Domains & SSL Certificates

Domain Name

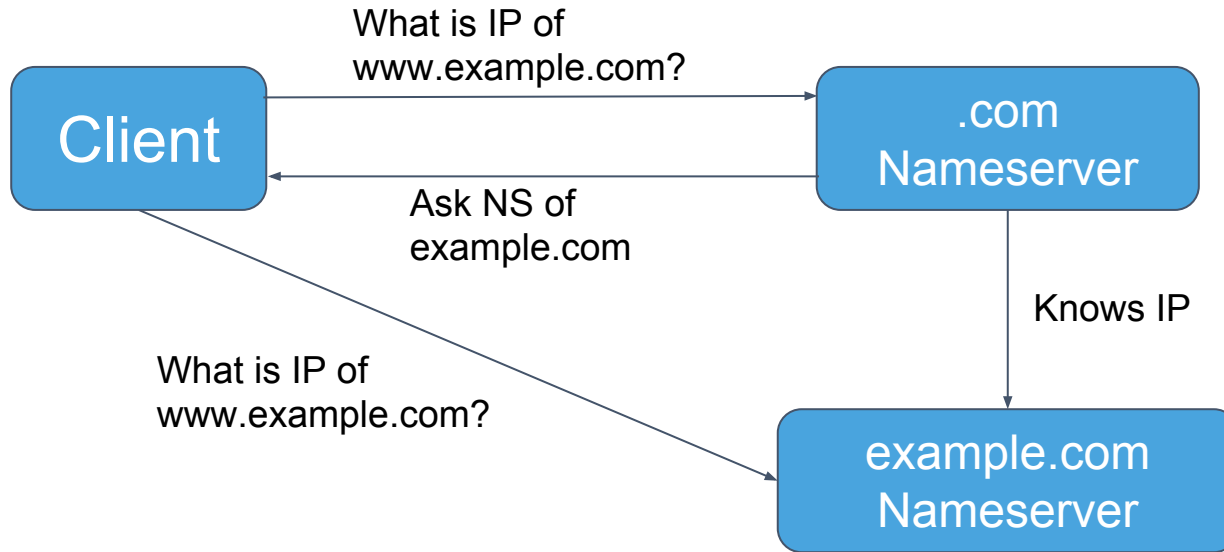| www / cc	. .	example / bartaga	. .	com / me

Subdomain   Second Level Domain   Top Level Domain (TLD)
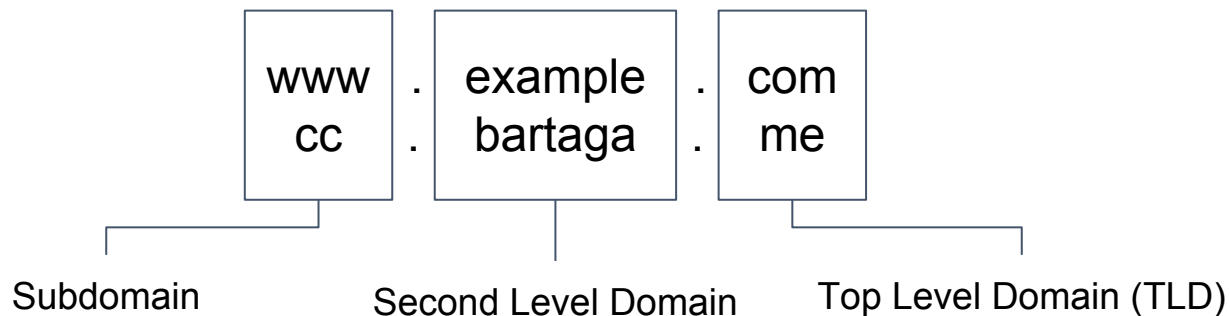
➡ Resolve the name to an IP

Hack & Schne

Domain Name System - DNS

DNS Records

- **A:** Resolve name to IPv4 address
- **AAAA:** Same as above for IPv6

- **CNAME:** Alias from one name to another

- **MX:** Mail Exchange
- **NS:** Nameserver

Hack & Söhne

Domain Registrars

Domain: bartaga.me

Type	Host	Value	TTL	
A Record	cc	138.68.82.53	Automatic	🗑
CNAME Record	@	⬛⬛⬛⬛⬛.myfritz.net.	30 min	🗑
CNAME Record	home	bartaga.me.	30 min	🗑
CNAME Record	ocds	bartaga.me.	30 min	🗑
CNAME Record	www	bartaga.me.	30 min	🗑

Dynamic DNS

Want a way to access hosts in local network

Usually don't have fixed public IP at home

Dynamically update the A record

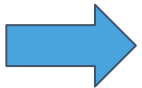# Typical Setup of DDNS

1. Get credentials from DDNS provider
2. Setup by either:
   a. Entering DDNS credentials in router
   b. Installing and setting up software client on a host
3. Forward/open ports to hosts behind the router
   (e.g. Server, RaspberryPi)

Note: FRITZ!Box includes DDNS with free service "MyFritz!".

Domains similar to 0d6abb0kftx9zj68.myfritz.net

SSL/TLS

Secure Socket Layer/Transport Layer Security
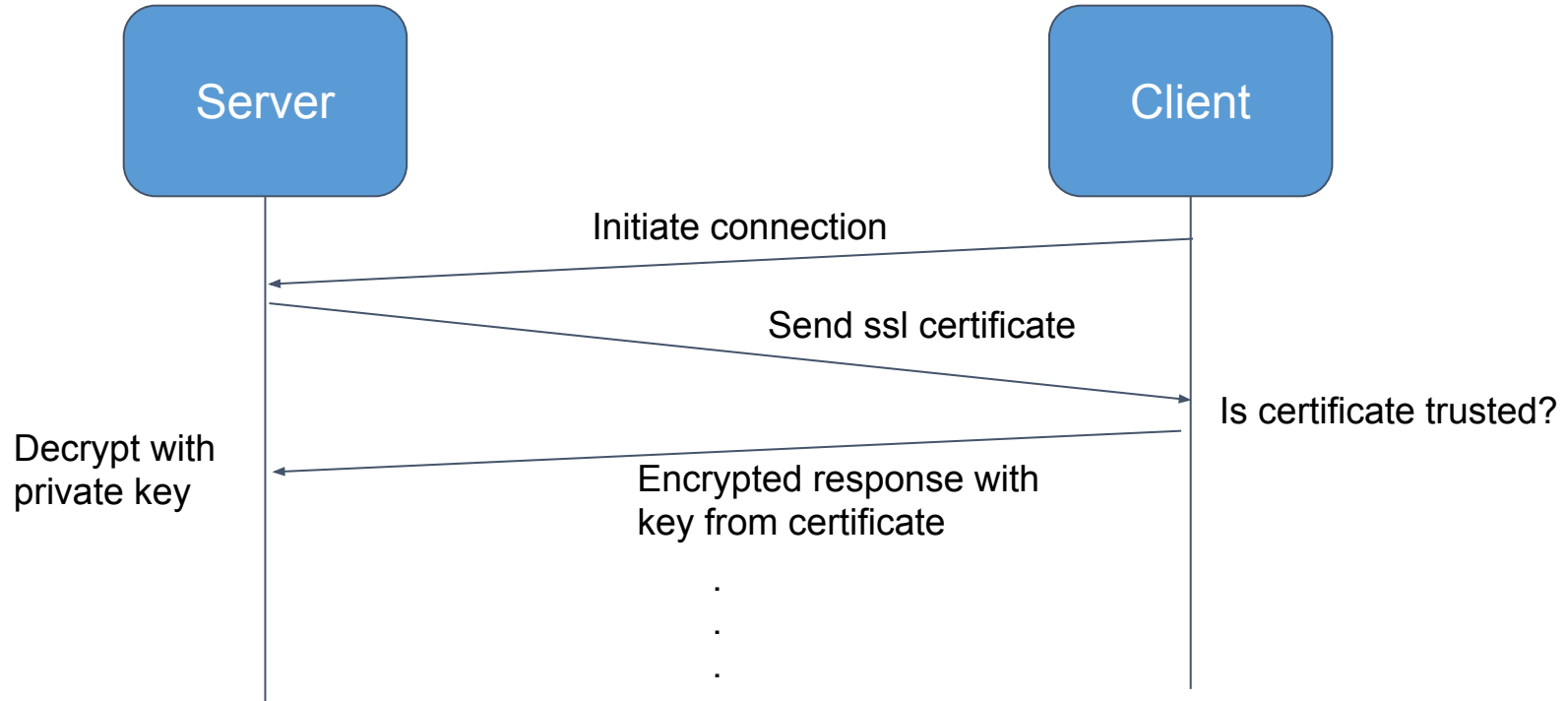
Secure connection is a must!

Unsecured connections allow to:
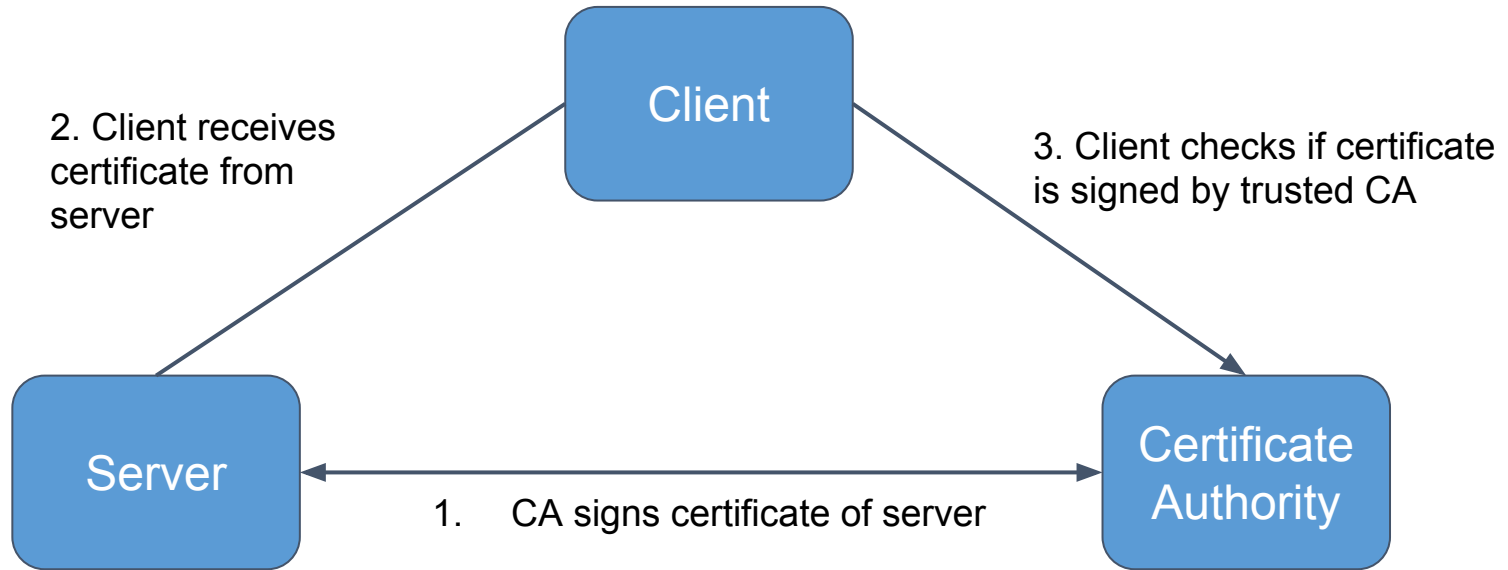
- Steal Login/Session
- Personal data
- Manipulate data

Current browsers give warnings or block device APIs for unsecured connections!

SSL/TLS enables secure connection

Server

Client

Initiate connection

Send ssl certificate

Is certificate trusted?

Decrypt with
private key

Encrypted response with
key from certificate

.
.
.

Hack
&
Sohne

CA gives trusted certificate

Client

2. Client receives certificate from server

3. Client checks if certificate is signed by trusted CA

Server

1. CA signs certificate of server

Certificate Authority

SSL Certificate in Practice

Path to public keychain file

Excerpt from Nginx webserver config:

```
1  server {
2          server_name home.bartaga.me;
3          listen 443 ssl;
4
5          ssl_certificate        /etc/letsencrypt/live/home.bartaga.me/fullchain.pem;
6          ssl_certificate_key    /etc/letsencrypt/live/home.bartaga.me/privkey.pem;
7
```

Path to private key file

Free SSL Certificates