Intro to security

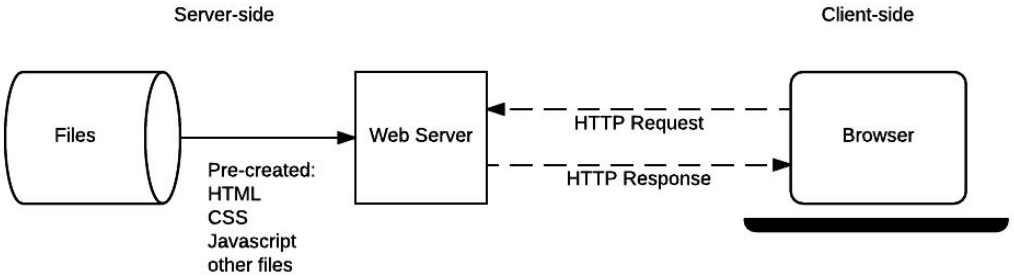
Slides are based on **Introduction to Computer Security : Bishop, Matt**

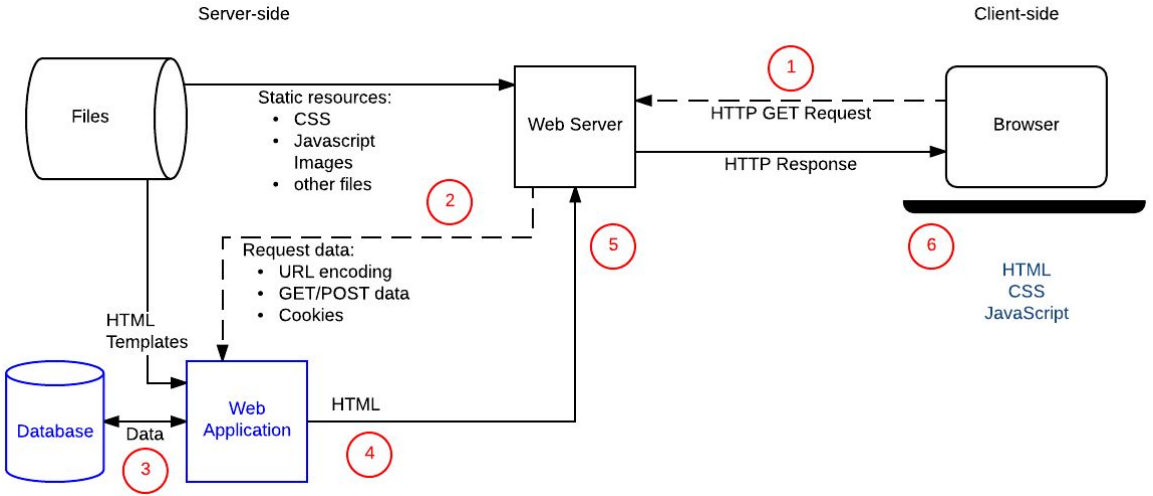
https://cs.lmu.edu/~ray/notes/introsecurity/

Many security terms and definitions

Some practical examples

Last lecture: Static sites & dynamic sites



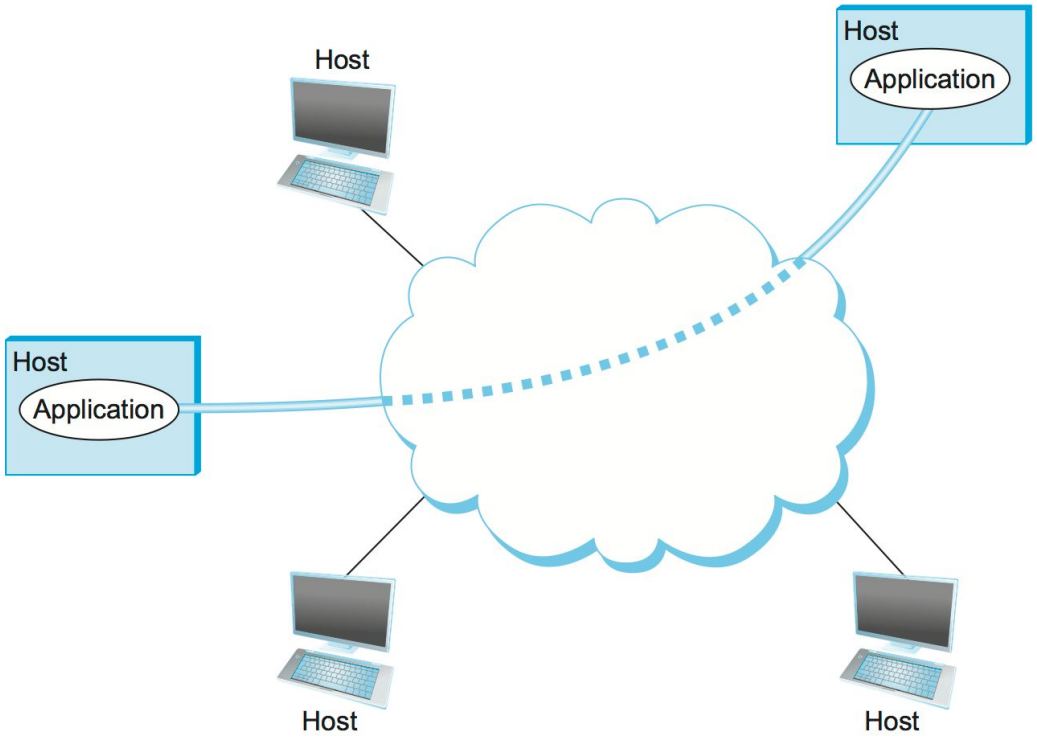


https://developer.mozilla.org/en-US/docs/Learn/Server-side/First_steps/Introduction

Last lecture: Transmission of data over a network

- Transmission of data over a network
  - LAN, WAN, internet
  - Layered architecture
    - Protocols
      - HTTP, IP, etc
    - IP routing
    - Port numbers

..



https://book.systemsapproach.org

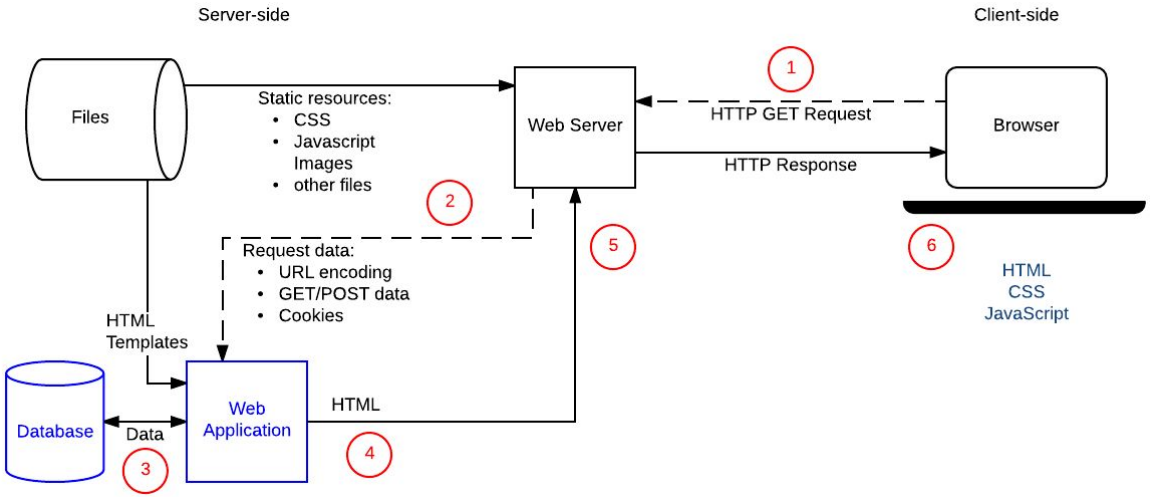
This week: How to secure data?

Secure data transmission

Secure data storage

Secure data access

etc.



What to protect?

Basic security components: (CIA)

Confidentiality

the concealment of information or resources

- You cannot enter some offices in university
- You cannot see information of other students in ubys.medeniyet.edu.tr

Access control mechanisms support confidentiality.

- Example: **a cryptographic key:** scramble data so only people with the key can read/understand

Integrity

the trustworthiness of data or resources

- data integrity
- origin integrity
  - **Authentication:** source of data

Integrity mechanisms

- prevention mechanisms
  - Blocking any unauthorized attempts to change the data
  -
- detection mechanisms.
  - report that the data's integrity is no longer trustworthy

Availability

the ability to use the information or resource desire

Attempts to block availability, called **denial of service attacks**

More examples on confidentiality

Example confidential information

- Medical records?
- Student records?
-

Threats to security

A threat is a potential violation of security.

- The violation need not actually occur for there to be a threat

The fact that the violation **might occur** means that

- those actions that could cause it to occur must be guarded against (or prepared for)

Attacks: Those actions

Attackers: Those who execute such actions

Many threats fall into 4 main classes

1. **Disclosure,**
   - unauthorized access to information;
2. **Deception**
   - acceptance of false data
3. **Disruption**
   - interruption or prevention of correct operation
4. **Usurpation**
   - unauthorized control of some part of a system

Threats:Snooping

The unauthorized interception of information, is a form of disclosure

It is passive, suggesting simply that some entity is listening to (or reading) communications or browsing through files or system information

Wiretapping, or **passive wiretapping**, is a form of snooping in which a network is monitored

Confidentiality services counter this threat

Threats:Modification or alteration

an unauthorized change of information,

- covers three classes of threat

The goal may be deception

Unlike snooping, modification is active

- **man-in-the-middle attack**: an intruder reads messages from the sender and sends (possibly modified) versions to the recipient
    - Integrity services counter this threat

Threats: Masquerading or spoofing

an impersonation of one entity by another,

- is a form of both deception and usurpation.

It lures a victim into believing that the entity with which it is communicating is a different entity

Delegation(an allowed form of masquerading): one entity authorizes a second entity to perform functions on its behalf

if a user tries to log into a computer across the Internet but instead reaches another computer that claims to be the desired one,

- **the user has been spoofed!**

Threats: Repudiation of origin

a false denial that an entity sent (or created) something,

- a form of deception

Threats: Denial of receipt

a false denial that an entity received some information or message,

- a form of deception.

Threats: Delay

a temporary inhibition of a service

- a form of usurpation
- can play a supporting role in deception.

Let’s say: delivery of a message or service requires some time t;

- **delay**: an attacker can force the delivery to take more than time t,

If an entity is waiting for an authorization message that is delayed,

- it may query a secondary server for the authorization.
    - The attacker may be unable to masquerade as the primary server,
        - may masquerade as that secondary server and supply incorrect information

Threats: Denial of service

a long-term inhibition of service

- a form of usurpation
- often used with other mechanisms to deceive

denial may occur

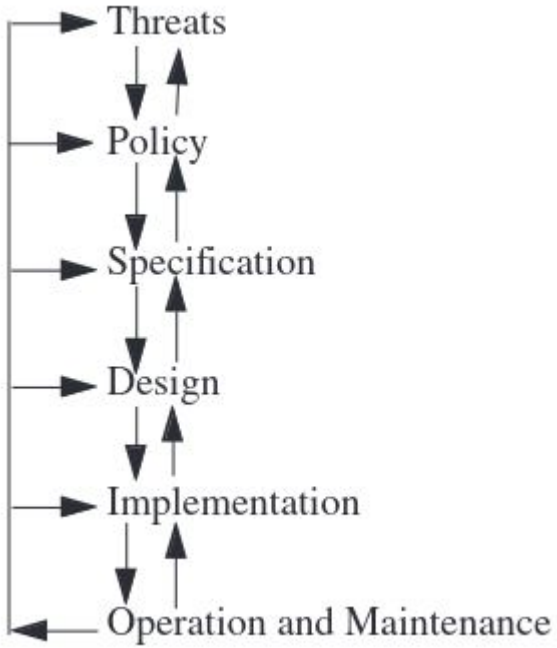
- at the source
  - preventing the server from obtaining the resources needed to perform its function
- at the destination
  - blocking the communications from the server
- or along the intermediate path
  - discarding messages from either the client or the server, or both

Availability mechanisms counter this threat.

Denial of service or delay may result from **direct attacks** or from **non-security related** problems

- we view it as an attempt to breach system security
  - it compromises system security,
  - or is part of a sequence of events leading to the compromise of a system,

Security life cycle



Human issues pervade each stage of the cycle and each cycle feeds info back

Example:A major corporation decided to improve its security.

- It hired consultants,
- determined the threats,
- and created a policy.
- From the policy, the consultants derived several specifications that the security mechanisms had to meet.
- They then developed a design that would meet the specifications
- During the implementation phase,
  - the company discovered that employees could connect modems to the telephones without being detected.
  - The design required all incoming connections to go through a firewall
  - **The design had to be modified to** divide systems into two classes:
    - systems connected to “the outside,” which were put outside the firewall;
    - and all other systems, which were put behind the firewall.
  -
- **The operation and maintenance stage is critical to the life cycle**
  - The company discovers that several “trusted” hosts (those allowed to log in without authentication) were physically outside the control of the company.
    - **This violates policy!**

Operational Issues

Cost-Benefit Analysis

Example: salary info of employees

- If database altered, it is **financial loss!**
  - Requires strongest possible integrity mechanism
- If we distribute copies to branch offices and the salaries are not distributed based on this copies
  - The copies are not as important as the original database since they are not used!
    - **No financial loss**

Risk Analysis

To determine whether an asset should be protected, and to what level, requires analysis of the potential threats against that asset and the likelihood that they will materialize.

- likely /unlikely attacks

Operational Issues

Laws and Customs

- **Laws restrict the availability and use of technology and affect procedural controls.**

Example: US has imported restrictions on Huawei

- Any security policy depends on Huawei manufactured device needs to take this account.

Human Issues

- Organizational Problems
- People Problems
  - The heart of any security system is people
  - You can bypass many technological controls by human intervention
  - Many successful break-ins have arisen from the art of **social engineering.**
  -

Basic Cryptography

The word cryptography comes from two Greek words meaning

- “secret writing” and
- is the art and science of concealing meaning.

Classical cryptosystems (single-key or symmetric cryptosystems)

cryptosystems that use **the same key** for **encipherment** and **decipherment**.

Transposition Ciphers: rearranges characters, the key is a permutation function

Example: “HELLO, WORLD” ->

HLOOL
ELWRD
+
—----------
“HLOOLELWRD.”

Cesar cipher

“HELLO” in alphabet positions

7 4 11 11 14

Choose a shift(key) **k**

New code = (26+c-k) mod 26

Example: k=3

10 7 14 14 1

You can also use ASCII codes!

Classical cryptosystems (single-key or symmetric cryptosystems)

Substitution Ciphers

A substitution cipher changes characters in the plaintext to produce the ciphertext.

- **Cesar cipher**
- **Vigenère Cipher**
  - **A longer key, uses a tableau**

	A	*B*	*C*	*D*	*E*	*F*	*G*	*H*	*I*	*J*	*K*	*L*	*M*
A	A	B	C	D	E	F	G	H	I	J	K	L	M
B	B	C	D	E	F	G	H	I	J	K	L	M	N
C	C	D	E	F	G	H	I	J	K	L	M	N	O
D	D	E	F	G	H	I	J	K	L	M	N	O	P
E	E	F	G	H	I	J	K	L	M	N	O	P	Q
F	F	G	H	I	J	K	L	M	N	O	P	Q	R
G	G	H	I	J	K	L	M	N	O	P	Q	R	S

EXAMPLE: The first line of a limerick is enciphered using the key "BENCH," as follows.

Key	B	ENCHBENC	HBENC	HBENCH	BENCHBENCH
Plaintext	A	LIMERICK	PACKS	LAUGHS	ANATOMICAL
Ciphertext	B	PVOLSMPM	WBGXU	SBYTJZ	BRNVVNMPCS

One-Time Pad: if the key as long as the text

Public Key Cryptography

Two keys: encipherment and decipherment keys

Public (encipherment) **key** is public!

Private (decipherment) **key** is know only to owner!

RSA

$$c = m^e \bmod n$$

$$m = c^d \bmod n$$

- **φ(n)**
  - **the number of numbers less than n with no factors in common with n**
- **Choose e: e < n relatively prime to φ(n).**
- **Find d: ed mod φ(n) = 1**

The public key is (e, n)

the private key is d

n = pq, p and q primes

In addition to confidentiality, RSA can provide data and origin authentication.

RSA Example

Let p = 7 and q = 11.

Then n = 77 and φ(n) = 60.

Alice chooses e = 17,

so her private key is d = 53.

- **ed mod φ(n) = 1**
  - 17x53 mod 60 = 1

00 (A) and 25 (Z); 26 represents a blank

“HELLO WORLD.”

07 04 11 11 14 26 22 14 17 11 03.

07 17 mod 77 = 28

04 17 mod 77 = 16

11 17 mod 77 = 44

...

03 17 mod 77 = 75

or 28 16 44 44 42 38 22 42 19 44 75.

Cryptographic Checksums

Alice wants to send Bob a message of n bits.

She wants Bob to be able to verify that the message he receives is the same one that was sent.

checksum function: a mathematical function she applies to generate a smaller set of k bits from the original n bits.

This smaller set is called the **checksum** or **message digest**.

When Bob gets the message, he recomputes the checksum and compares it with the one Alice sent.

- If they match, he assumes that the message has not been changed.

Cryptographic Checksums

A cryptographic checksum function(a strong hash function or a strong one-way function)

h: A → B is a function:

- For any x ∈ A,
  - h(x) is easy to compute
- For any y ∈ B,
  - it is **computationally infeasible** to find x ∈ A such that h(x) = y.
- it is **computationally infeasible** to collision:
  - x, x´ ∈ A,
  - for **x ≠ x´** and **h(x) = h(x´).**
    - a collision.
-

Key management

Session and Interchange Keys

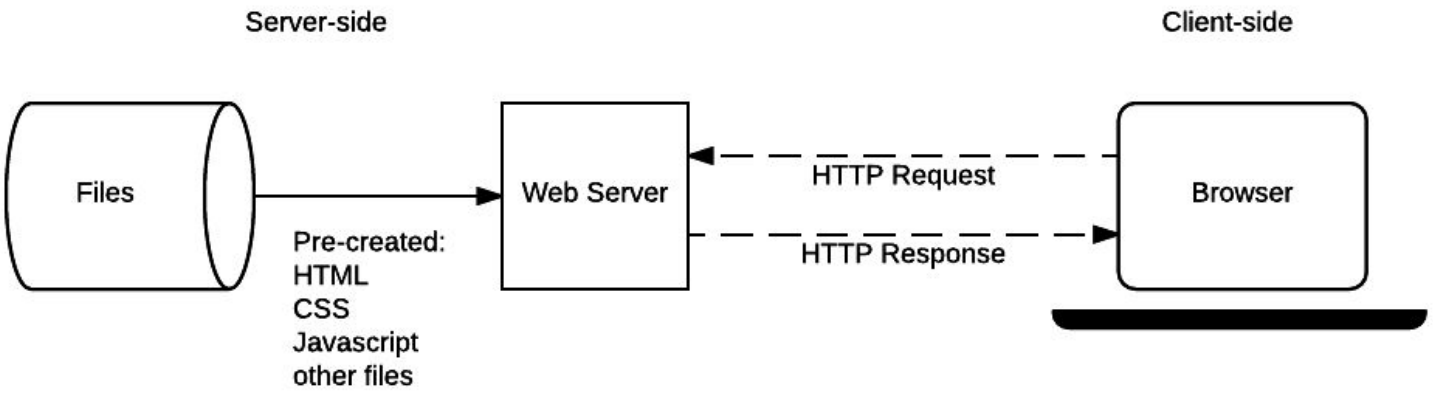
A session key is a cryptographic key associated with the communication itself.

An interchange key is a cryptographic key associated with a principal to a communication

- Key exchange
  - Classical Key exchange authentication
  - Kerberos
  - Public-private key exchange
- Key storage
- Key management
- Digital signatures
- And many other issues

Going back!

For communications, we have used **http**



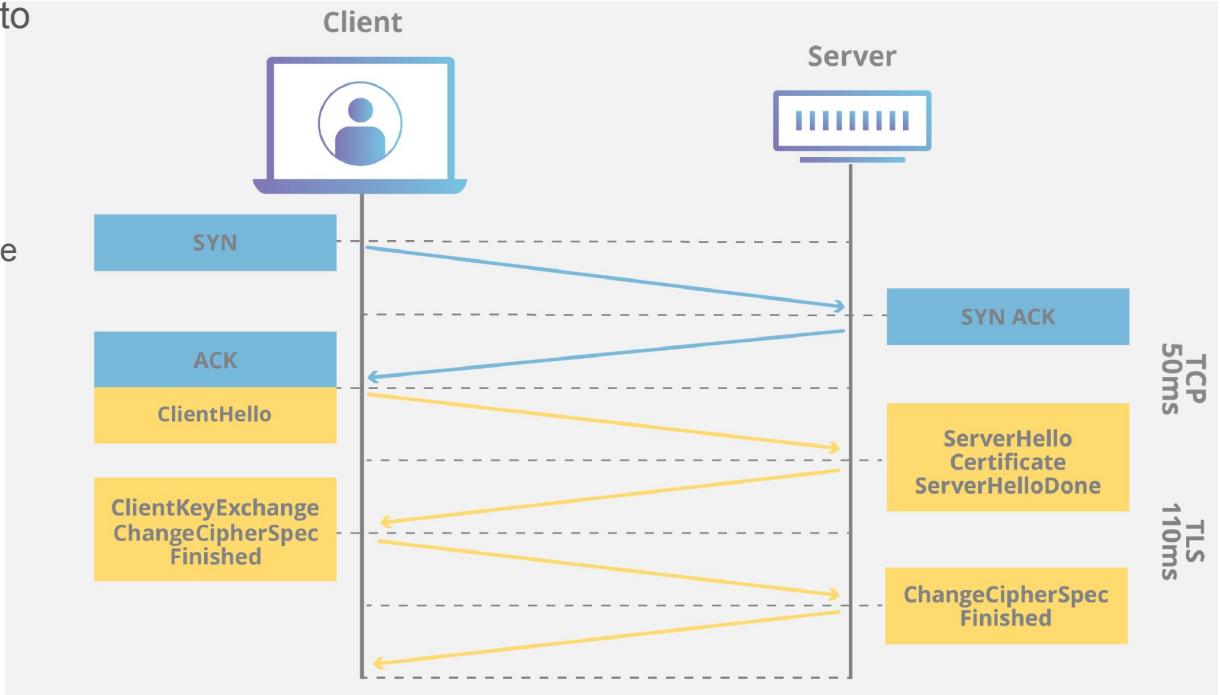
Https

The private key - this key is controlled by the owner of a website and it's kept private.

The public key - this key is available to everyone who wants to interact with the server in a way that's secure.

HTTPS uses an **encryption protocol** to encrypt communications.

- The protocol is called **Transport Layer Security (TLS)**,
  - formerly it was known as Secure Sockets Layer (SSL).
- HTTPS occurs based upon the transmission of TLS/SSL certificates,
  - which verify that a particular provider is who they say they are.

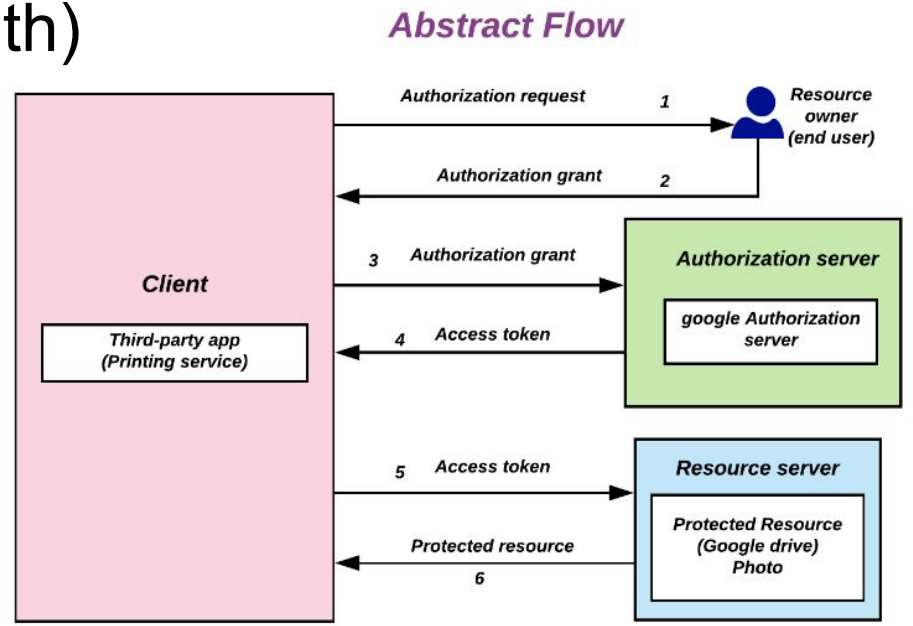


https://www.cloudflare.com/learning/ssl/what-happens-in-a-tls-handshake/

Open authorization(OAuth)

an open standard for access delegation,

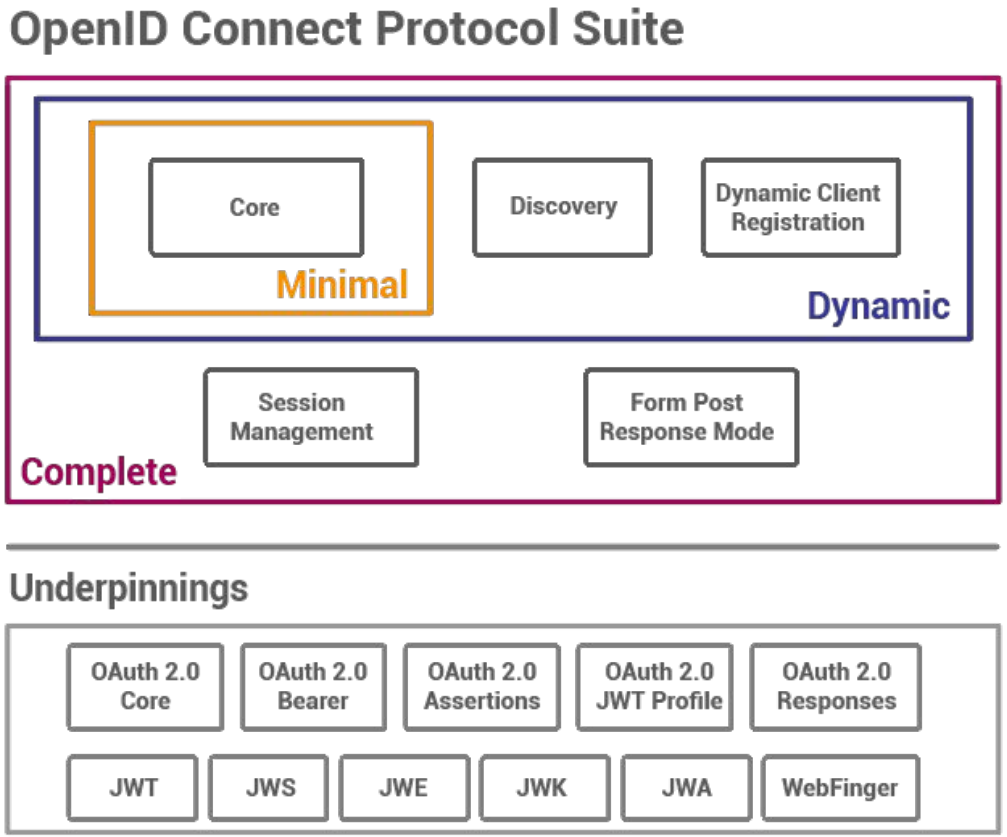
- commonly used as a way for internet users to grant websites or applications **access** to their information on **other websites** but **without giving them the passwords**



https://en.wikipedia.org/wiki/OAuth
https://oauth.net/2/

OpenId Authenticatication

OpenID Connect enables application and website developers to launch sign-in flows and receive verifiable assertions about users across Web-based, mobile, and JavaScript clients.



https://openid.net/developers/how-connect-works/