Man in the middle

Przemek Joniak

Man in the middle

1. Definition
2. Session hijacking
3. SSL hijacking & stripping
4. Certificate authority
5. HTTP Public Key Pinning
6. MITM Case studies

Getting into the middle

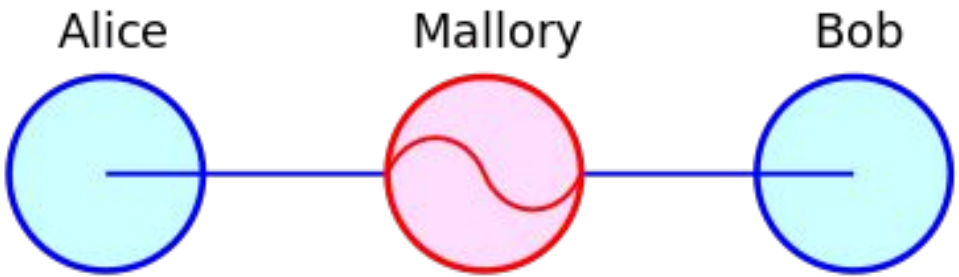
1. ARP spoofing
2. DNS spoofing
3. Rogue DHCP
4. GSM Security

Man in the middle

An attack where the attacker secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other.

Session Hijacking

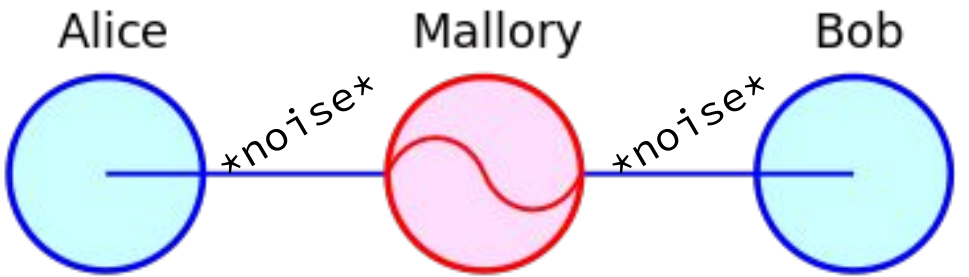
- intercept an unsecured connection, eg HTTP
- steal passwords, login credentials, cookies, etc
- use the credentials
- impersonate (eg. using cookies)



@wiki

Session Hijacking - defence

- simply encrypt your connection
- use HTTPS **EVERYWHERE**



@wiki

SSL strip

- strip away the encryption
- clients receives bare HTTP webpage
- solution: use *HTTP Strict Transport Security* (HSTS)
- HTTP header: ***Strict-Transport-Security***
- works fine on preload only

a picture here

or here if you're on the right

SSL Hijacking

- stip server certificate
- wrap the message with your own certificate

Certificate Authority (CA)

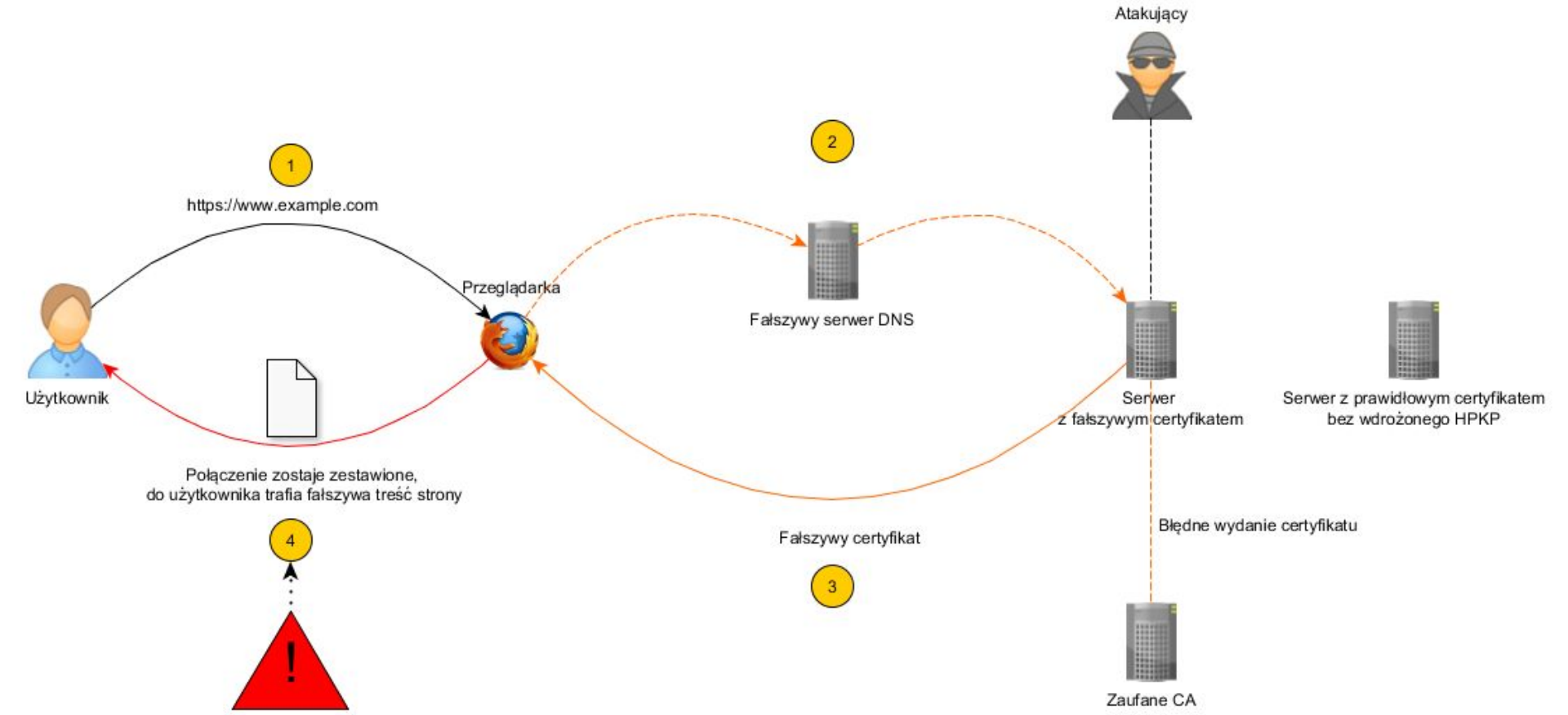
- trusted third party that issues digital certificates
- we send our keys to CA
- CA encrypts those keys with own private key, which nobody knows
- Public CA’s keys are usually pre installed with a device or a browser
- Which CA to trust?

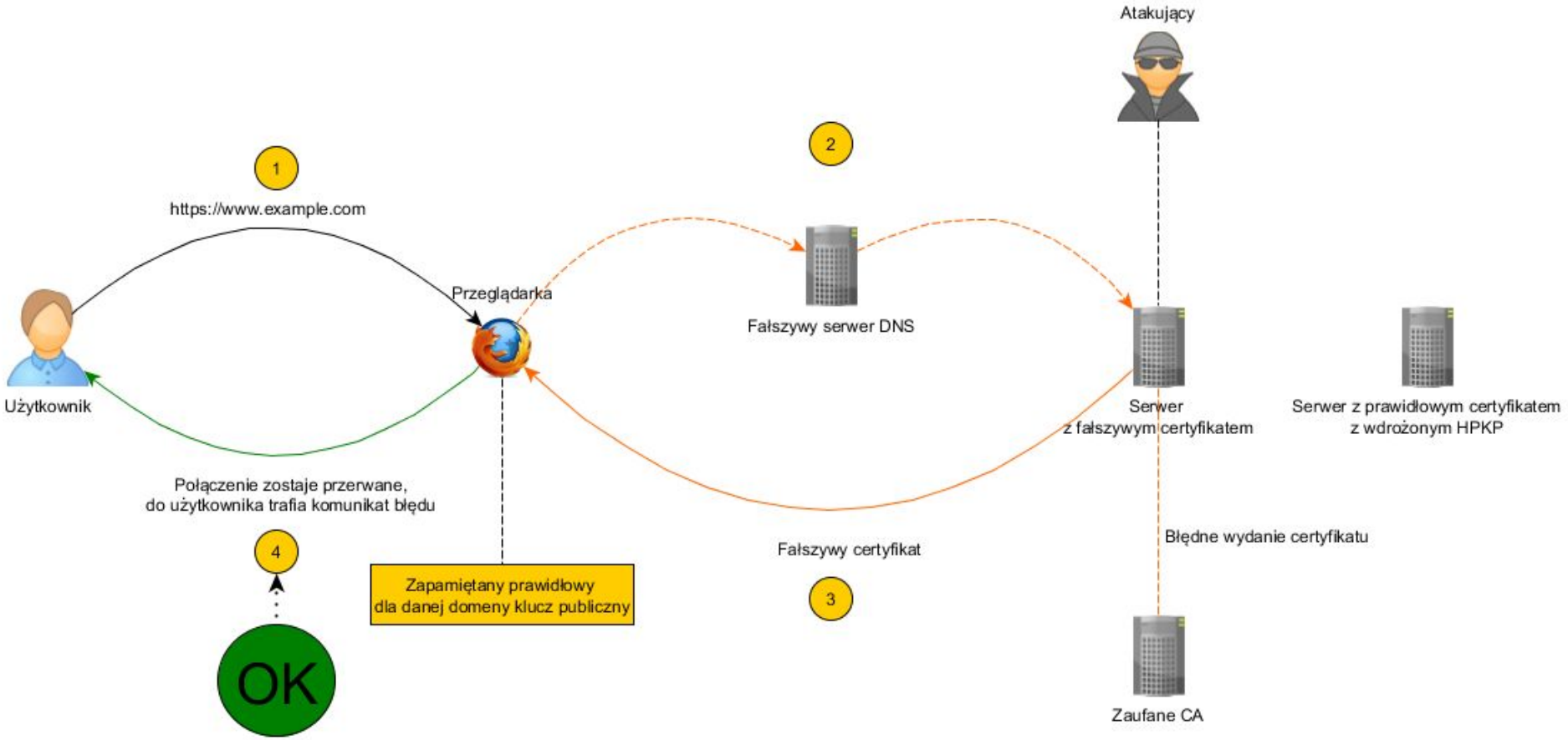
CA weaknesses - fraudulently signed keys

- In 2011 a Dutch CA ***DigiNotar*** was hacked
- about 500 valid signed certificates were generated (including *.google.com)
- around that time Iran was heavy user of DigiNotar
- 300k Iranian gmail users were vulnerable to MITM attack
- major web browsers blacklisted DigiNotar and the company declared bankruptcy within a month

HTTP Public Key Pinning

- a mechanism which delivers a set of public keys to the client (browser)
- the keys should be the only ones trusted for connections to this domain
- this way an owner of a website tell who (CA) to trust
- implemented in HTTP header in ***Public-Key-Pins*** field


Atakujący
1
https://www.example.com
2
Przeglądarka
Użytkownik
Fałszywy serwer DNS
Serwer
z fałszywym certyfikatem
Serwer z prawidłowym certyfikatem
bez wdrożonego HPKP
Połączenie zostaje zestawione,
do użytkownika trafia fałszywa treść strony
Błędne wydanie certyfikatu
Fałszywy certyfikat
4
3
!
Zaufane CA


Atakujący
1
https://www.example.com
2
Przeglądarka
Użytkownik
Fałszywy serwer DNS
Serwer
z fałszywym certyfikatem
Serwer z prawidłowym certyfikatem
z wdrożonym HPKP
Połączenie zostaje przerwane,
do użytkownika trafia komunikat błędu
Fałszywy certyfikat
Błędne wydanie certyfikatu
4
Zapamiętany prawidłowy
dla danej domeny klucz publiczny
3
OK
Zaufane CA

SSL hijacking: China vs. Google

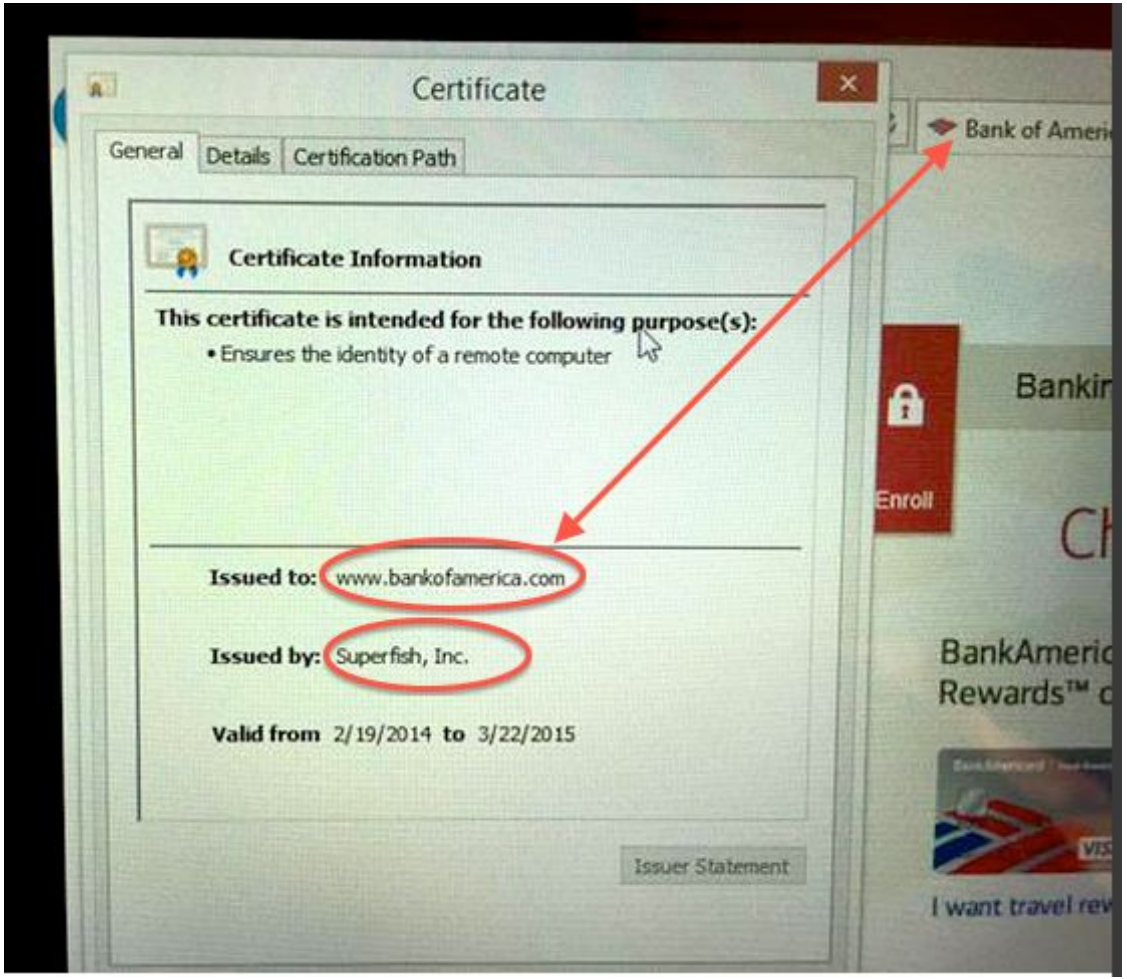
- in China Google services are blocked to public...
- ...but not to academic community via CERNET
- Since Google uses SSL, then the Firewall sees an ***encrypted*** traffic only
- The Firewall injects own SSL certificates

Does NSA do the same? → Quantum Insert

Lenovo Superfish

- injecting ads into Google search results
- a pre installed softwares, a self-signed root CA on low-end Lenovo laptops
- the Super~~fish~~phish's keys were hardcoded and **the same** (**!**) across all machines

- **always install vanilla Windows and Linux to prevent crapware!**



https://twitter.com/kennwhite/status/568270748638318593

SSL hijacking: Kazakhstan

- Kazakhstan citizens are obliged to install the governmental certificate
- reason: “protection of Kazakhstan users from foreign Internet resources”
- http://pki.gov.kz/index.php/en/

VPN vs MITM

- VPN is believed to protect against MITM
- IPS nor government cannot longer intercept
- but what if one MITMs an outgoing traffic from VPN server
- but what if one MITMs initial connection with VPN server

SSH vs MITM

- the attack is super easy: ssh-mitm, sshmitm, and more…
- prevention is also super easy: just check machine **fingerprint**

```
$ ssh sample.ssh.com
The authenticity of host 'sample.ssh.com' cannot be established.
DSA key fingerprint is 04:48:30:31:b0:f3:5a:9b:01:9d:b3:a7:38:e2:b1:0c.
Are you sure you want to continue connecting (yes/no)?
$ yes
Warning: Permanently added 'sample.ssh.com' (DSA) to the list of known hosts.
```

Getting into the middle

ARP Spoofing - ARP recap

- *Address Resolution Protocol* maps IP to MAC addresses
- *ARP request* contains: sender IP & MAC and requested IP
- the request is broadcast to a local network
- a host whose IP matches sends back its MAC in *ARP reply*
- the MAC address is put into a *ARP cache*

ARP Spoofing - ARP Vulnerabilities

- hosts tend to send a request with their IP to say “hello” and to avoid IP collision
- having received a request from an unknown host, a cache is updated
- **the cache can be updated without sending a request!**

ARP Spoofing - The Attack

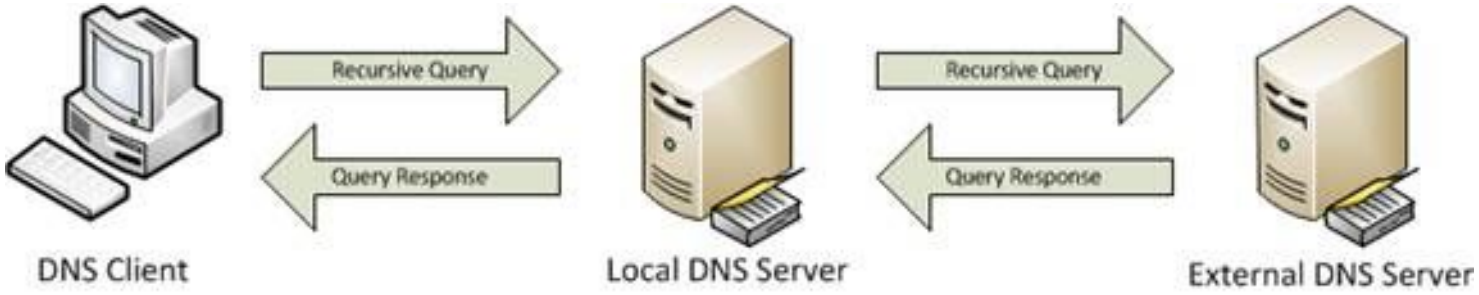
- broadcast an ARP request with a router’s IP within a local network
- a victim’s traffic is now routed to the attacker’s host

ARP Spoofing - defence

- use static ARP cache entries
- use ARP spoofing detection and prevention software
- configure OS so it does not accept random replies
- secure your LAN
- do not connect to open WiFis

DNS Spoofing

- DNS has a hierarchical structure
- a local DNS server ask recursively server which is higher in a hierarchy
- from a client's perspective only two packets are exchanged: a query and a response



http://techgenix.com/Understanding-Man-in-the-Middle-Attacks-ARP-Part2/

DNS Spoofing - poisoning victim cache

- every DNS query has a unique ID
- the ID associates a query with a response
- all what needs to be done is to send forged response with the same ID
- this can be achieved with ARP spoofing
- forged data can contain eg. IP of attckers’s machine (phishing)
- can be done on handshake only contrary to APR spoofing

DNS Spoofing - poisoning server cache

- injecting forged DNS records into a server cache
- it can be done by sending a fabricated responses
- the server should be configured to reject those messages
- accept traffic from other trusted DNS servers (DNSSEC) only

DNS Spoofing - The Great Firewall in the USA

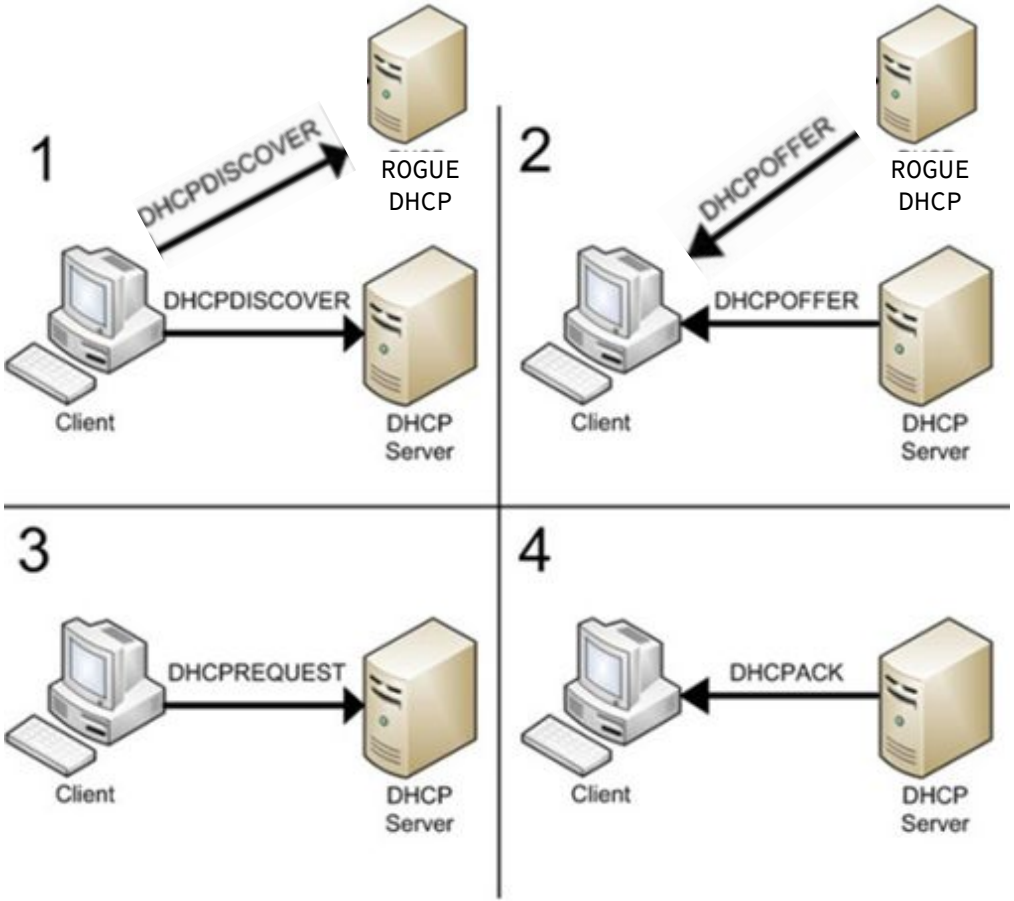
- PRC intentionally poisons DNS entries to block access to illegal websites
- in 2010 a small IPS began fetching information from chinese root DNS
- information propagated quickly
- twitter, youtube, facebook and more were inaccessible in a part of the USA and Chile
- a probable cause: misconfigured DNS server

China vs. Github

- in 2011 github was 276th most popular webpage in PRC
- HTTPS only
- a list of The Great Firewall contributors was published to github
- github was blocked for a few days → SSL hijacking
- the “official” reason, *the train ticket theory* is ridiculous
- github is not the only one
- github was also banned in Russia, Turkey and India

Rogue DHCP

- **Dynamic Host Configuration Protocol** serves network configuration to newly connected hosts
- a host ask for a configuration by broadcasting a DISCOVER
- DHCP replies with an OFFER
- if we set a rogue DHCP then both servers compete
- if the host accepts rogue DHCP’s answer then MITM is succeeded


1
DHCPDISCOVER
ROGUE
DHCP
DHCPDISCOVER
Client
DHCP
Server
2
DHCPOFFER
ROGUE
DHCP
DHCPOFFER
Client
DHCP
Server
3
DHCPREQUEST
Client
DHCP
Server
4
DHCPACK
Client
DHCP
Server

DHCP starvation

- flood DHCP server with fake MACs addresses
- a pool with available IP addresses runs up quickly
- behavior of flooded DHCP depends on a implementation

- having sent a DISCOVER with a fake MAC, the DHCP requires DHCPPREQUEST from a machine with the MAC
- an IP address is reserved for the MAC temporarily

GSM security

- 2G uses weak, easy to break A5/1 algorithm
- although: encryption is no compulsory
- a cell phone connects to the nearest BTS
- so-called IMSI-Catcher is a fake “BTS” which enforces no encryption

How to make a simple $7 IMSI Catcher

93 192 wyświetlenia

843 12

Resources & further reading

- A **MITM video** by Computerphile: https://www.youtube.com/watch?v=-enHfpHMBo4
- **ARP, DNS spoofing, SSL, hijacking** explained: http://techgenix.com/Understanding-Man-in-the-Middle-Attacks-ARP-Part1/
- **Kazakhstan, SSL**: https://www.techdirt.com/articles/20151204/07412332986/kazakhstan-decides-to-break-internet-wage-all-out-war-encryption.shtml, official site: http://pki.gov.kz/index.php/en/
- **Forged DigiNotar certificates**: Google's statement on the attack https://security.googleblog.com/2011/08/update-on-attempted-man-in-middle.html,
  BBC News: http://www.bbc.com/news/technology-14789763,
  General description: https://en.m.wikipedia.org/wiki/DigiNotar,
  Tech details: https://blog.torproject.org/diginotar-damage-disclosure,
  Another news: https://www.cnet.com/news/google-users-in-iran-targeted-in-ssl-spoof/
- **HTTP Public Key Pinning**: explained (PL) https://kryptosfera.pl/post/http-public-key-pinning/,
  is HPKP dead? https://blog.qualys.com/ssllabs/2016/09/06/is-http-public-key-pinning-dead ,
  tech details: https://developer.mozilla.org/en-US/docs/Web/HTTP/Public_Key_Pinning

Resources & further reading #2

- **China vs Google**: https://www.infosecurity-magazine.com/news/china-man-in-the-middle-attack/, https://www.techdirt.com/articles/20140909/03424628458/china-using-man-in-the-middle-attack-against-google.shtml, https://en.greatfire.org/blog/2014/sep/authorities-launch-man-middle-attack-google, BONUS: Google picks up a fight with chinese CAs: https://www.theverge.com/2015/4/2/8331691/google-china-cnnic-ssl-https-certificate-authority

- Does NSA mitm google? **Quantum Insert** https://www.wired.com/2015/04/researchers-uncover-method-detect-nsa-quantum-insert-hacks/, Detecting Quantum Insert attack, Bro conference https://www.youtube.com/watch?v=sUhourxa58g

- Lenovo **Superfish** scandal: Details https://en.m.wikipedia.org/wiki/Superfish#Lenovo_security_incident,, Lenovo fined $3.5m http://www.bbc.co.uk/news/technology-41179214, Cool article: http://www.slate.com/articles/technology/bitwise/2015/02/lenovo_superfish_scandal_why_it_s_one_of_the_worst_consumer_computing_screw.html, details (PL) https://www.pcworld.pl/news/Superfish-adware-w-laptopach-Lenovo-Jak-dziala-i-jak-go-usunac,400970.html

- **DNS** Spoofing https://en.wikipedia.org/wiki/DNS_spoofing, DNS Spoofing vs Cache Poisoning https://security.stackexchange.com/questions/33257/dns-spoofing-vs-dns-cache-poisoning, dns/arp spoofing tutorial (PL): https://haker.edu.pl/2015/12/14/dns-spoofing-i-arp-poisoning/,

Resources & further reading #3

- **The Great Firewall in the USA**: article: https://www.computerworld.com/article/2516831/security0/china-s-great-firewall-spreads-overseas.html, DNS operators mails: https://lists.dns-oarc.net/pipermail/dns-operations/2010-March/005263.html

- **China vs github**: https://en.greatfire.org/blog/2013/jan/china-github-and-man-middle, the train ticket theory: https://en.greatfire.org/blog/2013/jan/github-blocked-china-how-it-happened-how-get-around-it-and-where-it-will-take-us, dns reachability: http://viewdns.info/chinesefirewall/, github censorship: https://en.m.wikipedia.org/wiki/Censorship_of_GitHub

- **Rogue DHCP** whitepaper: http://seclists.org/vuln-dev/2002/Sep/99, DHCP Starvation explained & tutorial: http://www.blacklabssecurity.info/dhcp-starvation.html, rogue DHCP https://medium.com/tech-jobs-academy/attack-a-network-by-using-a-rogue-dhcp-server-8c8acea315ab

- **DHCP Starvation**: http://www.omnisecu.com/ccna-security/dhcp-starvation-attacks-and-dhcp-spoofing-attacks.php

- **GSM security**: how **IMSI-catcher** works https://www.nstarpost.com/news/how-imsi-catchers-work/