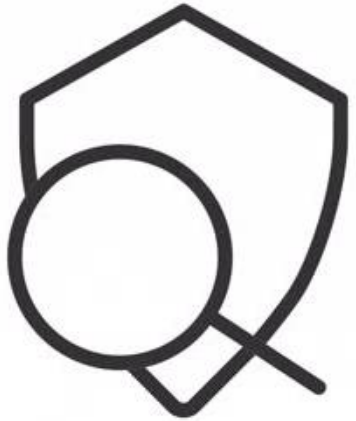
Introduction to Cybersecurity



Ashkan Jangodaz
British Columbia Institute of Technology

A Definition of Computer Security

- **Computer Security:** The protection afforded to an automated information system in order to attain the applicable objectives of preserving the **confidentiality, integrity**, and **availability** of information system resources (NIST):
  - Hardware
  - Software
  - Firmware
  - Information/data
  - Telecommunications

Security Objectives, CIA

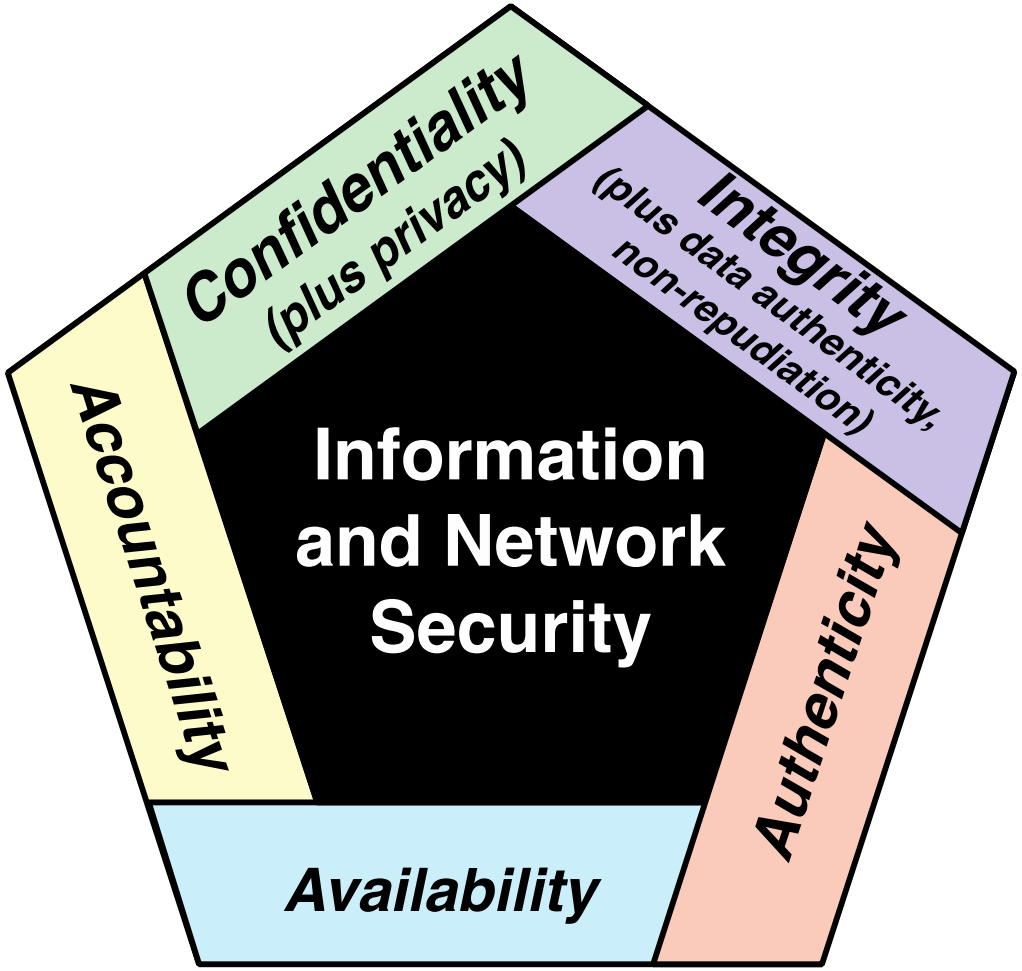


Figure 1.1 Essential Information and Network Security Objectives

Confidentiality

- **Confidentiality** covers two related concepts:
  - **Data confidentiality:** Assures that private or confidential information is not made available or disclosed to unauthorized individuals (Protecting Sensitive Data)
  - **Privacy:** Assures that individuals control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed

Integrity and Availability

- **Integrity** covers two related concepts:
  - **Data integrity:** Assures that data (both stored and in transmitted packets) and programs are changed only in a specified and authorized manner
  - **System integrity:** Assures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system
- **Availability:**
  - Assures that systems work promptly, and service is not denied to authorized users (Preventing Service Disruption)

Authenticity and Accountability

- **Authenticity:**
  - Ensuring that users are indeed who they claim to be and that all inputs to the system come from reliable sources
- **Accountability:**
  - The security principle that mandates the ability to uniquely trace and attribute actions to the responsible entity

* You can find some examples of the CIA in the 01-introduction-to-cybersecurity-notes.pdf document.

Security Terms – Vulnerability

- **Vulnerability** is a weakness or flaw in a system that a threat could exploit.
  - It can be a software, hardware, procedural, or human weakness that can be exploited.
- **Examples:**
  - Unpatched applications
  - Open port on a firewall
  - …

Security Terms – Threat

- **Threat** is any **potential danger** that could exploit a vulnerability to breach security and cause harm.
  - A threat agent could be an intruder accessing the network through a port on the firewall
  - A process accessing data in a way that violates the security policy
  - …

Security Terms – Exposure

- An **exposure** is an instance of being exposed to losses.
  - A vulnerability exposes an organization to possible damages.
- Examples:
  - If password management rules are not enforced, the organization is exposed to the possibility of having users' passwords compromised and used in an unauthorized manner.
  - If an organization does not have its wiring inspected and does not put proactive fire prevention steps into place, it exposes itself to potentially devastating fires.

Security Terms – Attack

- An **attack** is an **attempt to exploit a vulnerability** in order to **compromise an asset**, resulting in a violation of security goals.
- Examples:
  - Eavesdropping on network traffic
  - Packet sniffing
  - Traffic analysis
  - Man-in-the-Middle (MITM) attack
  - Replay attack
  - Denial-of-Service (DoS)
  - …

Passive Attack

- A **passive attack** attempts to learn or make use of information from the system
  - Does not affect system resources
  - Release of message contents and Traffic analysis
- Passive attacks are very difficult to detect
  - Because they do not involve any alteration of the data

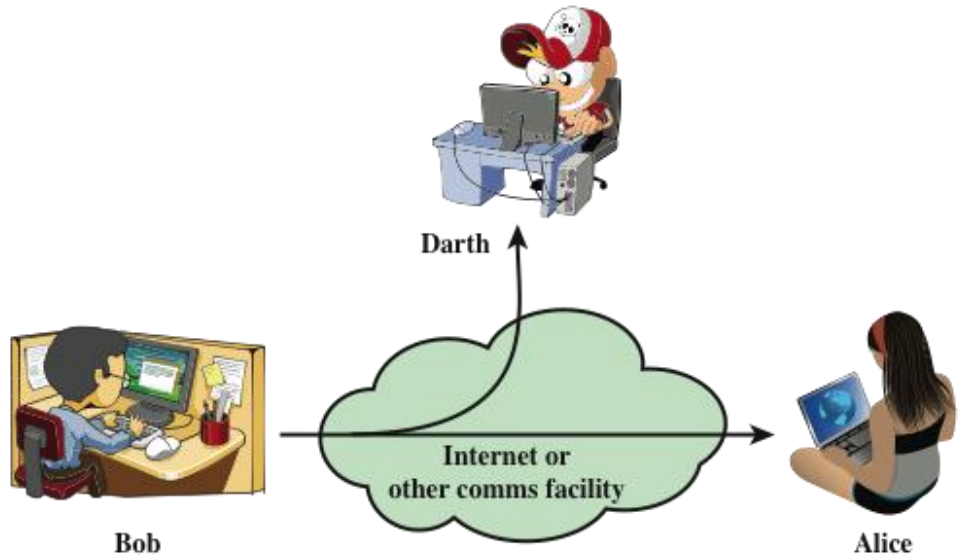
Active Attack

- An **active attack** attempts to alter system resources or affect their operation
  - Involves some modification of the data stream or the creation of a false stream, can be subdivided into four categories:
    1. Masquerade
    2. Replay
    3. Modification of messages
    4. Denial of service

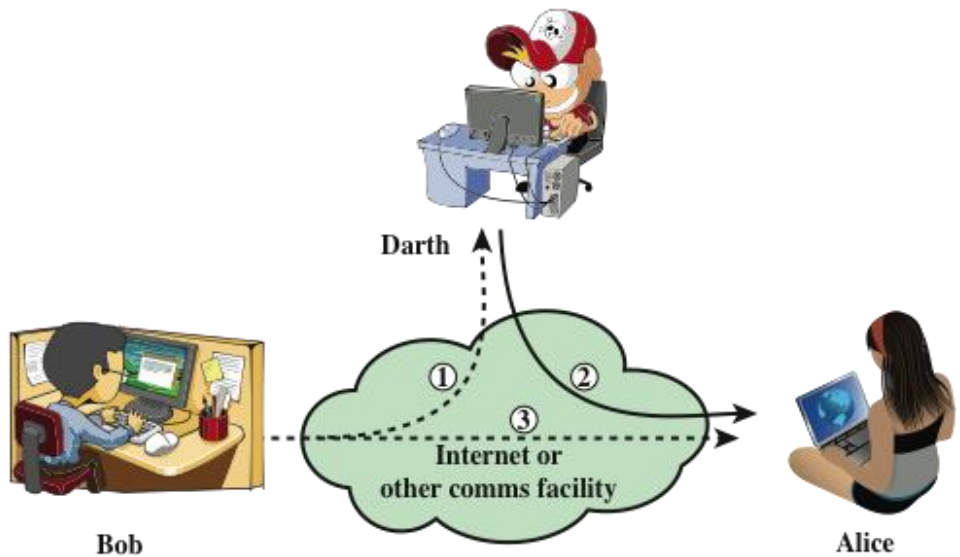
Active Attack

- Difficult to prevent because of the **wide variety** of potential physical, software, and network vulnerabilities
- Goal is to **detect** attacks and to **recover** from any disruption or delays caused by them

Masquerade	• Takes place when one entity pretends to be a different entity • Usually includes one of the other forms of active attack
Replay	• Involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect
Modification of messages	• Some portion of a legitimate message is altered, or messages are delayed or reordered to produce an unauthorized effect
Denial of service	• Prevents or inhibits the normal use or management of communications facilities

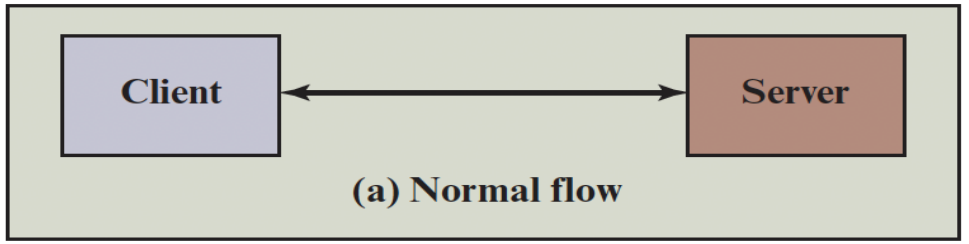


(a) Passive attacks

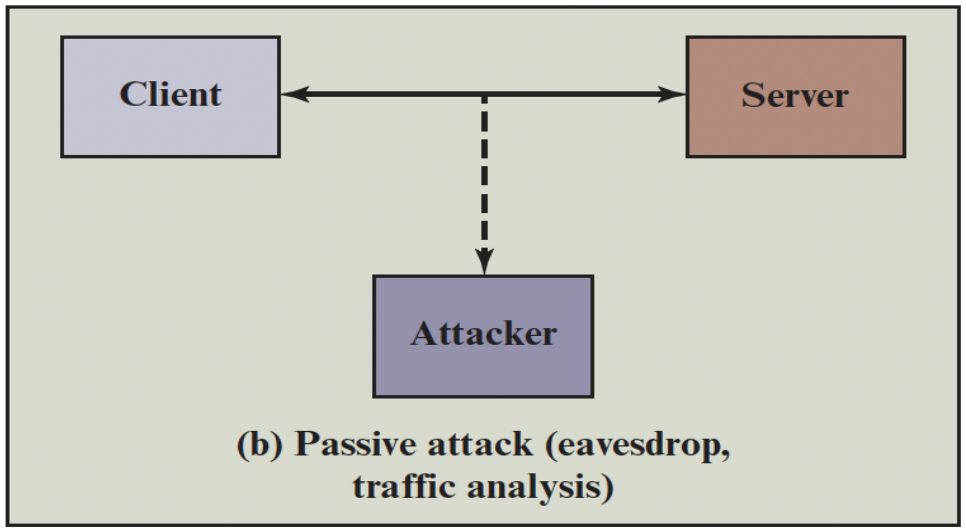


(b) Active attacks

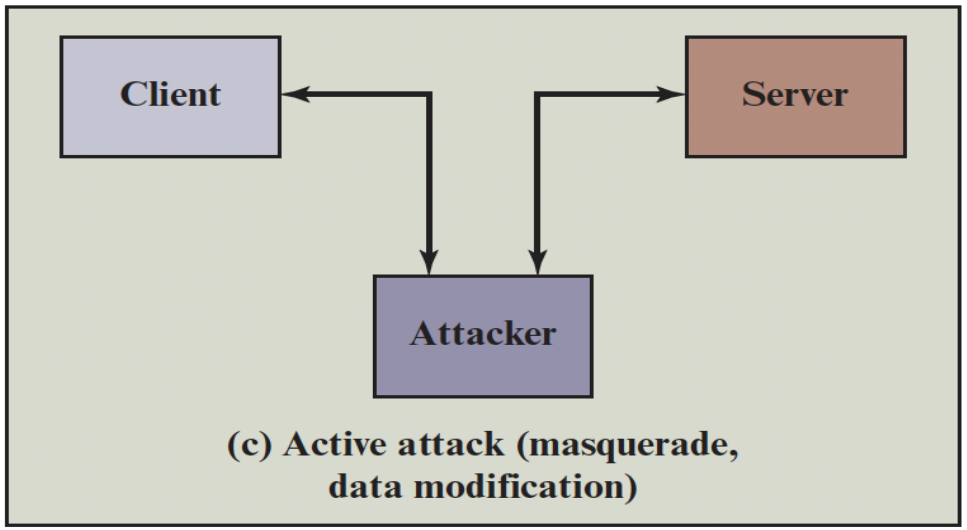
Figure 1.2 Security Attacks



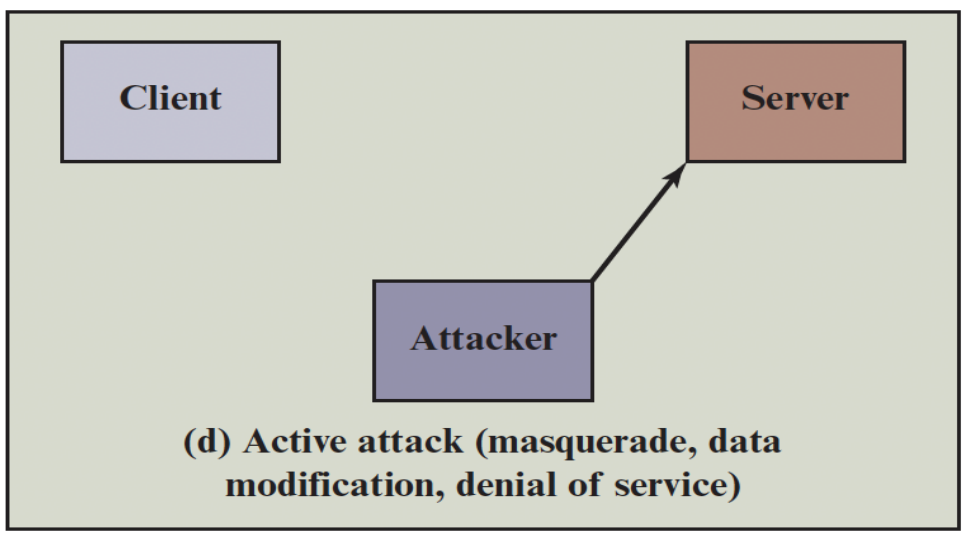
(a) Normal flow



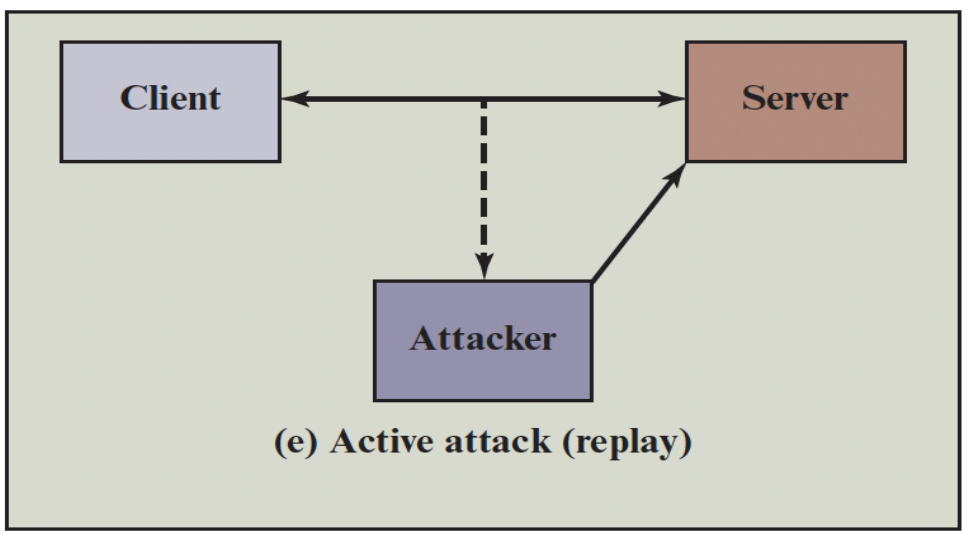
(b) Passive attack (eavesdrop, traffic analysis)



(c) Active attack (masquerade, data modification)



(d) Active attack (masquerade, data modification, denial of service)



(e) Active attack (replay)

Security Terms – Countermeasure

- A **control**, or **countermeasure**, is put into place to mitigate (reduce) the potential risk.
  - Strong password management
  - Firewalls
  - A security guard
  - Access control mechanisms
  - Encryption
  - Security awareness training
  - …

Security Terms – Asset

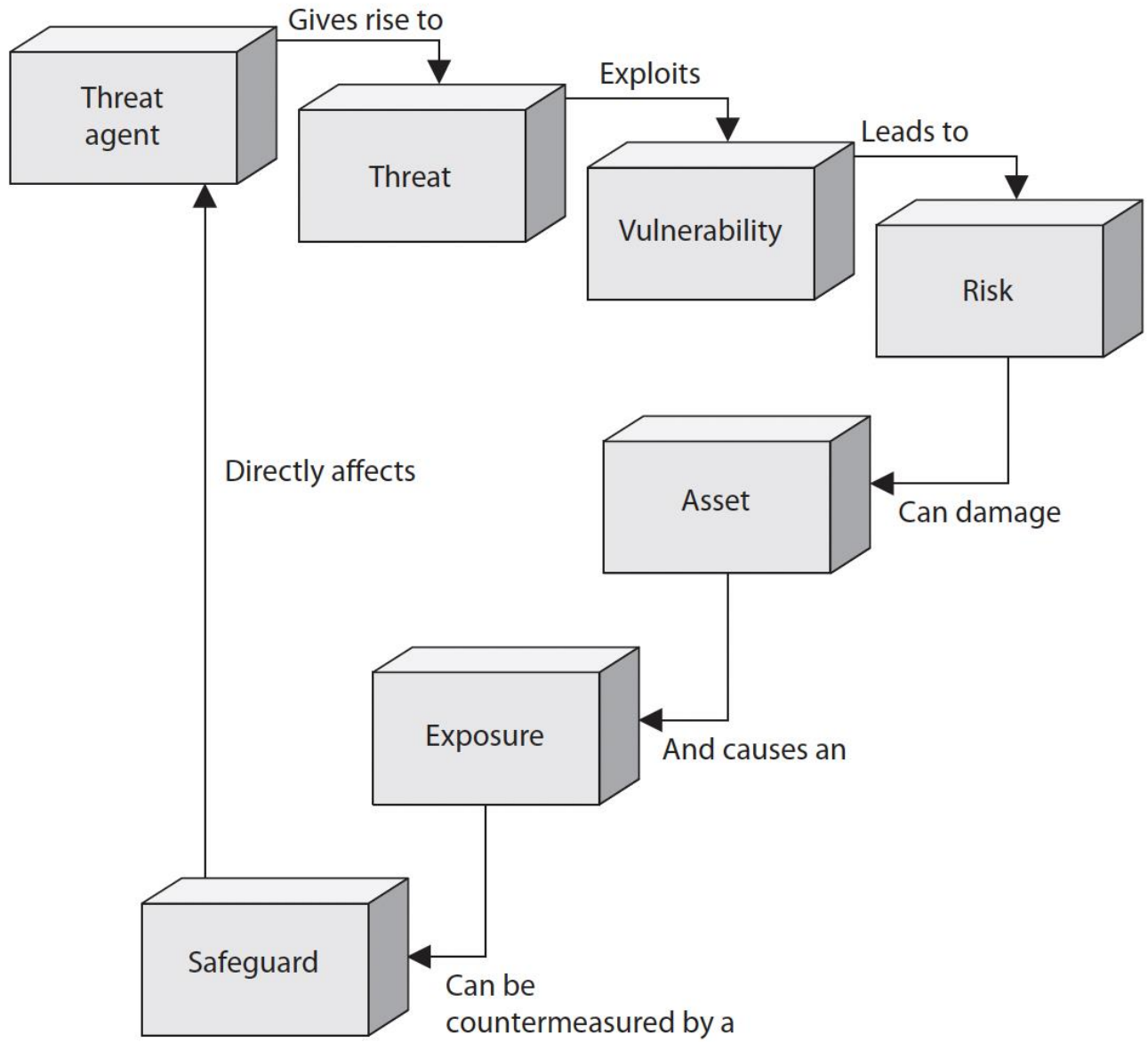
- An **asset** is **anything of value to an organization that must be protected** because its loss, compromise, or damage would negatively impact the organization.
  - Customer data
  - Servers and networking equipment
  - Operating systems
  - Databases
  - …

Security Terms – Risk

- A **risk** is the likelihood of a threat source exploiting a vulnerability and the corresponding business impact.
  - Risk ties the vulnerability, threat, and likelihood of exploitation to the resulting business impact.
- A **security risk** is a **path** to a specific asset that results in observable damage.
- Every meaningful security concern can be explained as:

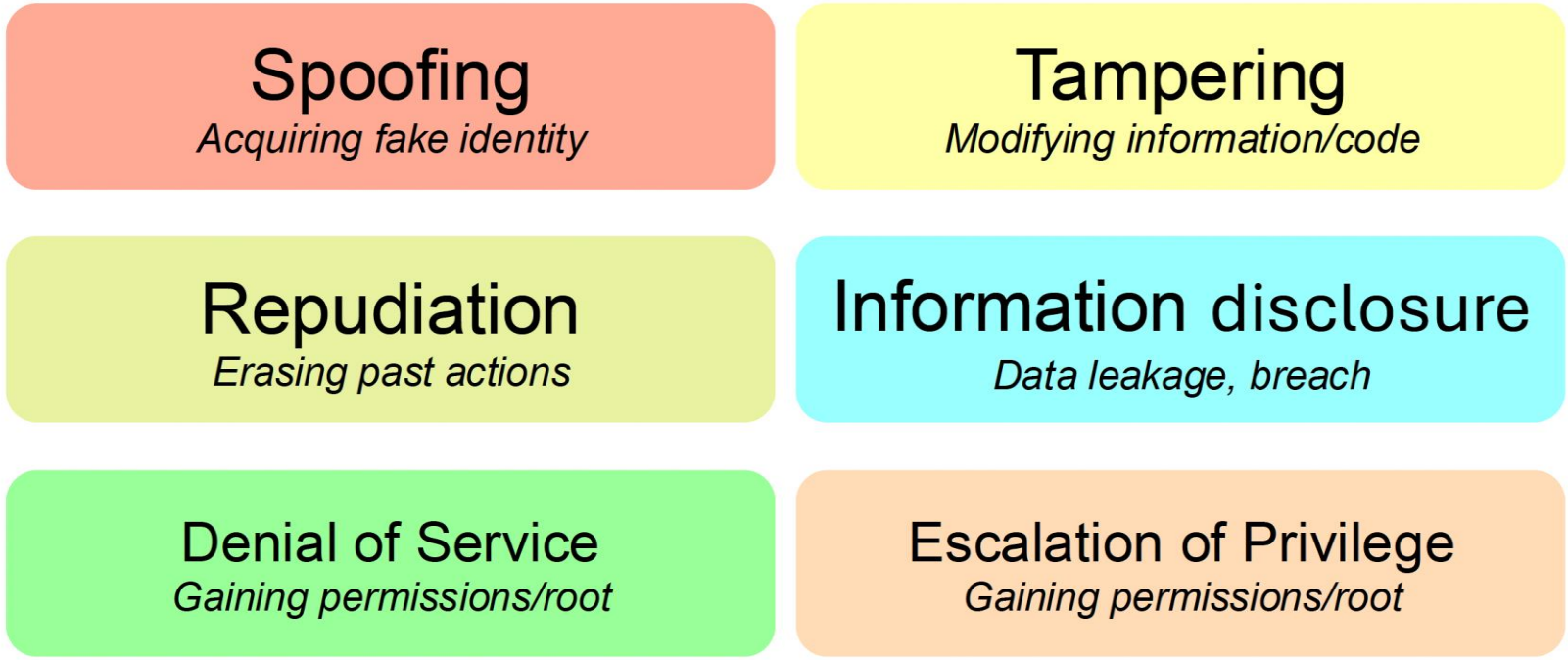
Asset → Entry Point → Weak Spot → Damage

Figure 1-1
The relationships among the different security concepts



Threat Model

- **Threat modeling** is the process of identifying and reviewing paths to assets that could lead to damage.
- **STRIDE** is a framework for classifying security threats by the kind of harm they cause.



Asset (what must not be harmed)

- An **asset** is a specific system object or function that matters.
  - A database table containing customer records
  - A payroll calculation function
  - A report generation pipeline
  - …

Entry Point (where typical activity begins)

- An **entry point** is a routine, legitimate way to start an interaction
  - A user logging in
  - A scheduled background job
  - A support workflow
- Entry points (workflows):
  - “User authentication workflow”
  - “Administrative task scheduler”
- Not entry points (attacks, not workflows):
  - “SQL injection on the login form”

Weak Spot (the condition that lowers resistance)

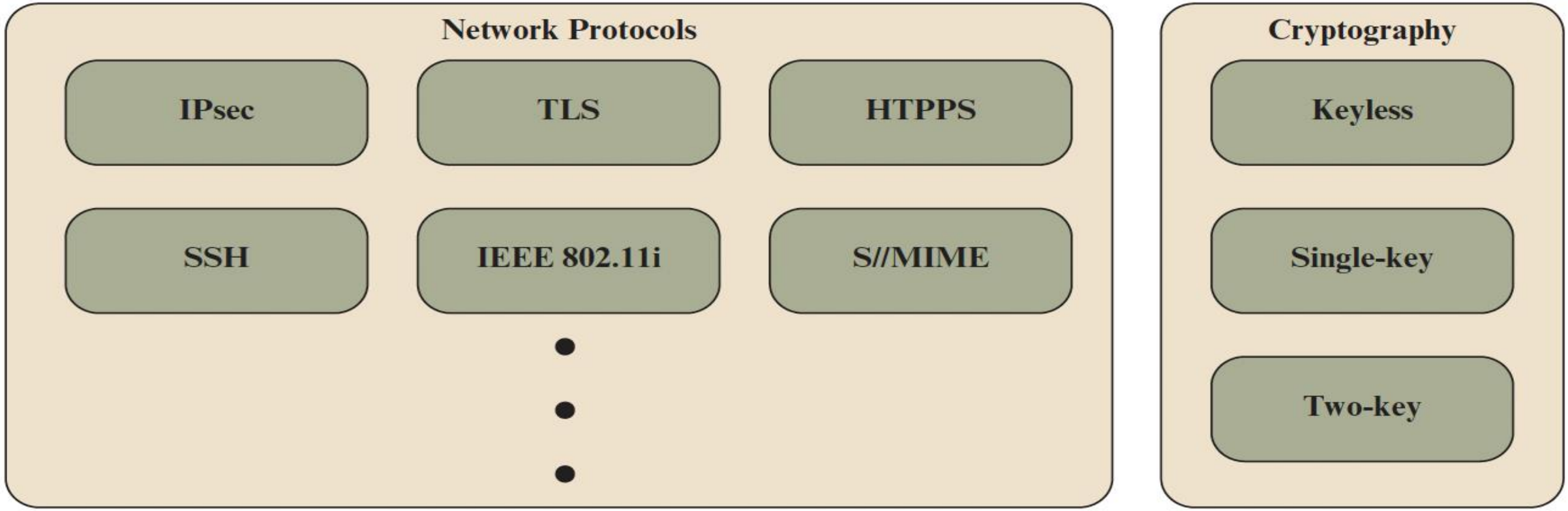
- A **weak spot** is a present-tense condition that exists right now.
  - Access is broader than responsibility
  - Changes can occur without review or evidence
  - State transitions lack authorization checks
  - …

Damage (what actually goes wrong)

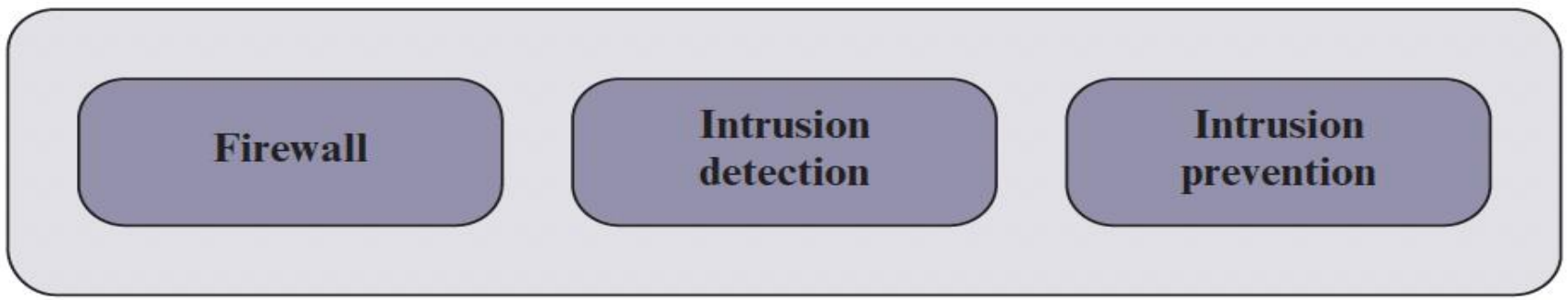
- **Damage** is the observable outcome if the path completes.
- Good damage descriptions:
  - “Invoices contain incorrect totals.”
  - “Private records are visible to unauthorized staff.”
  - “Reports are not delivered before the deadline.”
- Bad damage descriptions:
  - “The system is compromised.”
  - “This could be hacked.”

Network Vulnerabilities

- **Network vulnerabilities** are weaknesses or flaws in a network's design, configuration, implementation, or operation that can be exploited by an attacker.
  - Misconfigured firewalls or routers
  - Unpatched network services
  - Weak or unencrypted network protocols
  - Open or unused ports
  - Poor network segmentation
  - …



(a) Communications Security



(b) Device Security

Figure 1.5 Key Elements of Network Security

Code Vulnerabilities

- **Software vulnerabilities** are weaknesses or flaws in software design, implementation, or configuration that can be exploited by an attacker.
- These issues can allow attackers to execute arbitrary code, gain unauthorized access, or manipulate data
  - Such as **buffer overflows** and **SQL injection** flaws, can be particularly damaging in software development
  - Secure coding practices, such as **proper input validation** and **memory management**, mitigate these risks and ensure application security

Social engineering

- Attacks **psychologically** manipulate people into doing things that they shouldn't do, like downloading malware
  - Most common one, **Phishing** attack, involves tricking individuals into revealing personal information or installing malware through deceptive emails or messages
- It remains one of the most effective methods for attackers to gain initial access to systems
- Phishing was the leading infection vector, identified in 41% of incidents, making it the most common initial attack vector (IBM)

Malware

- Malware short for "**malicious software**" is a software that is **written intentionally** to harm a computer system or its users
  - Almost every modern cyberattack involves some type of malware
- Types of Malware:
  - Viruses
  - Worms
  - Trojan horses
  - Ransomwares
  - …

Virus

- Virus is malicious code that **hijacks** legitimate software to do damage and spread copies of itself
- **Viruses can't act on their own**
  - They hide snippets of their code in other executable programs
- When a user starts the program, the virus begins running, too
- Viruses are usually designed to delete important data, disrupt normal operations, and spread copies of themselves to other programs on the infected computer

Worms

- Worms are **self-replicating** malicious programs that can spread between apps and devices **without human interaction**
  - Compared to a virus, which can only spread if a user runs a compromised program
- While some worms do nothing more than spread, many have more severe consequences
  - For example, the WannaCry ransomware, which caused an estimated USD 4 billion in damages, was a worm that maximized its impact by automatically spreading between connected devices (IBM)

Trojans

- Trojan horses **disguise themselves as useful programs** or hide within legitimate software to trick users into installing them.

Ransomware

- Ransomware **locks up** a victim's devices or data and demands a ransom payment, usually in the form of cryptocurrency, to unlock them
- Cybercriminals may use additional tactics to increase the pressure on victims
  - In a double extortion attack, cybercriminals steal data and threaten to leak it if they're not paid


Wana Decrypt0r 2.0
Ooops, your files have been encrypted!
English
Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37
Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37
What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.
Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.
How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am
bitcoin ACCEPTED HERE
Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
Copy
About bitcoin
How to buy bitcoins?
Contact Us
Check Payment
Decrypt

Denial of Service (DoS)

- **DoS** attacks aim to make systems or networks **unavailable** by overwhelming them with traffic or triggering crashes
- Distributed Denial of Service (**DDoS**) attacks involve multiple compromised systems flooding a target
  - Making them even more difficult to defend against
- Some common types:
  - Application layer attacks (HTTP Flood)
  - Protocol attacks

The OSI Security Architecture

- **Security attack:** Any action that compromises the security of information owned by an organization
- **Security mechanism:** A process (or a device incorporating such a process) that is designed to detect, prevent, or recover from a security attack
- **Security service:** A processing or communication service that enhances the security of the data processing systems and the information transfers of an organization. **The services** are intended to counter security attacks, and they **make use of one or more security mechanisms** to provide the service

AUTHENTICATION

The assurance that the communicating entity is the one that it claims to be.

Peer Entity Authentication
Used in association with a logical connection to provide confidence in the identity of the entities connected.

Data-Origin Authentication
In a connectionless transfer, provides assurance that the source of received data is as claimed.

ACCESS CONTROL

The prevention of unauthorized use of a resource (i.e., this service controls who can have access to a resource, under what conditions access can occur, and what those accessing the resource are allowed to do).

DATA CONFIDENTIALITY

The protection of data from unauthorized disclosure.

Connection Confidentiality
The protection of all user data on a connection.

Connectionless Confidentiality
The protection of all user data in a single data block

Selective-Field Confidentiality
The confidentiality of selected fields within the user data on a connection or in a single data block.

Traffic-Flow Confidentiality
The protection of the information that might be derived from observation of traffic flows.

DATA INTEGRITY

The assurance that data received are exactly as sent by an authorized entity (i.e., contain no modification, insertion, deletion, or replay).

Connection Integrity with Recovery
Provides for the integrity of all user data on a connection and detects any modification, insertion, deletion, or replay of any data within an entire data sequence, with recovery attempted.

Connection Integrity without Recovery
As above, but provides only detection without recovery.

Selective-Field Connection Integrity
Provides for the integrity of selected fields within the user data of a data block transferred over a connection and takes the form of determination of whether the selected fields have been modified, inserted, deleted, or replayed.

Connectionless Integrity
Provides for the integrity of a single connectionless data block and may take the form of detection of data modification. Additionally, a limited form of replay detection may be provided.

Selective-Field Connectionless Integrity
Provides for the integrity of selected fields within a single connectionless data block; takes the form of determination of whether the selected fields have been modified.

NONREPUDIATION

Provides protection against denial by one of the entities involved in a communication of having participated in all or part of the communication.

Nonrepudiation, Origin
Proof that the message was sent by the specified party.

Nonrepudiation, Destination
Proof that the message was received by the specified party.

Table 1.2

Security Services (X.800)

(This table is found on page 12 in the textbook)

SPECIFIC SECURITY MECHANISMS	PERVASIVE SECURITY MECHANISMS
May be incorporated into the appropriate protocol layer in order to provide some of the OSI security services.	Mechanisms that are not specific to any particular OSI security service or protocol layer.
Encipherment The use of mathematical algorithms to transform data into a form that is not readily intelligible. The transformation and subsequent recovery of the data depend on an algorithm and zero or more encryption keys.	**Trusted Functionality** That which is perceived to be correct with respect to some criteria (e.g., as established by a security policy).
Digital Signature Data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery (e.g., by the recipient).	**Security Label** The marking bound to a resource (which may be a data unit) that names or designates the security attributes of that resource.
Access Control A variety of mechanisms that enforce access rights to resources.	**Event Detection** Detection of security-relevant events.
Data Integrity A variety of mechanisms used to assure the integrity of a data unit or stream of data units.	**Security Audit Trail** Data collected and potentially used to facilitate a security audit, which is an independent review and examination of system records and activities.
Authentication Exchange A mechanism intended to ensure the identity of an entity by means of information exchange.	**Security Recovery** Deals with requests from mechanisms, such as event handling and management functions, and takes recovery actions.
Traffic Padding The insertion of bits into gaps in a data stream to frustrate traffic analysis attempts.	
Routing Control Enables selection of particular physically secure routes for certain data and allows routing changes, especially when a breach of security is suspected.	
Notarization The use of a trusted third party to assure certain properties of a data exchange.	

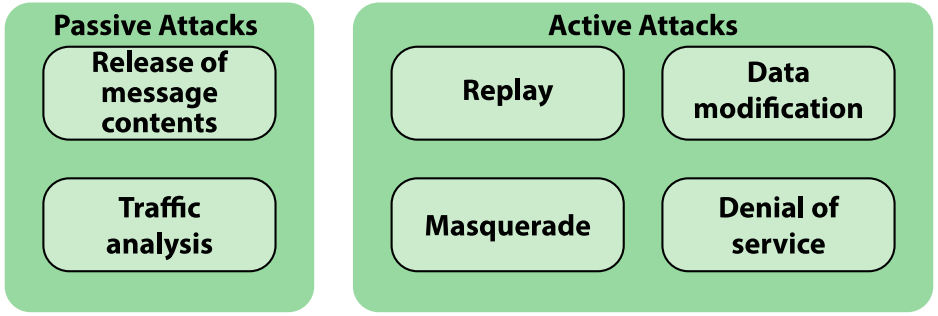
Table 1.3

Security Mechanisms (X.800)

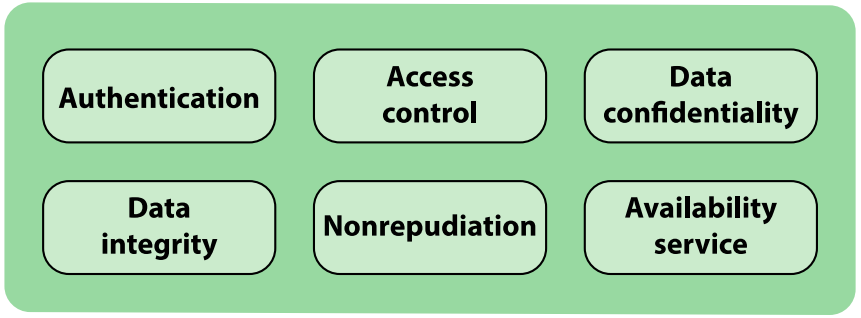
(This table is found on page 12 in the textbook)

Service	Encipherment	Digital signature	Access control	Data integrity	Authentication exchange	Traffic padding	Routing control	Notarization
	Mechanism							
Peer entity authentication	Y	Y			Y			
Data origin authentication	Y	Y						
Access control			Y					
Confidentiality	Y						Y	
Traffic flow confidentiality	Y					Y	Y	
Data integrity	Y	Y		Y				
Nonrepudiation		Y		Y				Y
Availability				Y	Y			

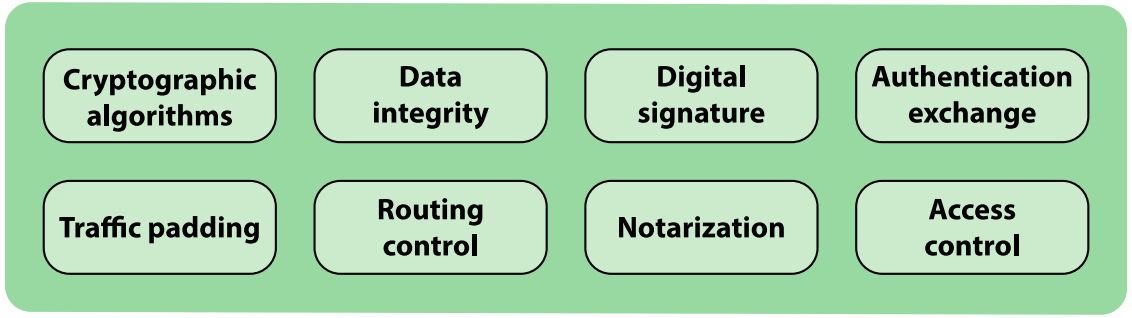
Table 1.4 Relationship Between Security Services and Mechanism (X.800)



(a) Attacks



(b) Services



(c) Mechanisms

Key Concepts in Security

Data **at Rest**

vs.

Data **in Motion**

vs.

Data **in Transit**

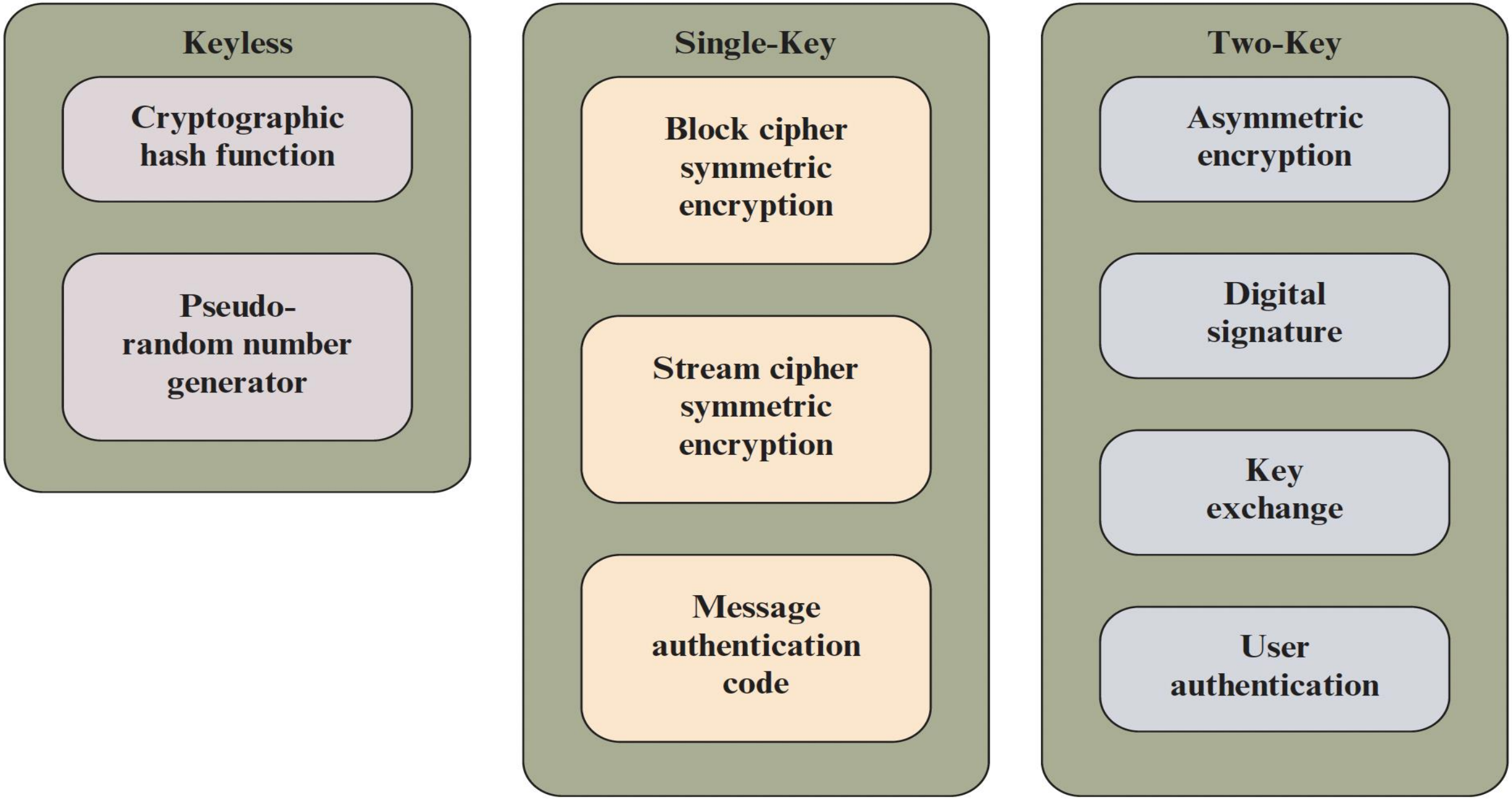


Figure 1.4 Cryptographic Algorithms

Authentication

- Concerned with assuring that a communication is **authentic**
  - **A single message:** assures the recipient that the message is from the source that it claims to be from
  - **Ongoing interaction:** assures the two entities are authentic and that the connection is not interfered with in such a way that a third party can masquerade as one of the two legitimate parties

Two specific authentication services are defined in X.800:

- **Peer entity authentication**
- **Data origin authentication**

Access Control

- These controls **restrict** who can access information or systems based on **roles**, **responsibilities**, and the **principle of least privilege**
- To achieve this, each entity trying to gain access must first be **identified**, or **authenticated**, so that access rights can be tailored to the individual
- This approach ensures minimizing the risk of insider threats and unauthorized access

Data Confidentiality

- The protection of transmitted data **from passive attacks**
  - Broadest service protects all user data transmitted between two users over a period of time
- The protection of traffic flow **from analysis**
  - This requires that an attacker not be able to observe the source and destination, frequency, length, or other characteristics of the traffic on a communications facility

Data Integrity

- Can apply to a **stream of messages**, a **single message**, or **selected fields** within a message
  - **Connection-oriented integrity** service **deals with a stream of messages** and assures that messages are received as sent with no duplication, insertion, modification, reordering, or replays
  - A **connectionless integrity** service **deals with individual messages** without regard to any larger context and generally provides protection against message modification only

Nonrepudiation

- Prevents either sender or receiver **from denying a transmitted message**
  - When a message is sent, the receiver can prove that the alleged sender in fact sent the message
  - When a message is received, the sender can prove that the alleged receiver in fact received the message

Availability service

- **Availability**
  - The property of a system or a system resource being accessible and usable upon demand by an authorized system entity
- **Availability service**
  - One that protects a system to ensure its availability
  - Addresses the security concerns raised by denial-of-service attacks
  - Depends on proper management and control of system resources

Firewall

- Firewalls are a barrier between trusted and untrusted networks, **filtering incoming and outgoing traffic** based on **predefined security rules**
  - A **hardware** and/**or software** capability that limits access between a network and devices attached to the network
  - In accordance with a specific security policy
- The **firewall acts as a filter** using a set of rules based on traffic content and/or traffic pattern

Firewall

- Different types of firewalls:
  - Packet filtering
  - Stateful inspection
  - Next-generation firewalls
- Each type of firewall has its strengths and is suitable for different scenarios
  - Selecting the appropriate one based on specific needs is vital for effective protection

Intrusion Detection/Prevention System

- **IDS:** Hardware or software products that gather and analyze information from various areas within a computer or a network for the purpose of finding
  - Providing real-time or near-real-time warning of, attempts to access system resources in an unauthorized manner
- **IPS:** Hardware or software products designed to detect intrusive activity and attempt to stop the activity, ideally before it reaches its target

Attack surface

- Consists of the reachable and exploitable vulnerabilities in a system
  - Network attack surface
  - Software attack surface
  - Human attack surface
  - …

The Challenges of Computer Security

1. Security is not simple
2. Potential attacks on the security features need to be considered
3. Procedures used to provide particular services are often counter-intuitive
4. It is necessary to decide where to use the various security mechanisms
5. Requires constant monitoring
6. Is too often an afterthought

The Challenges of Computer Security

7. Security mechanisms typically involve more than a particular algorithm or protocol
8. Security is essentially a battle of wits between a perpetrator and the designer
9. Little benefit from security investment is perceived until a security failure occurs
10. Strong security is often viewed as an impediment to efficient and user-friendly operation

References

1. Stallings, W. (2016). Network security essentials: Applications and standards (6th ed.). Pearson.
2. Stallings, W. (2020). Cryptography and network security (8th ed.). Pearson.
3. Maymí, F., & Harris, S. (2021). CISSP all-in-one exam guide (9th ed.). McGraw-Hill.