Man In The Middle (MITM)

By

Alan S H Lam

shlam@ie.cuhk.edu.hk

Seminar Outlines

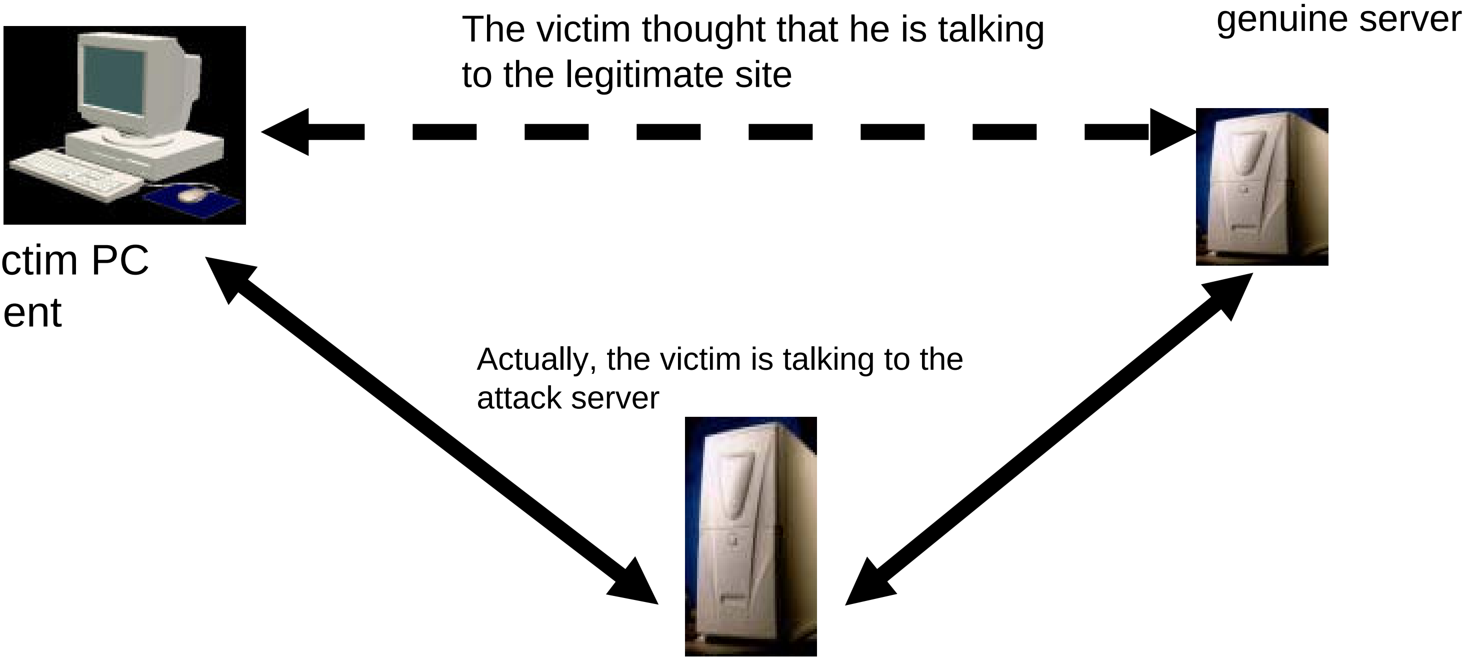
- Working principle of MITM attack
- MITM attack techniques (with live demos)
  - ARP poisoning
  - DNS poisoning
  - DNS hijack
  - Trojan Horse Program
- The Threats
- Countermeasures against MITM attack

What is MITM

In the MITM attack, attacker pretends to be the server to the client and the client to the server allowing him/her to intercept and modify the traffic between two parties without either party knowing that the link between them has been compromised

Man in the Middle Attack

Attacker redirects the traffic of a client or/and a server to the attacker server where the attacker can intercept and modify the traffic before relaying the traffic for both parties



The victim thought that he is talking to the legitimate site

genuine server

Victim PC
client

Actually, the victim is talking to the attack server

Attacker server intercept and modify the traffic between the victim and genuine server

MITM Techniques

- ARP poisoning
  - In LAN environment
- DNS poisoning
  - Can launch the attack from remote network
- DNS Hijack
  - Need to observe the DNS packets either at the client or DNS server side
- Trojan Horse program
  - Once installed or activated, the victim traffic will be redirect to attacker server automatically

Intercept SSL and SSH

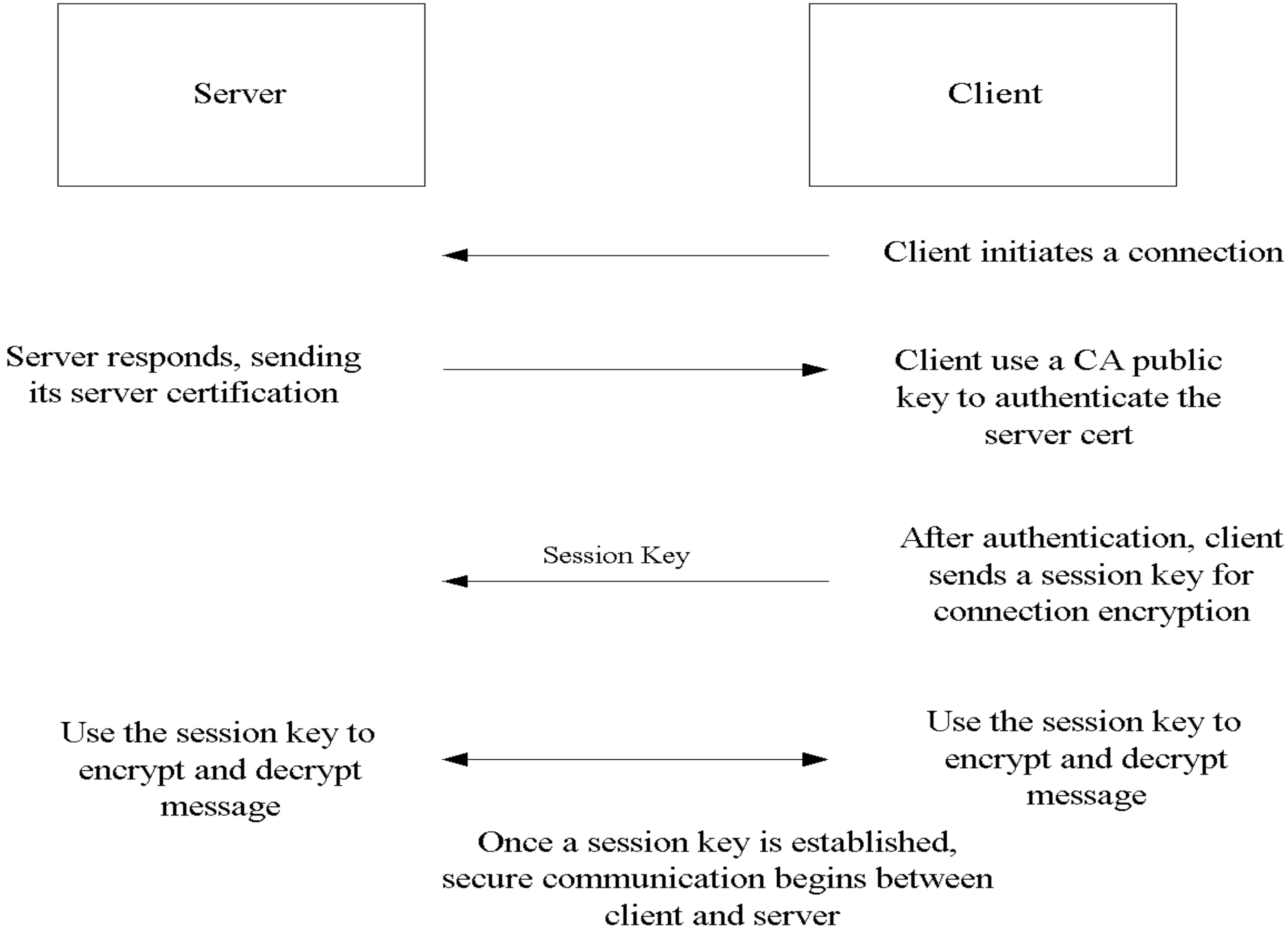
Under certain condition, MITM can decrypt session protected by

- SSL (***S**ecure **S**ockets **L**ayer) which is commonly used in secure HTTP*

  and

- SSHv1 (***S**ecure **S**hell, Version 1) which is commonly used to log into another computer over a network, to execute commands in a remote machine*

A normal SSL connection is protected by session keys



Server

Client

Client initiates a connection

Server responds, sending its server certification

Client use a CA public key to authenticate the server cert

Session Key

After authentication, client sends a session key for connection encryption

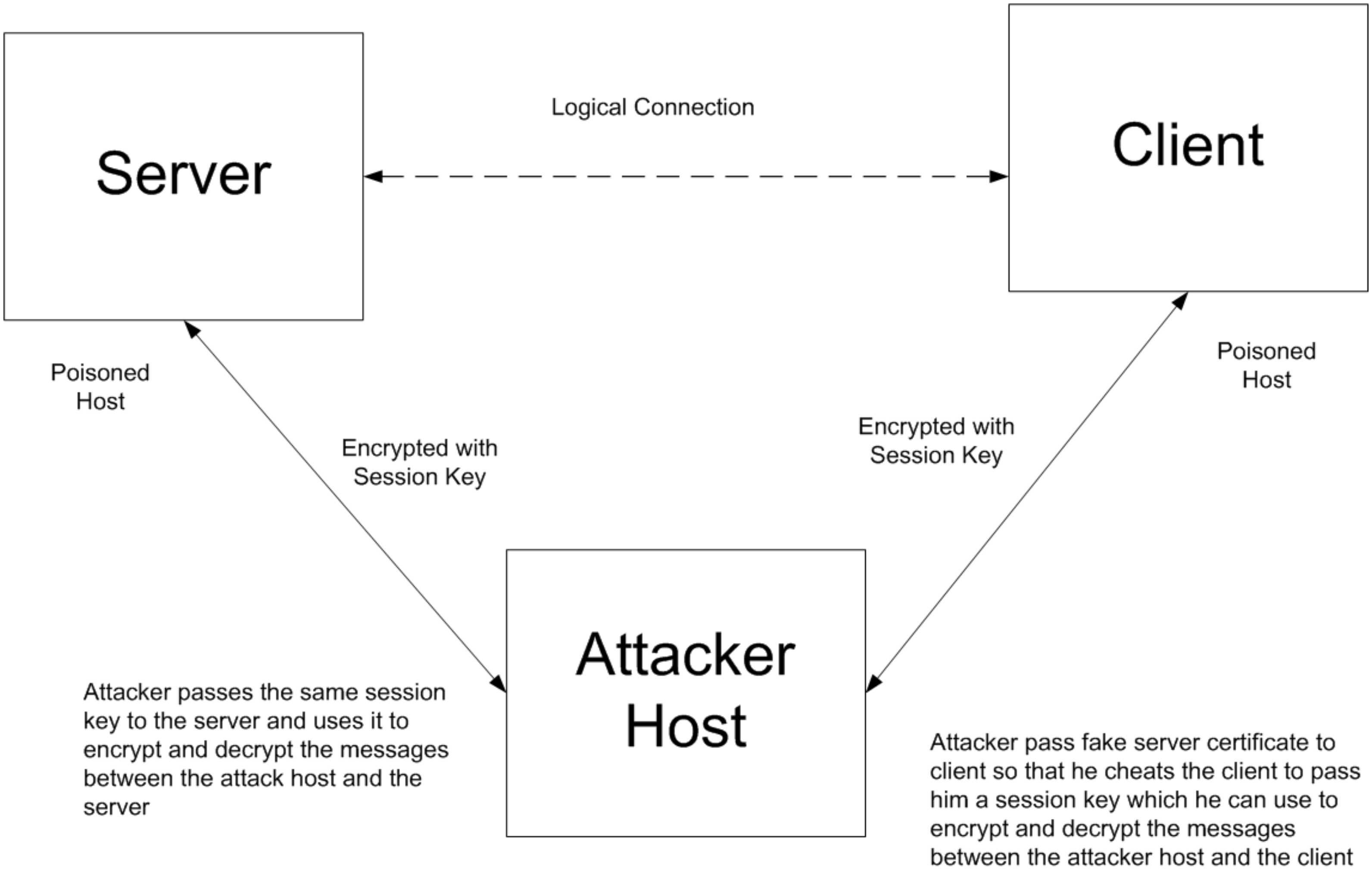
Use the session key to encrypt and decrypt message

Use the session key to encrypt and decrypt message

Once a session key is established, secure communication begins between client and server

Source: IEG7006, CUHK

MITM Attack in SSL connection



Attacker passes the same session key to the server and uses it to encrypt and decrypt the messages between the attack host and the server

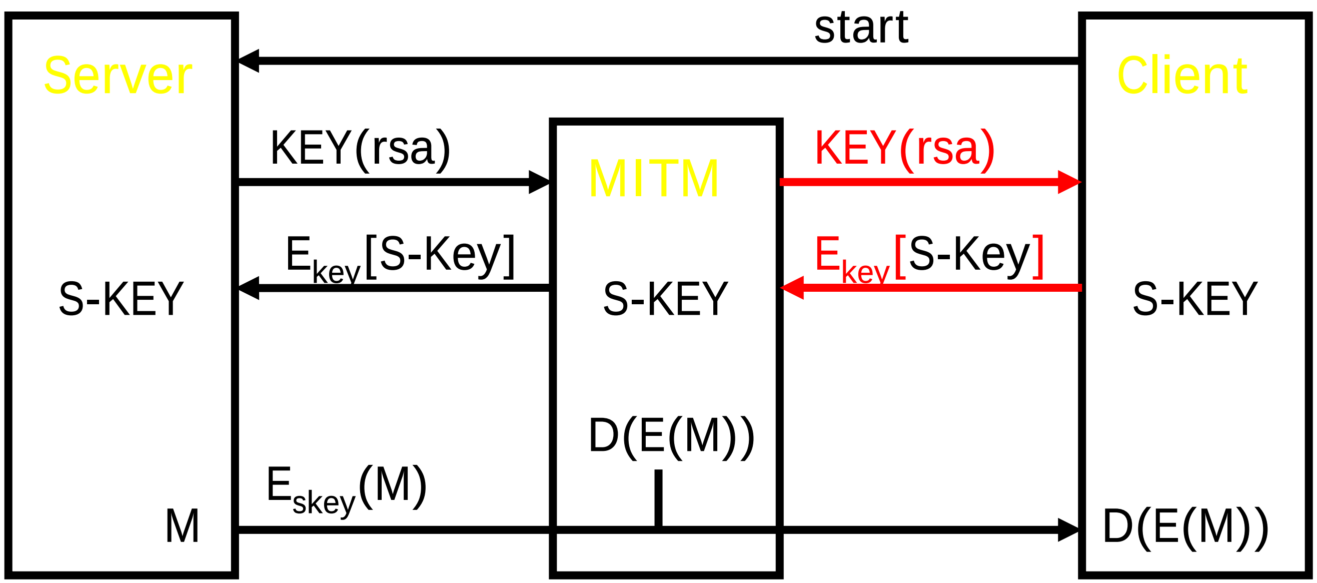
Attacker pass fake server certificate to client so that he cheats the client to pass him a session key which he can use to encrypt and decrypt the messages between the attacker host and the client

Source: IEG7006, CUHK

Key Manipulation

SSH v1

- Modification of the public key exchanged by server and client.



Source: antifork.org

MITM Techniques

- How to fool the two victims and make them to redirect the traffic (originally to their partners) to the attacker server.
- At the attacker server, attacker can
  - just observe the traffic and then relay the traffic for both victims, or
  - modify the traffic before relay the traffic, or
  - block certain traffic between two victims
- The attacker needs to make the victims to believe that they talking to their partners without either party knowing that the link between them has been compromised; hence the attacker need to maintain a good proxy server for relaying the true or fake traffic.

ARP Poisoning

The arp protocol has an intrinsic insecurity. In order to reduce the traffic on the cable, it will insert an entry in the arp cache even if it hadn't request it. In other words, EVERY arp reply that goes on the wire will be inserted in the arp table and there is no authentication for any arp entry updating.

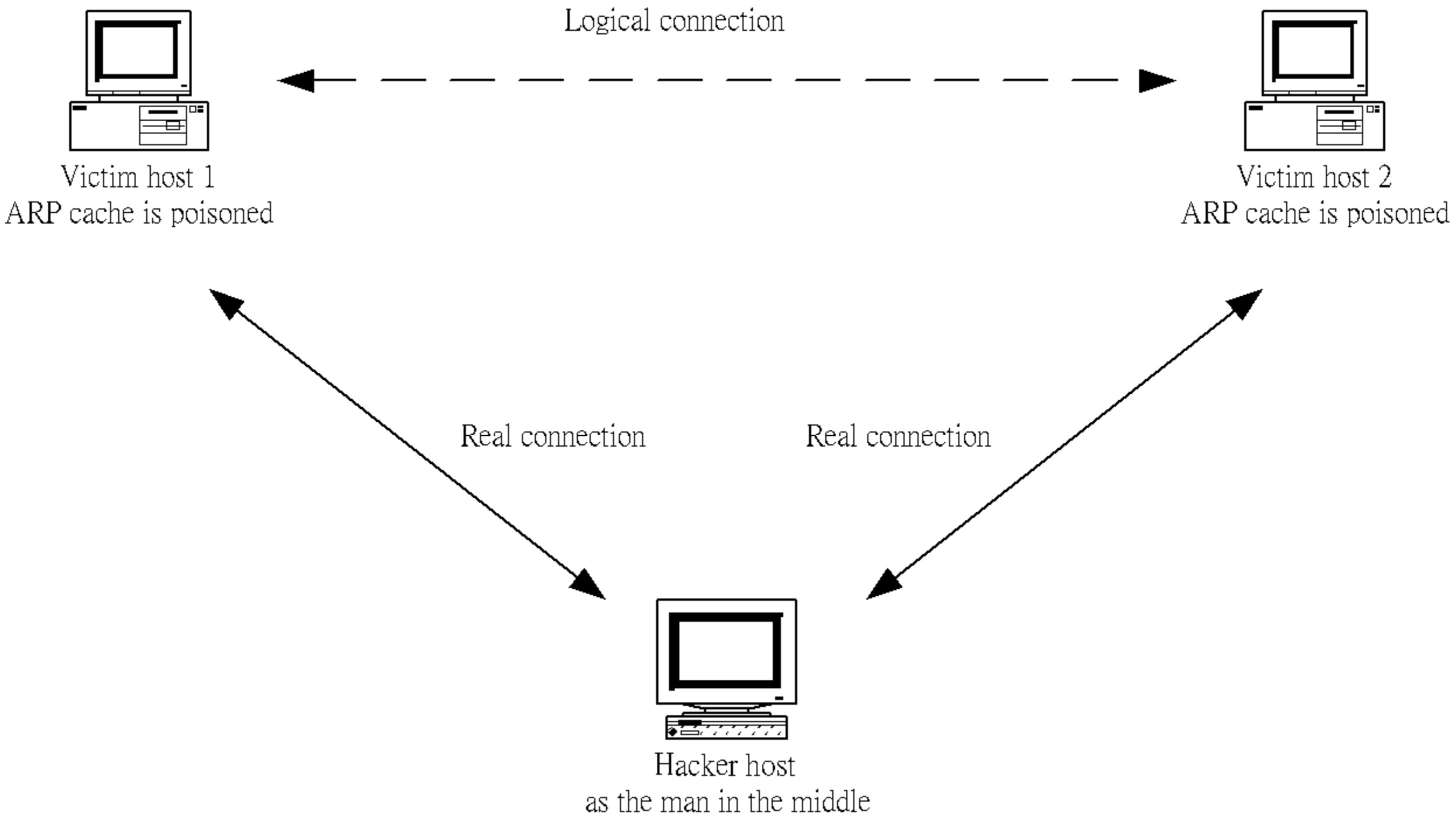
Source: IEG7006, CUHK

ARP Poisoning

Attacker can send fake arp replies to the two victim hosts they want to attack. He/she will tell that the mac address of their partner hosts is the one hard-coded on his/her NIC. The victim hosts with the arp cache poisoned will now send packets (which originally should go to their partner hosts) to the attacker host, because the victim hosts have cached the attacker mac address as their partner hosts mac address.

Source: IEG7006, CUHK

ARP Poisoning



Source: IEG7006, CUHK

ARP Poisoning

ARP poisoning works effectively on LAN environment including WLAN. Some arp poison tools can launch the arp poisoning attack in rapid rate even down to microsecond.

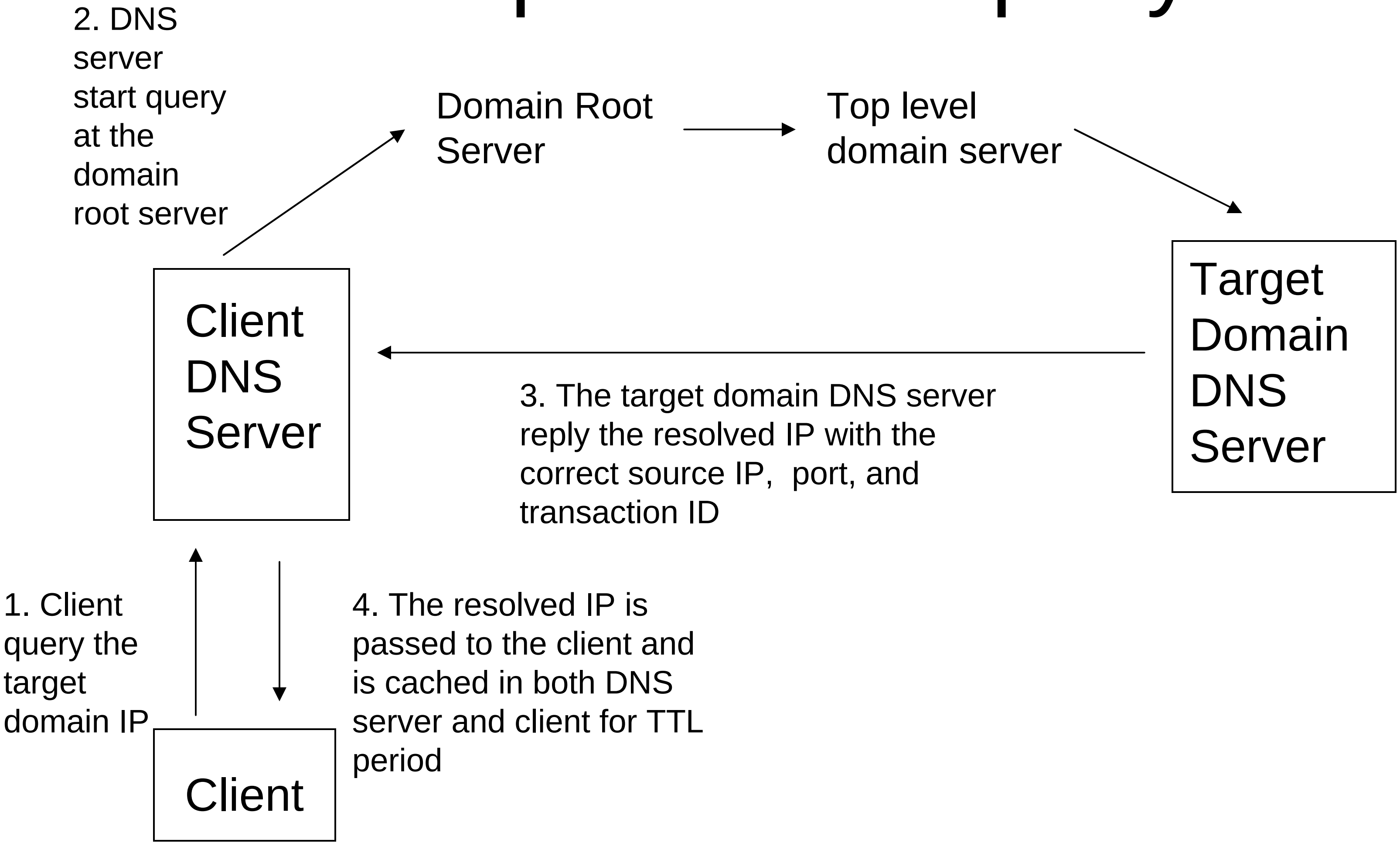
DNS Poisoning

Recalling the steps of DNS query:

1. The client will contact its configured DNS server and ask for target domain to be resolved. This query will contain information about the client’s source UDP port, IP address and a DNS transaction ID.
2. The client’s DNS server since it is not authoritative for the target domain will through recursive queries via the Internet root DNS servers contact the target domain DNS server and get an answer for the query.
3. This successful query will then be passed back to the client and this information is cached by both the name server and the client for a specified TTL (time to live) period.

Source: IEG7006, CUHK

Steps of DNS query



2. DNS server start query at the domain root server

Domain Root Server

Top level domain server

Target Domain DNS Server

Client DNS Server

3. The target domain DNS server reply the resolved IP with the correct source IP, port, and transaction ID

1. Client query the target domain IP

4. The resolved IP is passed to the client and is cached in both DNS server and client for TTL period

Client

Source: IEG7006, CUHK

DNS Poisoning

The client's DNS server only accept the DNS query reply if it is

- From the target domain DNS server IP address
- To the client's DNS server source port
- With the DNS transaction ID that the client's DNS server sent to the target domain DNS server

The above three pieces of information are use to authenticate a DNS query reply.

Source: IEG7006, CUHK

DNS Poisoning

DNS Poisoning by DNS Transaction ID Prediction

Knowing the target domain DNS server IP is easy as it can be easily queried by host or nslookup tool.

The client’s DNS server source port can also be obtained if the client’s DNS server reuse the same source port for DNS query on the behalf of its clients. In such case, an attacker can make a query of his own domain and then review the source port at his domain DNS server

Source: IEG7006, CUHK

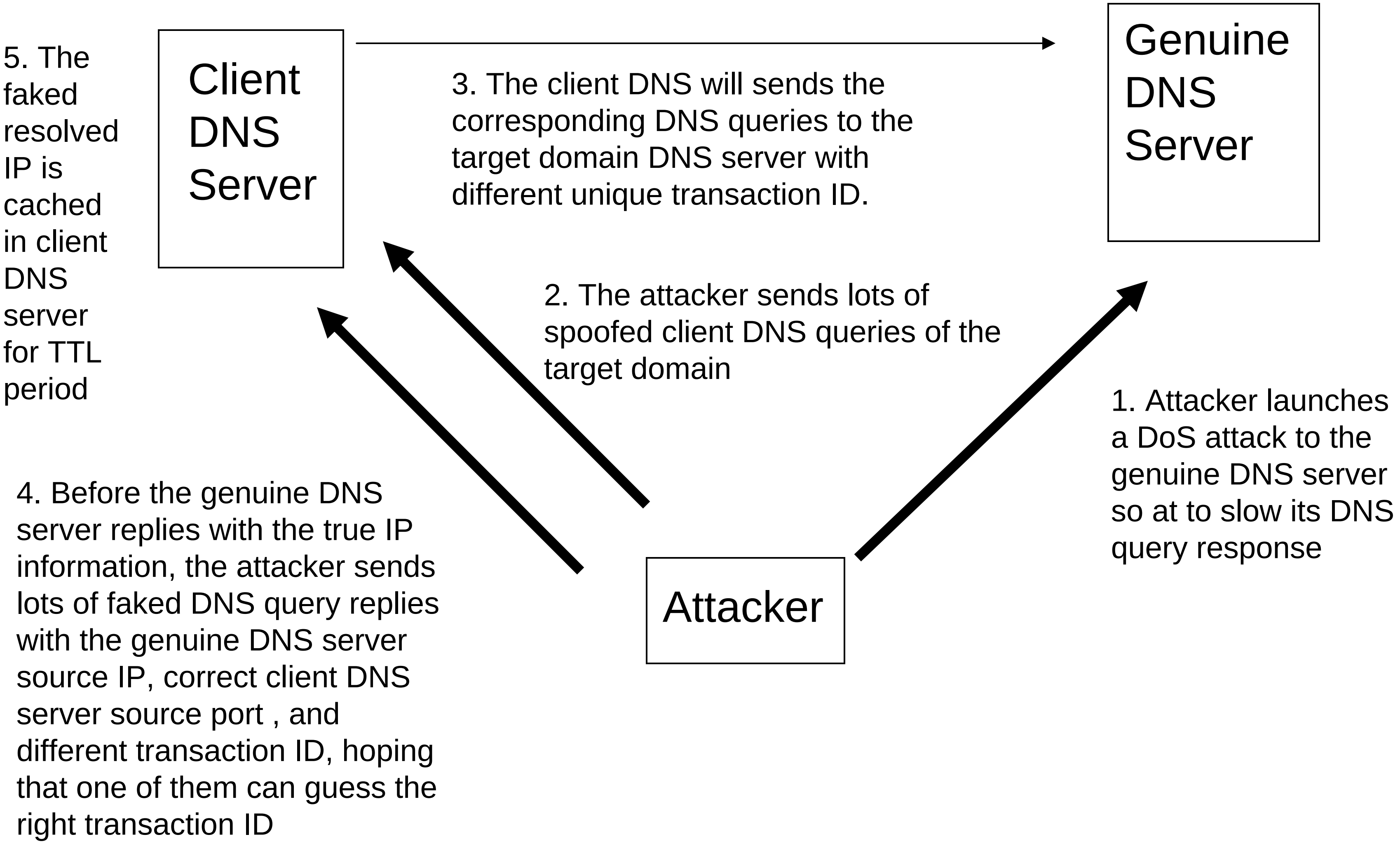
DNS Poisoning

To guess the right DNS transaction ID, an attacker can proceed with the follow steps:

1. Send lots of DNS query of the target domain to the victim with different spoofed source IP. In such case, the victim will generate lots of unique transaction ID to the target domain DNS server
2. While the victim is waiting for the DNS query replies from the genuine DNS server, the attacker send lots of faked DNS replies to the victim with the right DNS server IP, right source port, and different transaction ID hoping one of them can guess the correct transaction ID.

Source: IEG7006, CUHK

Steps of DNS Poisoning



1. Attacker launches a DoS attack to the genuine DNS server so at to slow its DNS query response

2. The attacker sends lots of spoofed client DNS queries of the target domain

3. The client DNS will sends the corresponding DNS queries to the target domain DNS server with different unique transaction ID.

4. Before the genuine DNS server replies with the true IP information, the attacker sends lots of faked DNS query replies with the genuine DNS server source IP, correct client DNS server source port , and different transaction ID, hoping that one of them can guess the right transaction ID

5. The faked resolved IP is cached in client DNS server for TTL period

Source: IEG7006, CUHK

DNS Poisoning

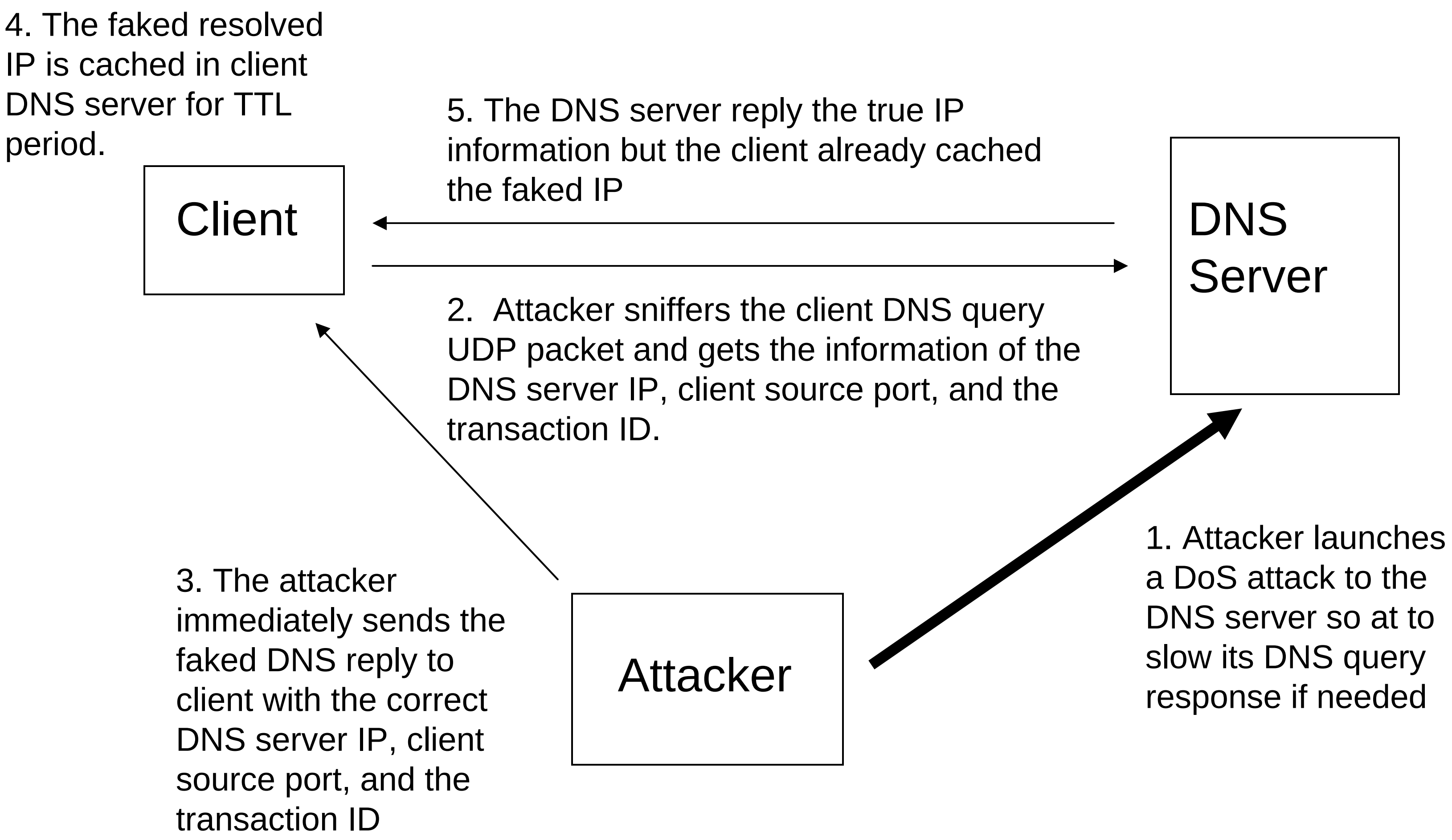
Unlike ARP poisoning which need to be launched in LAN environment. DNS poisoning can be launched from a remote network. However, in order to make the attack successful, the attacker need to send lots of faked DNS query replies which may be detected by most IDS

DNS Hijacking

If an attacker is inserted between the client and the DNS server, he can easily reviewed the correct source IP, source port, and transaction ID. In such case, he may send faked DNS query reply to the client directly before the real one return from the DNS server. In order to make his faked DNS query arrive the client before the real one, the attacker may launch deny of server attack to the DNS server so as to slow down the DNS server response.

Source: IEG7006, CUHK

Steps of DNS Hijacking



1. Attacker launches a DoS attack to the DNS server so at to slow its DNS query response if needed

2. Attacker sniffers the client DNS query UDP packet and gets the information of the DNS server IP, client source port, and the transaction ID.

3. The attacker immediately sends the faked DNS reply to client with the correct DNS server IP, client source port, and the transaction ID

4. The faked resolved IP is cached in client DNS server for TTL period.

5. The DNS server reply the true IP information but the client already cached the faked IP

Source: IEG7006, CUHK

DNS Hijacking

DNS hijacking is effective if the attacker can observe the victim DNS query traffic. In most case the DoS attack to DNS server is unnecessary as the fake DNS reply usually come before the true one from the DNS server. However, the attacker need to be close to the victim or the DNS server so as to observe the DNS query traffic.

Trojan Horse Program

Once Trojan horse program has been installed in victim host through the victim system security hole, the victim host traffic can be redirected to attacker server by changing the victim host configuration such as

- modifying the hosts file,
- disabling firewall and anti-virus,
- installing fake CA cert,
- setting the web proxy or socks5 proxy,
- changing the default gateway, or
- even setting up a tunnel back to the attack network.

Other Attacks Techniques

- DHCP spoofing
  - – Rely the victim with fake gateway and DNS server information when receive victim DHCP broadcast request
- Route mangling
  - – Pretend to be the gateway by spoofing routing protocol

The Threats

- Compromise of sensitive information
- Misinformation
- Privacy infringement
- Increase chance of intrusion
- Disturbance of normal operation between client and server

When people feel unsafe in the Cyberspace, they will reluctant to use Internet.

Countermeasure against ARP poisoning

Monitoring the change of ARP entry on network (e.g. arpwatch)

Pros

- It can be easily deployed at gateway or server side.

Cons

- It can only send alert but cannot block the poisoning.
- Detection is difficult in large and dynamic network.
- It cannot detect the poisoning at gateway or server side if attacker launches one-way poisoning attack at the client side only.

Countermeasure against ARP poisoning

Set static MAC address in client and server hosts.

Pros

- It make the arp poisoning very difficulty as all hosts no longer learn any MAC address from the network via ARP.

Cons

- May not operate effectively in large and dynamic network which different hosts come and go frequently.

Countermeasure against ARP poisoning

Set secure port to allow only authorized hosts tap into your LAN.

Pros

- It prevent outsiders to launch the attack in your LAN

Cons

- Cannot prevent insiders to launch the attack and tracking the attackers could be difficult.
- May not operate effectively in large and dynamic network (such as WLAN) which guest users come and go frequently.

Countermeasure against ARP poisoning

Broadcast servers and gateway MAC address periodically.

Pros

- It can interfere with ARP poisoning and make the attack more difficult.

Cons

- It will increase the broadcast traffic.
- It may not block the poisoning if attacker launch the attack aggressively (e.g. sending the poison packet in every microsecond). Thought ARP packet rate can be limited in a switch port to counter act the rapid poison packet, it may also block the normal ARP packets if lots of hosts are connected in that port.

Countermeasure against ARP poisoning

Set Dynamic ARP Inspection (DAI) to validate ARP entries in each switch ports.

Pros

- It can automatically validate the ARP entries in each switch ports if one side of partners is using DHCP to obtain IP

Cons

- If both sides do not use DHCP to obtain IP, the MAC entries in each switch port need to be hard coded manually.
- Hosts before the switch port are not protected. (e.g. attacker and victim hosts are connecting to the same AP in WLAN)

Countermeasure against DNS poisoning

Hard code the important server DNS entries in system hosts file.

Pros

- It makes the attack to these important servers difficult

Cons

- Difficult to operate for large and dynamic network and cannot protect for all hosts.

Countermeasure against DNS poisoning

Patch the DNS server to generate random transaction ID for each DNS query and rate limit the DNS query.

Pros

- It makes the brute force of spoofing DNS reply difficult

Cons

- It may affect the normal DNS operation when the DNS server need to serve lots of clients.

Countermeasure against DNS hijack

Avoid using hub, detect multiple DNS replies, and adopt the DNS Security Extensions (DNSSEC)

Pros

- It makes the sniffing and spoofing of DNS packet difficult.

Cons

- It can detect the hijack but may not block it. Some network infrastructure may not support DNSSEC

Countermeasure against Trojan Horse Program

Update patch; install firewall, anti-virus, and IDS; do not surf unsafe web pages; do not open unsolicited mails

Pros

- It makes intrusion difficult.

Cons

- Layman may not know how to operate and maintain these sophisticated security measures. Products that support generic environment unusually give false alarms.

More Countermeasures

Enable secure communication protection at both server and client side. E.G. IPSec, SSLv3 (using both server and user cert), PGP

Pro

- It makes the intercept more difficult

Con

- May not be supported by some network infrastructures and users need more effort to adopt these measures.

Conclusion

- More features, more user friendly, more easy to use => more security holes
- More security => lesser features, less user friendly, difficult to use
- We need to find a balance point to secure our cyberspace effectively and restore people confident to use Internet.