Tactics for Security (1)

主讲教师： 王灿

Email: wcan@zju.edu.cn

TA: 李奇平 liqiping1991@gmail.com

Course FTP: ftp://sa:sa@10.214.51.13

Some Proverbs

- No fortress is impregnable
- A chain is only as strong as its weakest link
- The easiest way to capture a fortress is from within

Security and Attack

- Security is about system’s ability to protect data and information from unauthorized access while still providing access to people and systems that are authorized

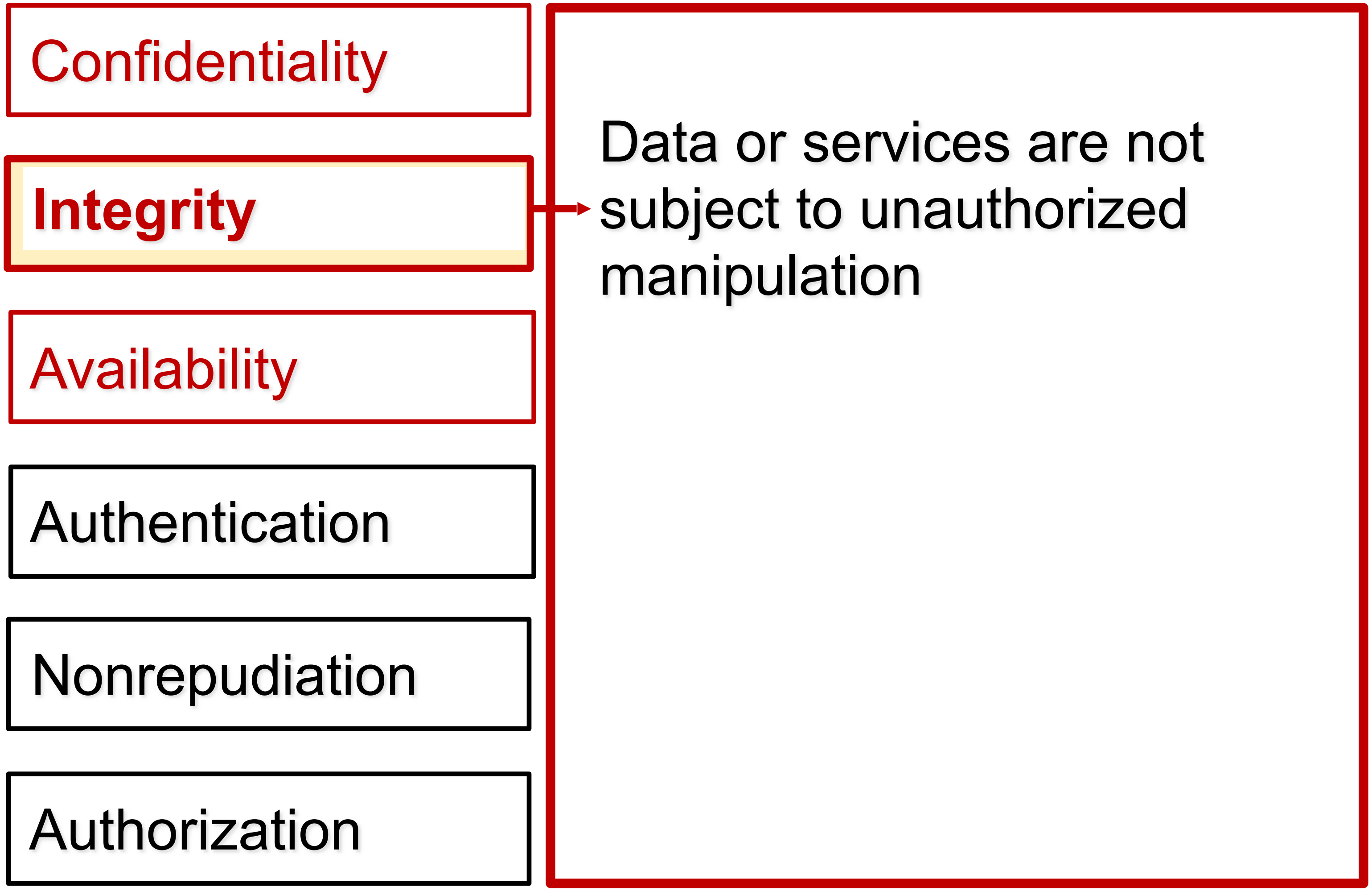
- Attack – is an attempt to breach security
    - Unauthorized login
    - Sniffing data on communication channel
    - Unauthorized access/modification of data
    - Denial of services attacks – crash the system
    - ……

Security: Confidentiality

- **Confidentiality**
- Integrity
- Availability
- Authentication
- Nonrepudiation
- Authorization

Confidentiality → Data or services are protected from unauthorized access

Security: Integrity



Confidentiality

Integrity

Availability

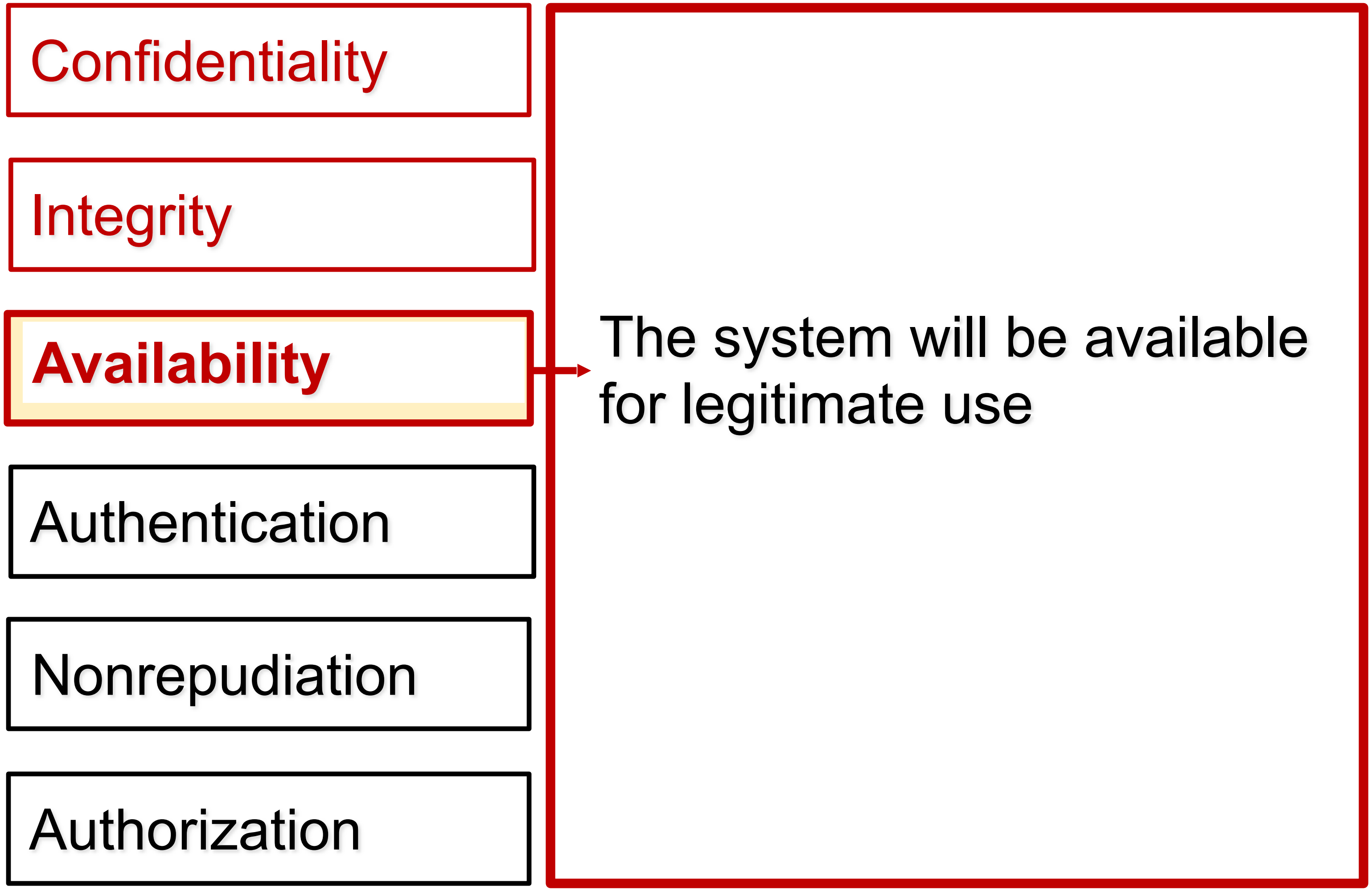
Authentication

Nonrepudiation

Authorization

Data or services are not subject to unauthorized manipulation

Security: Availability



Confidentiality

Integrity

Availability

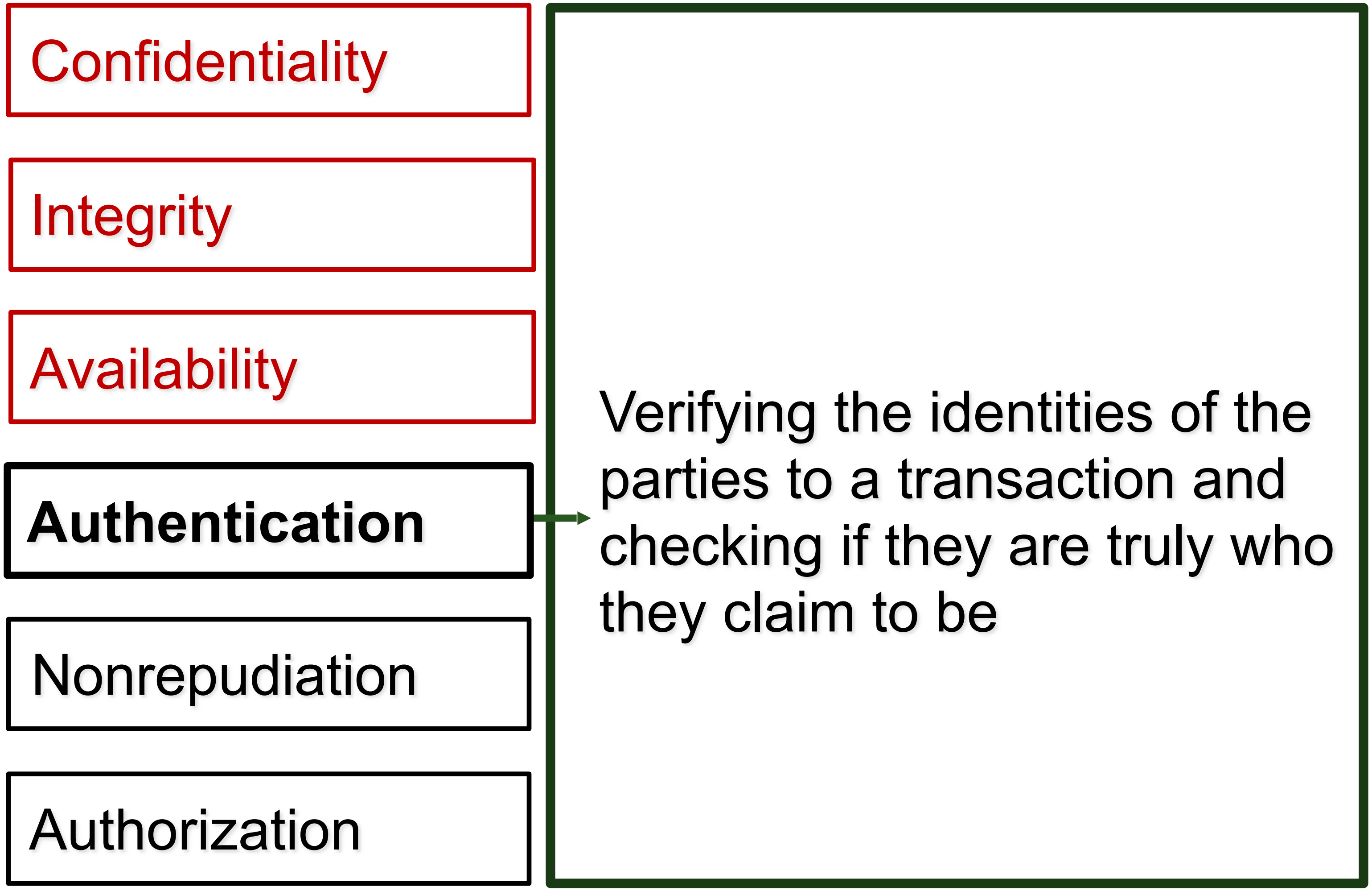
Authentication

Nonrepudiation

Authorization

The system will be available for legitimate use

Security: Authentication



Confidentiality

Integrity

Availability

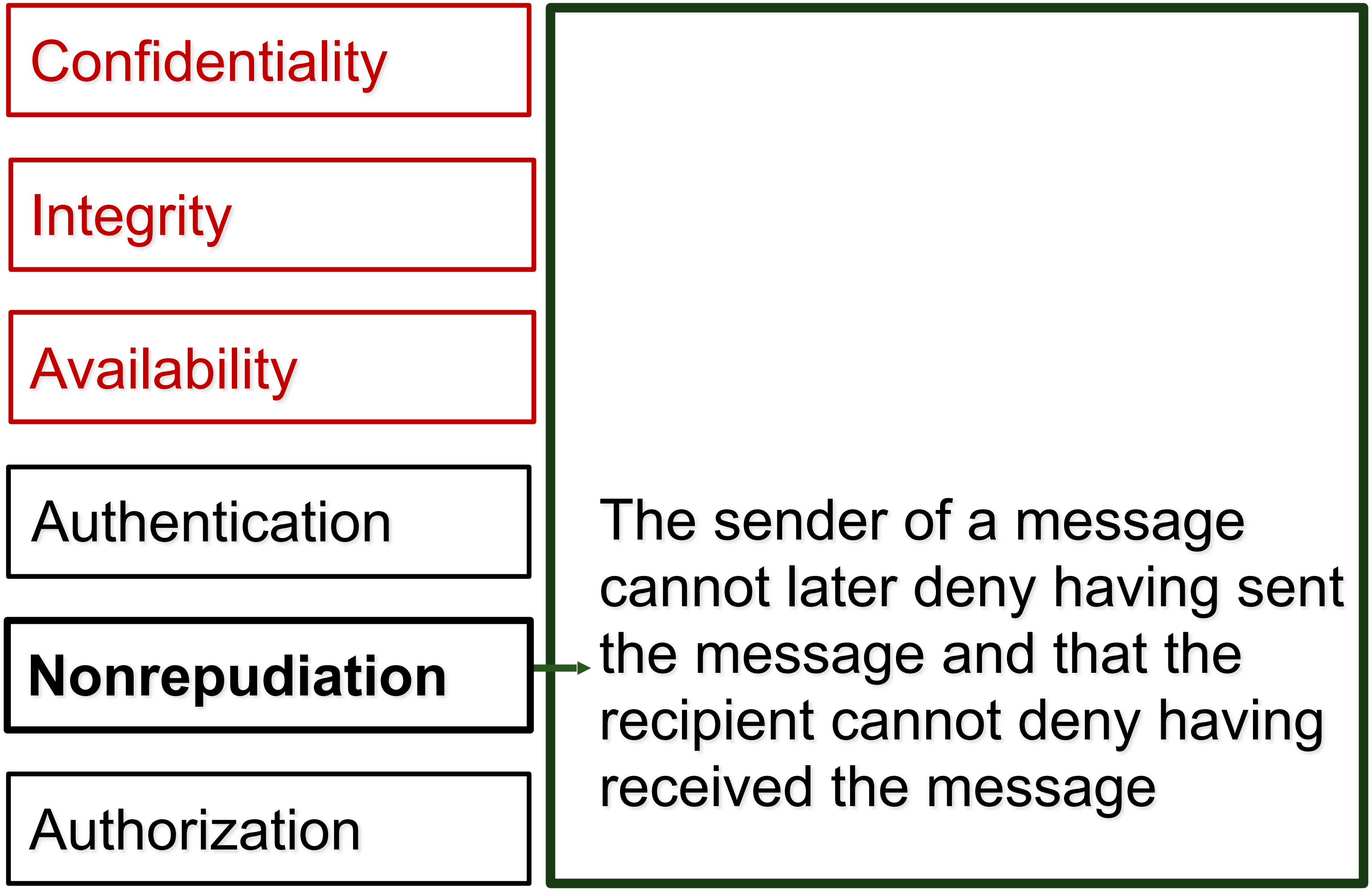
Authentication

Nonrepudiation

Authorization

Verifying the identities of the parties to a transaction and checking if they are truly who they claim to be

Security: Nonrepudiation



Confidentiality

Integrity

Availability

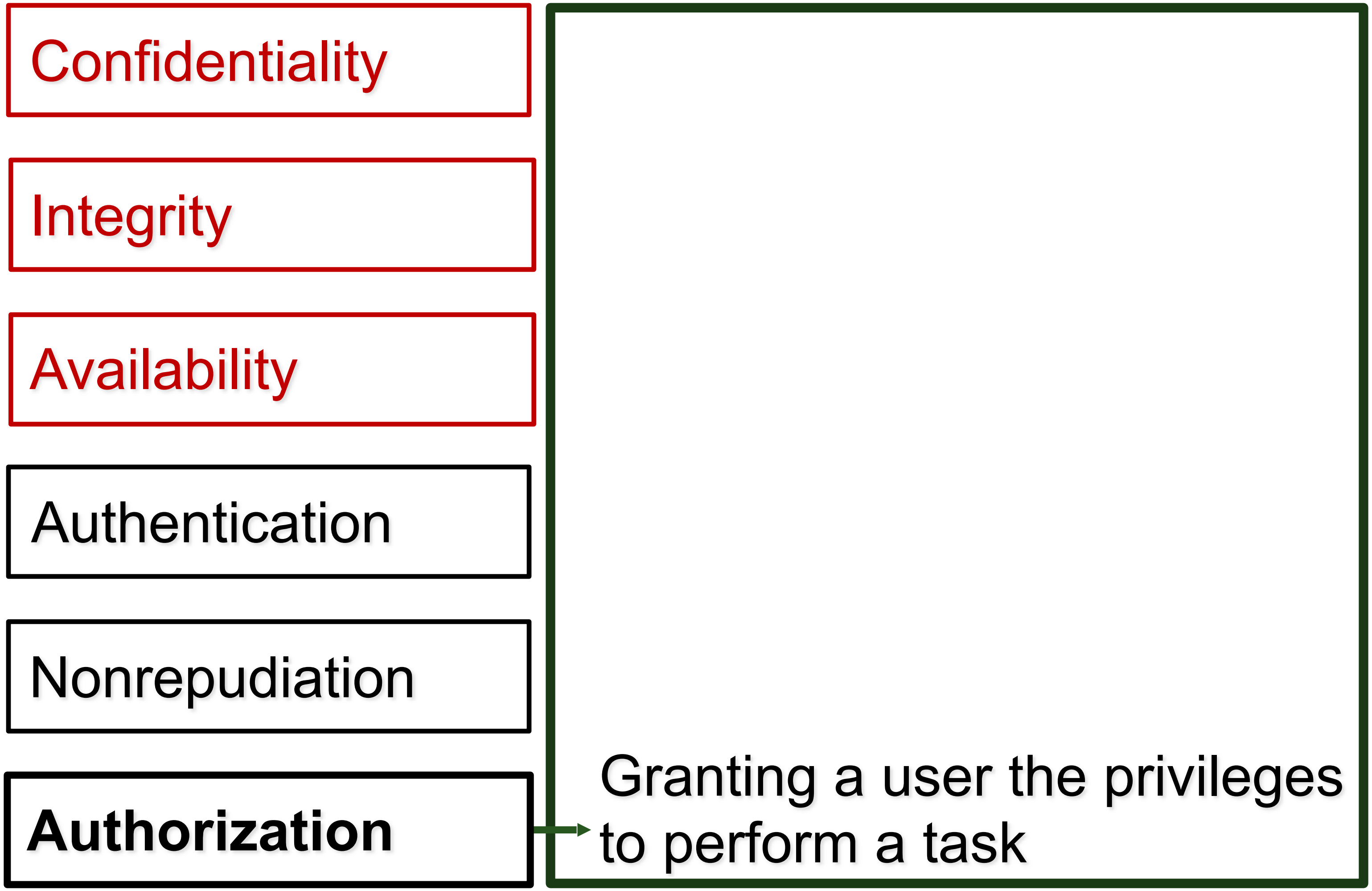
Authentication

Nonrepudiation

Authorization

The sender of a message cannot later deny having sent the message and that the recipient cannot deny having received the message

Security: Authorization



Confidentiality

Integrity

Availability

Authentication

Nonrepudiation

Authorization

Granting a user the privileges to perform a task

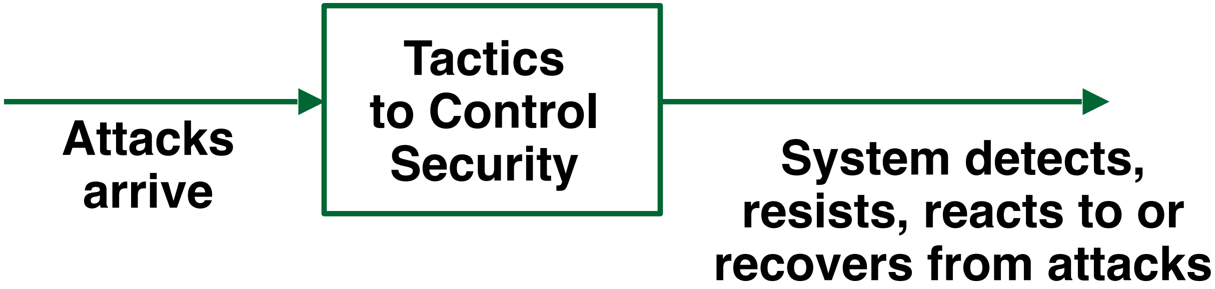
Security General Scenario (1)

- Stimulus
  - Unauthorized attempts to display/modify/delete data or access system services, change service behavior or reduce availability
- Source of stimulus
  - Human/system
  - Identified/unknown
  - Internal/external
  - Limited access/access to vast resource
- Response
  - Ensure CIA, authentication, nonrepudiation, authorization, track activities & notify

Security General Scenario (2)

- Response Measure
  - How much of a system is compromised when a particular component or data value is compromised
  - Time passed before an attack was detected
  - Number of attacks resisted
  - Time to recover from an attack
  - How much data was vulnerable to a particular attack
- Artifact
  - System services; data within, produced or consumed by the system; vulnerable parts in a system
- Environment
  - Online/offline, fire-walled/open, fully/partially/not operational

Security Tactics



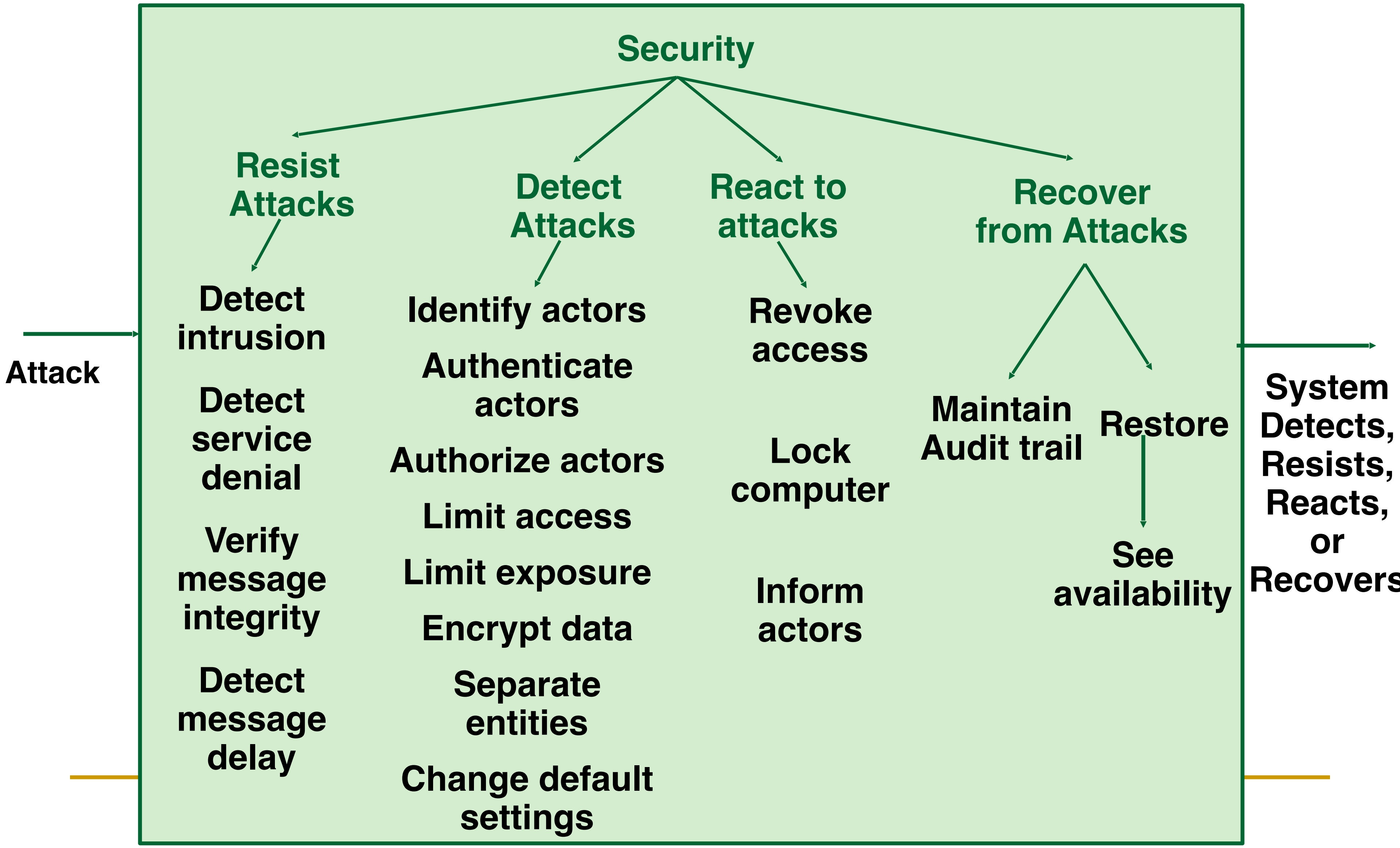
Attacks arrive

Tactics to Control Security

System detects, resists, reacts to or recovers from attacks

- Security tactics can be divided into four groups
  - Resisting attacks
  - Detecting attacks
  - Reacting to attacks
  - Recovering from attacks

Security Tactics Hierarchy



Attack

Security

Resist Attacks

Detect intrusion

Detect service denial

Verify message integrity

Detect message delay

Detect Attacks

Identify actors

Authenticate actors

Authorize actors

Limit access

Limit exposure

Encrypt data

Separate entities

Change default settings

React to attacks

Revoke access

Lock computer

Inform actors

Recover from Attacks

Maintain Audit trail

Restore

See availability

System Detects, Resists, Reacts, or Recovers

Detect Attacks: Detect Intrusion

- Comparing network traffic or service request patterns within a system to a set of signatures or known patterns of malicious behavior stored in a database
    - The signatures can be based on protocol, TCP flags, payload sizes, applications, source or destination address, or port number
    - Typically done with the help of an intrusion detection system (IDS)

Detect Attacks: Detect Service Denial

- Comparing the pattern or signature of network traffic coming into a system to historic profiles of known denial-of-service (DOS) attacks
- Typical forms of DOS attack
  - Local DOS against hosts
    - fork() bomb; intentionally generate errors to fill logs, consuming disk space, crashing
  - Network-based DOS
    - Flood attack, ping of death (PoD), smurf attack, DDOS

Detect Attacks: Verify Message Integrity

- Using techniques such as *checksums* or *hash* values to verify the integrity of messages, resource files, deployment files, and configuration files

Detect Attacks: Detect Message Delay

- Detecting message interception by checking the time it takes to deliver a message
  - When there are more variation in delivery time, such as in case of network congestion, more false alerts will result

Resist Attacks: Identify Actors

- Identifying the source of any external input to the system
  - User IDs, access codes, IP addresses, protocols, ports etc.

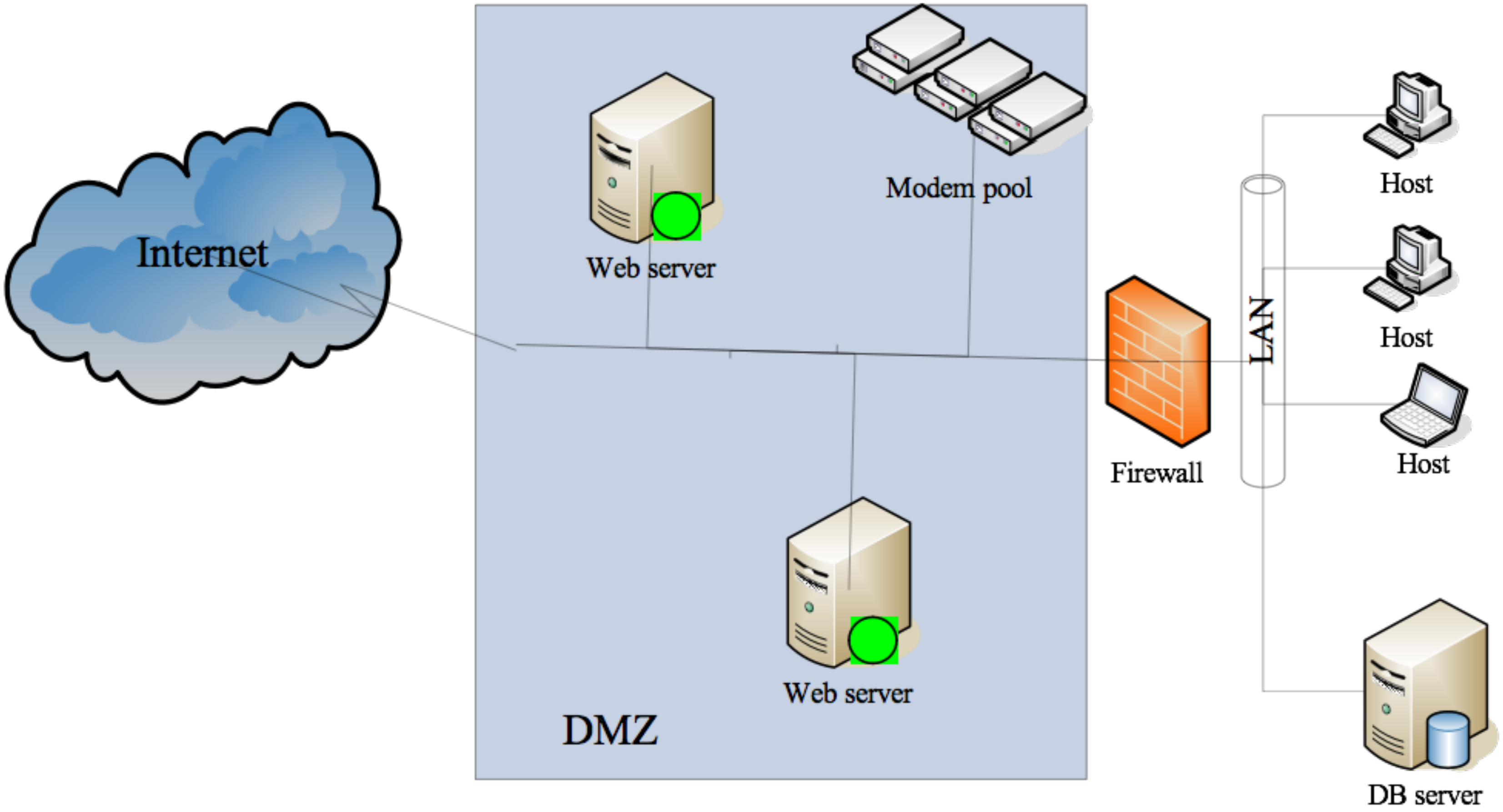
Resist Attacks: Authenticate & Authorize Actors

- Authenticate actors– assuring that an actor is actually who or what it says it is
  - Passwords
  - One-time passwords
  - Digital certificates
  - Biometric identification
  - ……
- Authorize actors– ensuring that an authenticated actor has the right to access/ modify data or services
  - Access control by privileges or by roles

Resist Attacks: Limit Access

- Memory protection, blocking a host, closing a port, or rejecting a protocol etc.
- Firewalls (source, destination port)
  - But it is not always possible to limit access to known sources, e.g. a public Web site.
- DMZ – demilitarized zone: access to Web but not to the rest of the LAN

DMZ


Internet
Web server
Modem pool
Firewall
LAN
Host
Host
Host
Web server
DMZ
DB server

Resist Attacks: Limit Exposure

- Attacks typically exploit a single weakness on a host to get access to all of its data
- Limit exposure is typically realized by having the least possible number of access points
  - The architect can minimize risk by allocation of services/data to hosts and limit exposure on each host

Resist Attacks: Encrypt Data

- Data should be protected from unauthorized access by applying some form of encryption to data and to communication
- Encryption of data
  - Symmetric key: DES→AES
  - Public-key encryption: RSA
- Encryption of communication links
  - SSL (Secure Sockets Layer)
  - VPN – virtual private networks

Resist Attacks: Separate Entities

- Physical separation on different servers that are attached to different networks
- Virtual machines
- "Air gap"
- Separate sensitive data from non-sensitive data

Resist Attacks: Change Default Settings

- Forcing the user to change default settings will prevent attackers from gaining access to the system through settings that are publicly available

React to Attacks: Revoke Access

- Revoke a system's or a user's access to sensitive resources when an attack is detected or expected. E.g.
  - When a computer is infected with virus, access to certain resources may be limited
  - Revoke the access of a user account when attack using this accout is detected

React to Attacks: Lock Computer

- Limit access from a particular computer if there are repeated failed attempts to access an account from that computer
  - E.g. Lock a computer when encountered with repeated failed login attempts
  - Usually only lock for a certain time period

React to Attacks: Inform Actors

- Ongoing attacks may require action by operators, other personnel, or cooperating systems
  - Notify these actors when a system attack is detected

Reading Assignment

- Read Chapter 9 & 10 of the textbook.