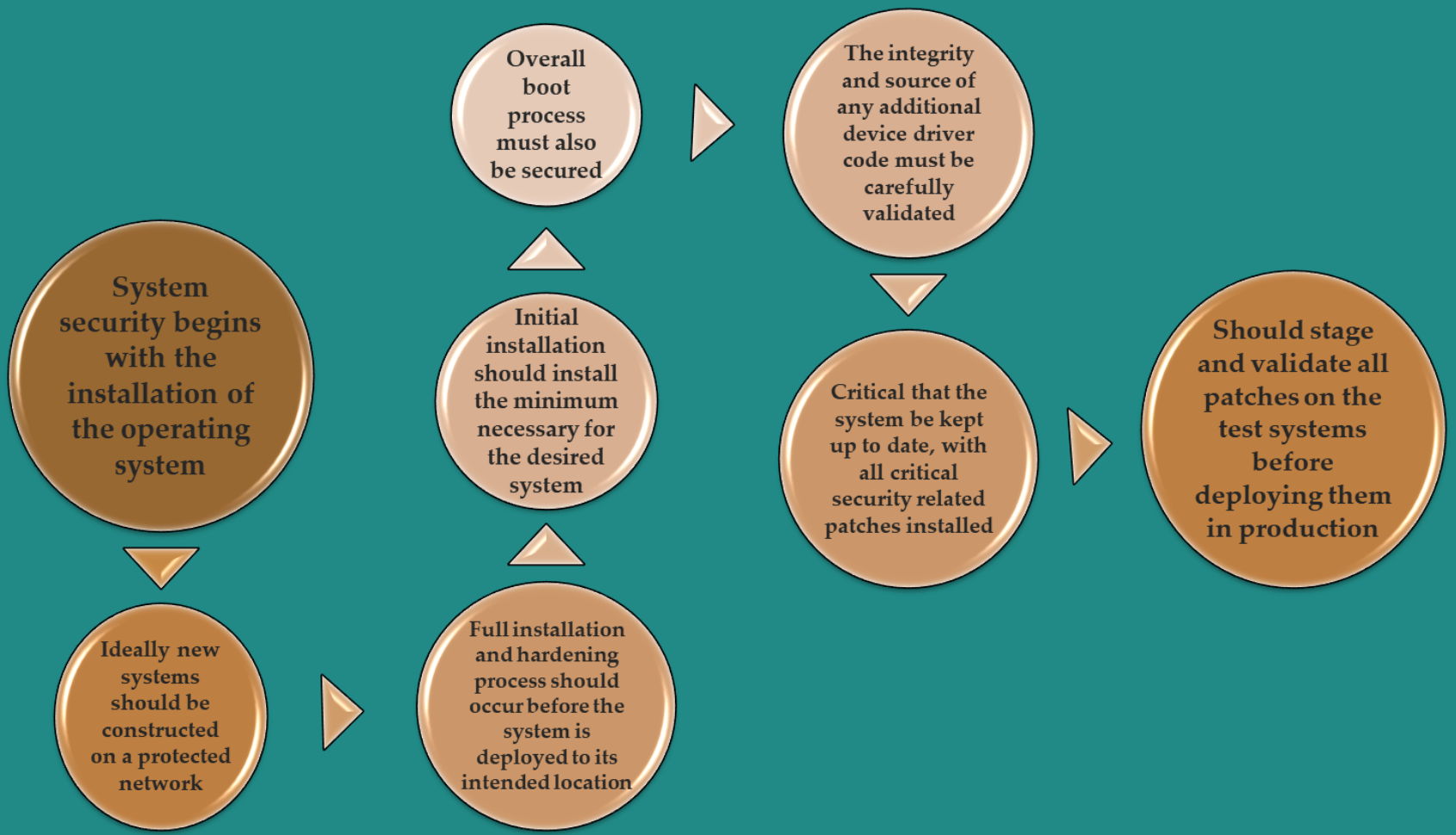
System Security Planning Process



Operating Systems Hardening

- First critical step in securing a system is to secure the base operating system and:
  - Install and patch the operating system
  - Address the identified 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 Your controls

INITIAL SETUP AND PATCHING



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

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. Goals are:
  - Ensure the previous security configuration steps are correctly implemented
  - Identify any possible vulnerabilities
- Checklists are included in security hardening guides
- 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

Application Configuration

- May include:
  - Creating and specifying appropriate data storage areas for application
  - Making appropriate changes to the application or service default configuration details
- Some applications or services may include:
  - Default data
  - Scripts
  - User accounts
- Of particular concern with remotely accessed services such as Web and file transfer services
  - Risk is reduced by ensuring that most of the files can only be read, but not written, by the server

SECURITY MAINTENANCE

- Process of maintaining security is continuous
- Security maintenance includes:
  - Monitoring and analysing 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, and to monitor and revise configuration as needed

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

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
- Implements a form of the Biba Integrity model

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

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
  - ☞ 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

LINUX/UNIX SECURITY

Remote access controls

- Several host firewall programs may be used
- Most systems provide an administrative utility to select which services will be permitted to access the system

Logging and log rotation

- Should not assume that the default setting is necessarily appropriate

LINUX/UNIX SECURITY

- chroot jail
  - Restricts the server's view of the file system to just a specified portion
  - Uses chroot system call to confine a process by mapping the root of the filesystem to some other directory
  - File directories outside the chroot jail aren't visible or reachable
  - Main disadvantage is added complexity

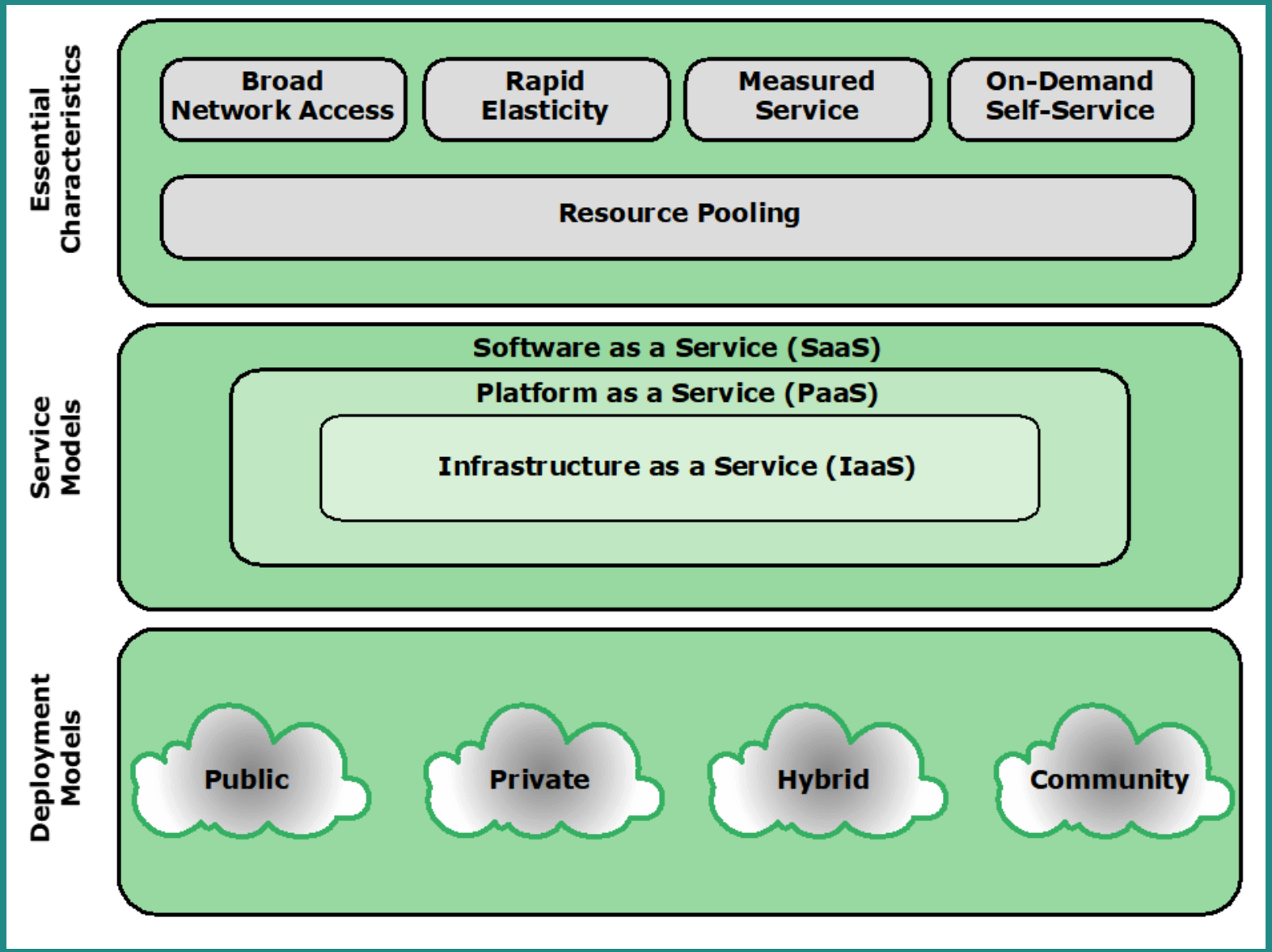
Cloud Computing Security

CLOUD COMPUTING:

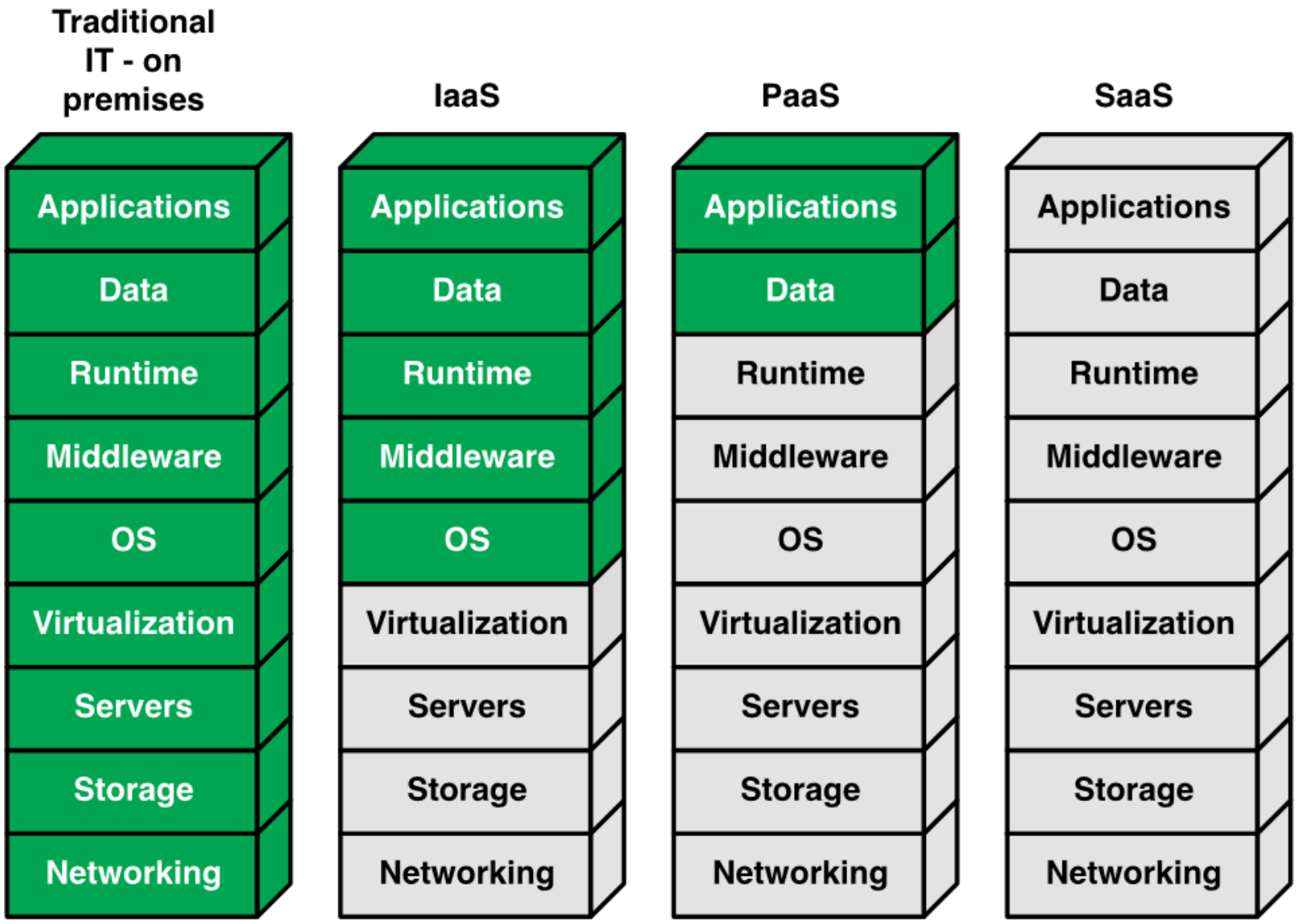
NIST defines cloud computing, in NIST SP-800-145

"Cloud computing: A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models.

CLOUD COMPUTING ELEMENTS



Separation of Responsibilities in Cloud Service Models



Comparison of Cloud Deployment Models

	Private	Community	Public	Hybrid
Scalability	Limited	Limited	Very high	Very high
Security	Most secure option	Very secure	Moderately secure	Very secure
Performance	Very good	Very good	Low to medium	Good
Reliability	Very high	Very high	Medium	Medium to high
Cost	High	Medium	Low	Medium

Security Issues for Cloud Computing

- Security is a major consideration when augmenting or replacing on-premises systems with cloud services
- Availability is another major concern. Auditability of data must be ensured
- Businesses should perform due diligence on security threats both from outside and inside the cloud
  - ☞ Cloud users are responsible for application-level security
  - ☞ Cloud vendors are responsible for physical security and some software security
  - ☞ Security for intermediate layers of the software stack is shared between users and vendors

RISKS AND COUNTERMEASURES

- The Cloud Security Alliance lists the following as the top cloud-specific security threats:

1. Abuse and nefarious use of cloud computing.
   - Stricter initial registration and validation processes
   - Enhanced credit card fraud monitoring and coordination
   - Comprehensive inspection of customer traffic
   - Monitoring public blacklists for network blocks
2. Insecure interfaces and APIs. Countermeasures include:
   - Analysing the security model of CSP interfaces
   - Ensuring that strong authentication and access controls are implemented in concert with encrypted transmission

RISKS AND COUNTERMEASURES

3. Malicious insiders. Countermeasures include:
   - Enforce strict supply chain management and conduct a supplier assessment
   - Human resource requirements in the legal contract
   - Require transparency into information security, management practices and compliance reporting
   - Determine security breach notification processes
4. Shared technology issues. Countermeasures include:
   - Implement security best practices for installation/configuration
   - Monitor for unauthorized changes/activity
   - Promote strong authentication and access control
   - Enforce SLAs for patching and vulnerability remediation
   - Conduct vulnerability scanning and configuration audits

RISKS AND COUNTERMEASURES

5. Data loss or leakage. Countermeasures include:
   - Implement strong API access control
   - Protect integrity of data in transit and at rest
   - Analyse data protection at both design and run time
   - Implement strong key generation, storage and management, and destruction practices
6. Account or service hijacking. Countermeasures include:
   - Prohibit the sharing of account credentials between users and services
   - Leverage strong two-factor authentication techniques where possible
   - Employ proactive monitoring to detect unauthorized activity

DATA PROTECTION IN THE CLOUD

The threat of data compromise increases in the cloud, due to the number of, and interactions between, risks and challenges that are either unique to the cloud or more dangerous because of the architectural or operational characteristics of the cloud environment

Even with these precautions, corruption and other denial-of-service attacks remain a risk

Data must be secured while at rest, in transit, and in use, and access to the data must be controlled

For data at rest, the ideal security measure is for the client to encrypt the database and only store encrypted data in the cloud, with the CSP having no access to the encryption key

The client can employ encryption to protect data in transit, though this involves key management responsibilities for the CSP

The client can enforce access control techniques, but CSP is involved to some extent depending on the service model used

NIST Cloud Computing Reference Architecture

NIST Cloud Computing Reference Architecture, in NIST SP-500-292

"The NIST cloud computing reference architecture focuses on the requirements of "what" cloud services provide, not a "how to" design solution and implementation. The reference architecture is intended to facilitate the understanding of the operational intricacies in cloud computing. It does not represent the system architecture of a specific cloud computing system; instead it is a tool for describing, discussing, and developing a system-specific architecture using a common framework of reference.

Cloud Computing Reference Architecture Objectives

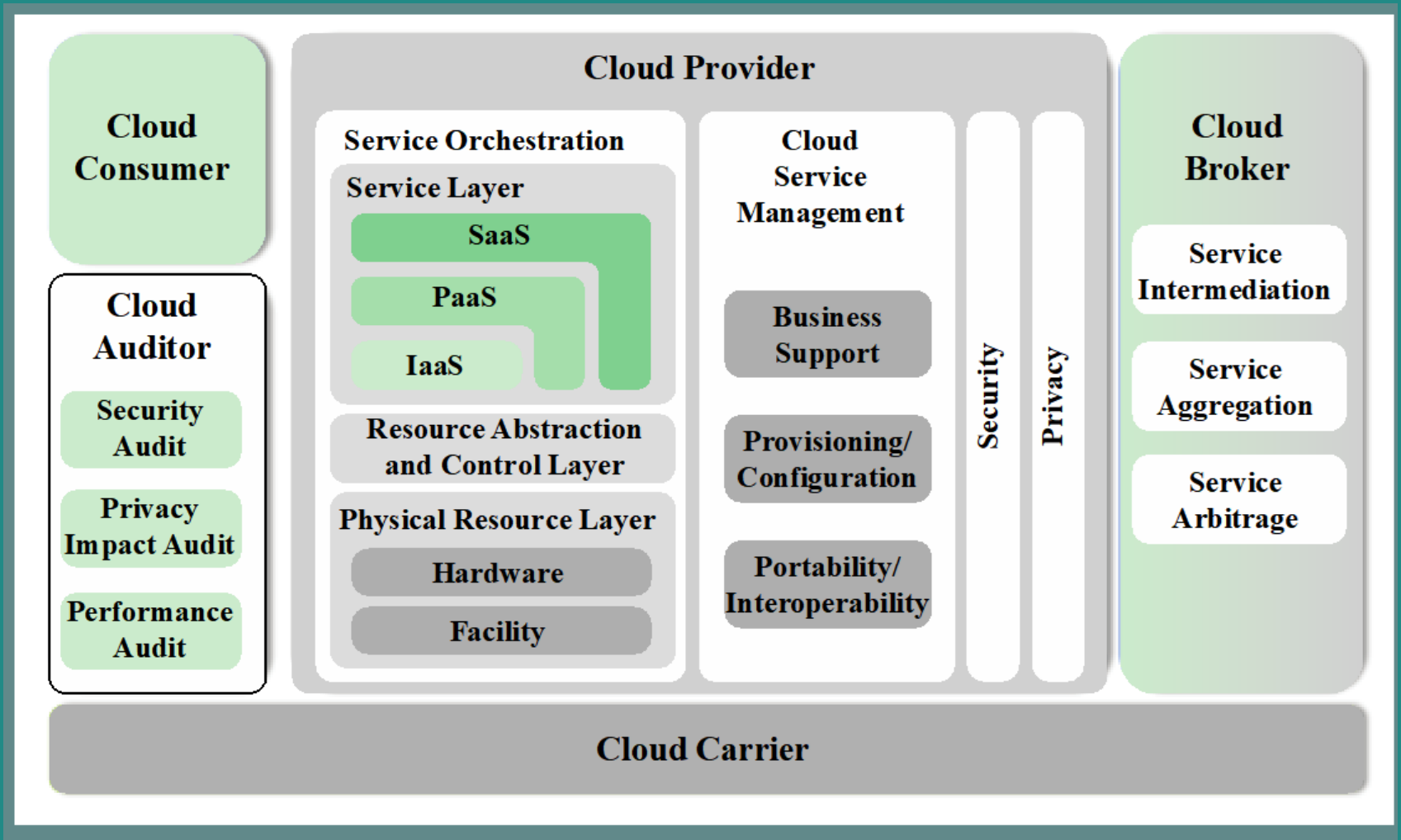
NIST developed the reference architecture with the following objectives in mind:

To illustrate and understand the various cloud services in the context of an overall cloud computing conceptual model

To provide a technical reference for CSCs to understand, discuss, categorize, and compare cloud services

To facilitate the analysis of candidate standards for security, interoperability, and portability and reference implementations

NIST CLOUD COMPUTING REFERENCE ARCHITECTURE



IoT Security

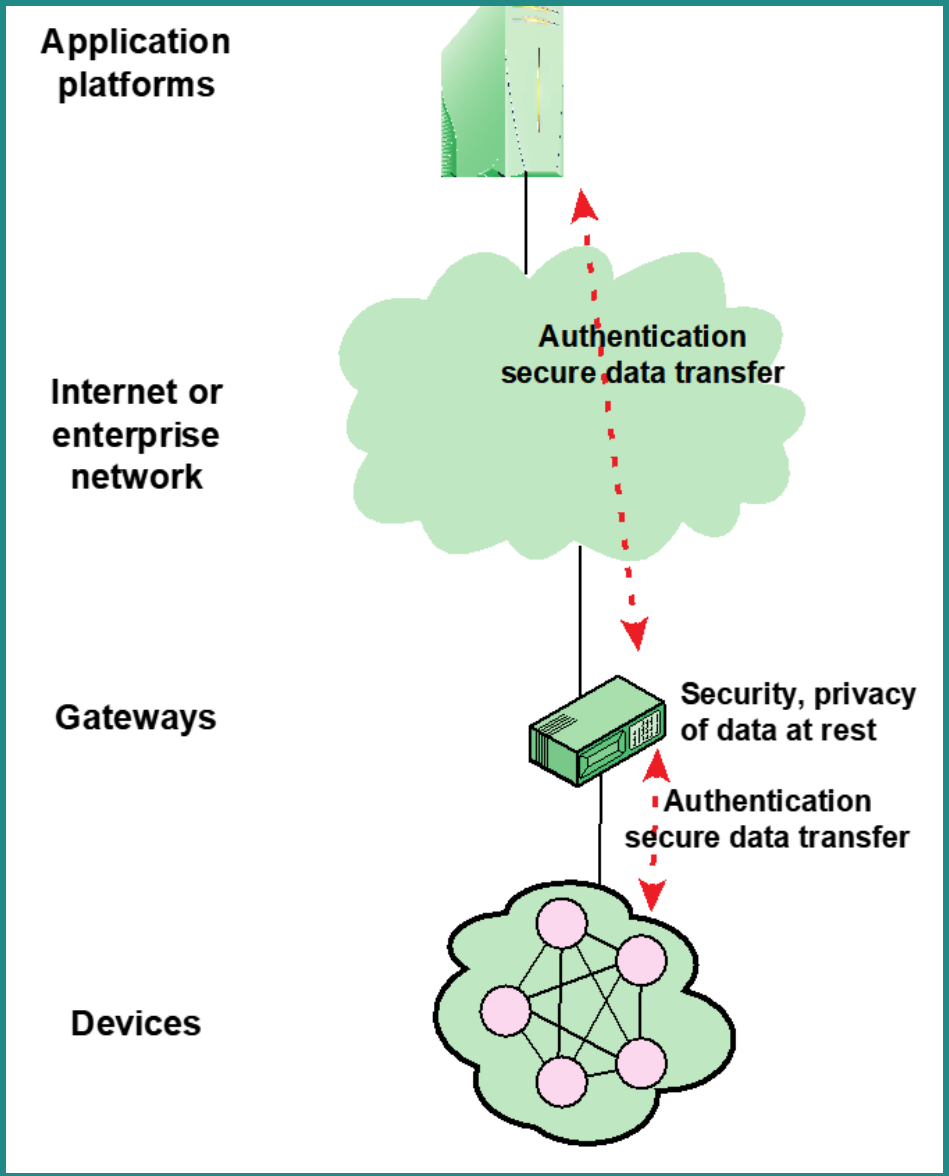
THE INTERNET OF THINGS (IOT)

- IoT is a term that refers to the expanding interconnection of smart devices, ranging from appliances to tiny sensors
  - A dominant theme is the embedding of short-range mobile transceivers into a wide array of gadgets and everyday items, enabling new forms of communication between people and things, and between things themselves
  - The Internet supports the interconnectivity usually through cloud systems
- The objects deliver sensor information, act on their environment, and in some cases modify themselves, to create overall management of a larger system
- The IoT is primarily driven by deeply embedded devices

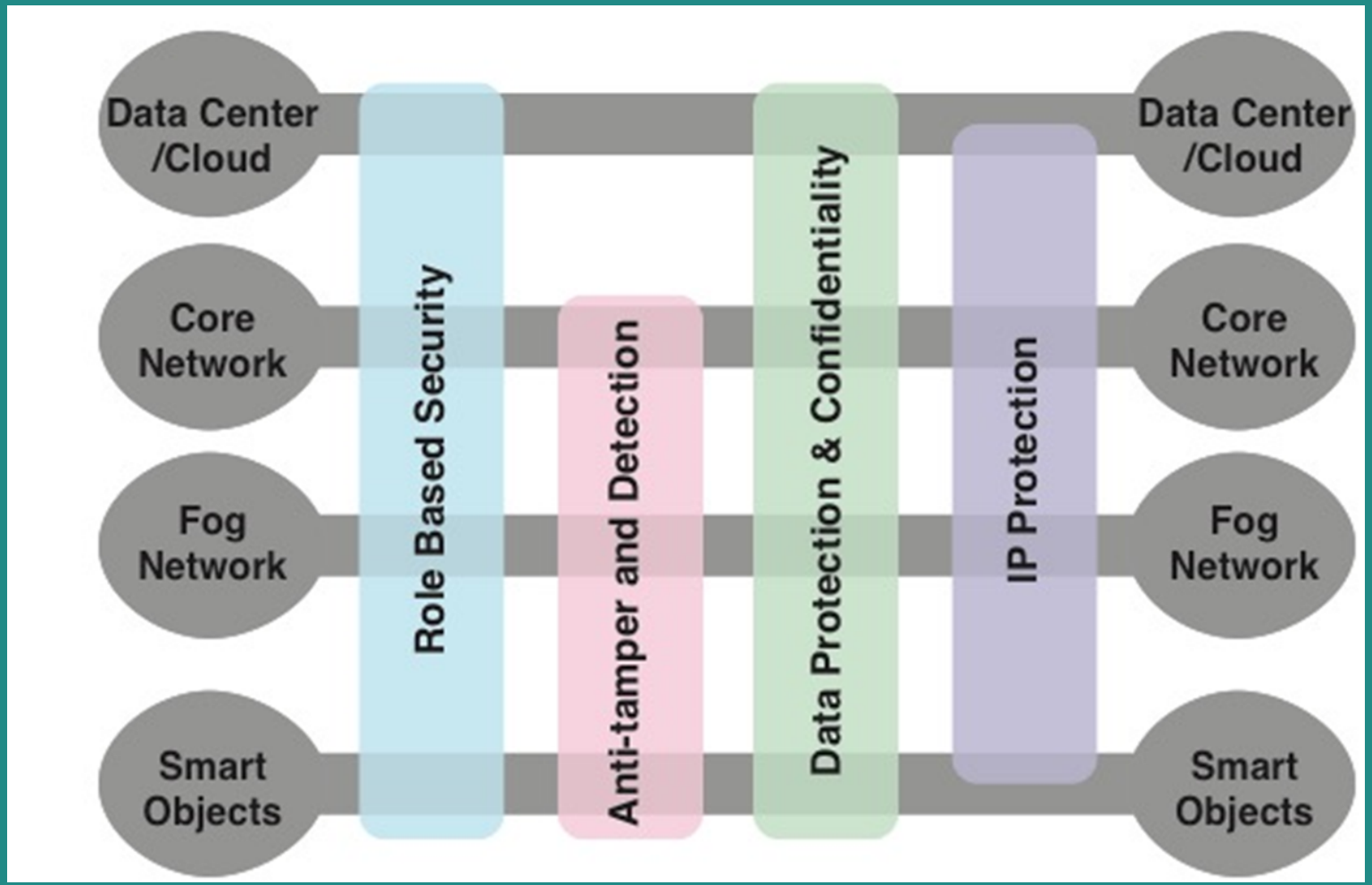
IoT Security and Privacy requirements

- ITU-T Recommendation Y.2066 includes a list of security requirements for the IoT
- The requirements are defined as being the functional requirements during capturing, storing, transferring, aggregating, and processing the data of things, as well as to the provision of services which involve things
- The requirements are:
  - Communication security
  - Data management security
  - Service provision security
  - Integration of security policies and techniques
  - Mutual authentication and authorization
  - Security audit

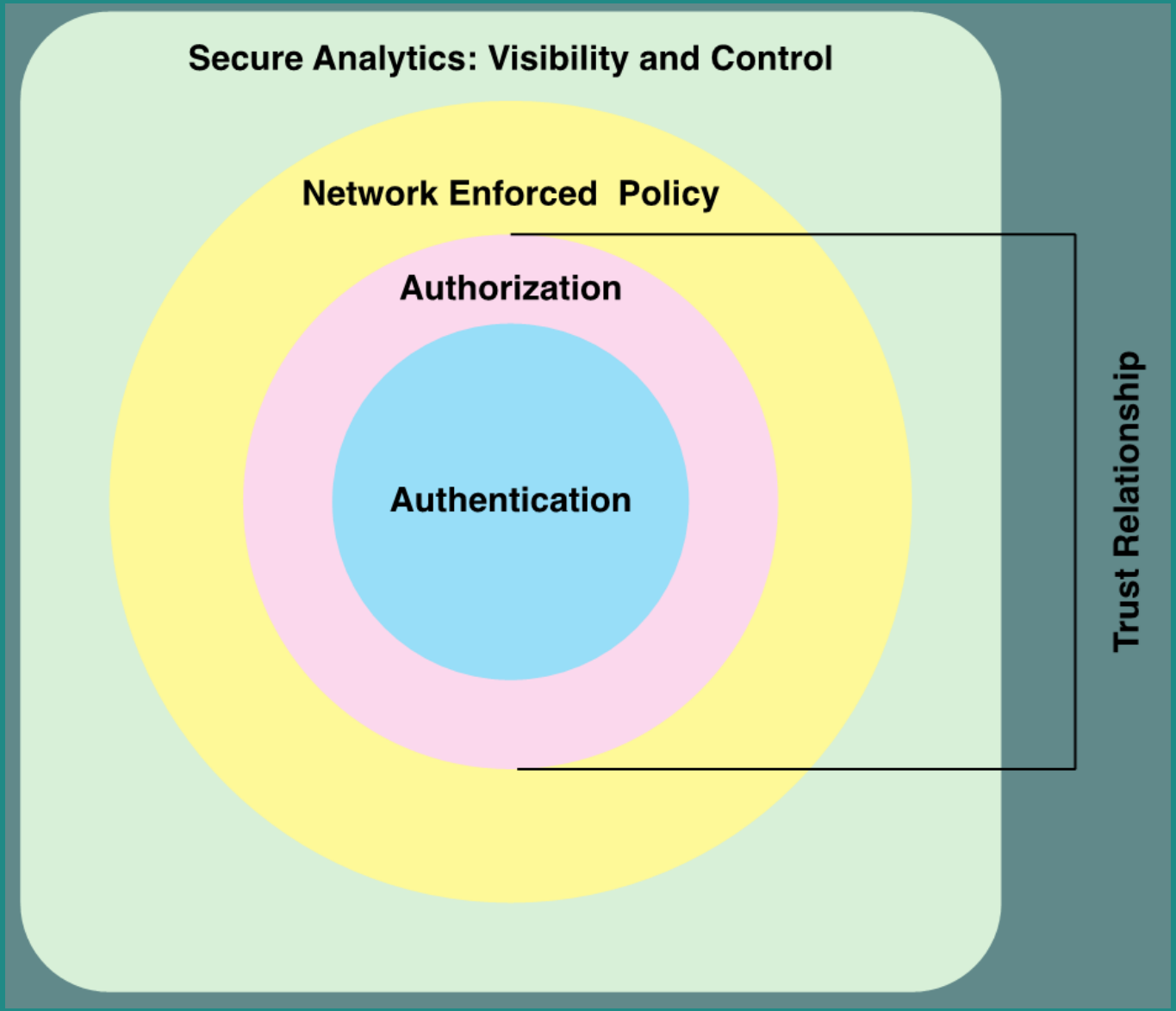
IoT Gateway Security Functions



IoT Security environment



SECURE IOT FRAMEWORK



REFERENCES

- The lecture notes and contents were compiled from my own notes and from various sources.
- Figures and tables are from the recommended books
- **Recommended Readings note:** Focus on what was covered in the class.
  - Chapters 12, 13- Computer Security: Principles and Practice, , William Stallings and Lawrie Brown
  - Chapter 11, CyBOK, The Cyber Security Body of Knowledge