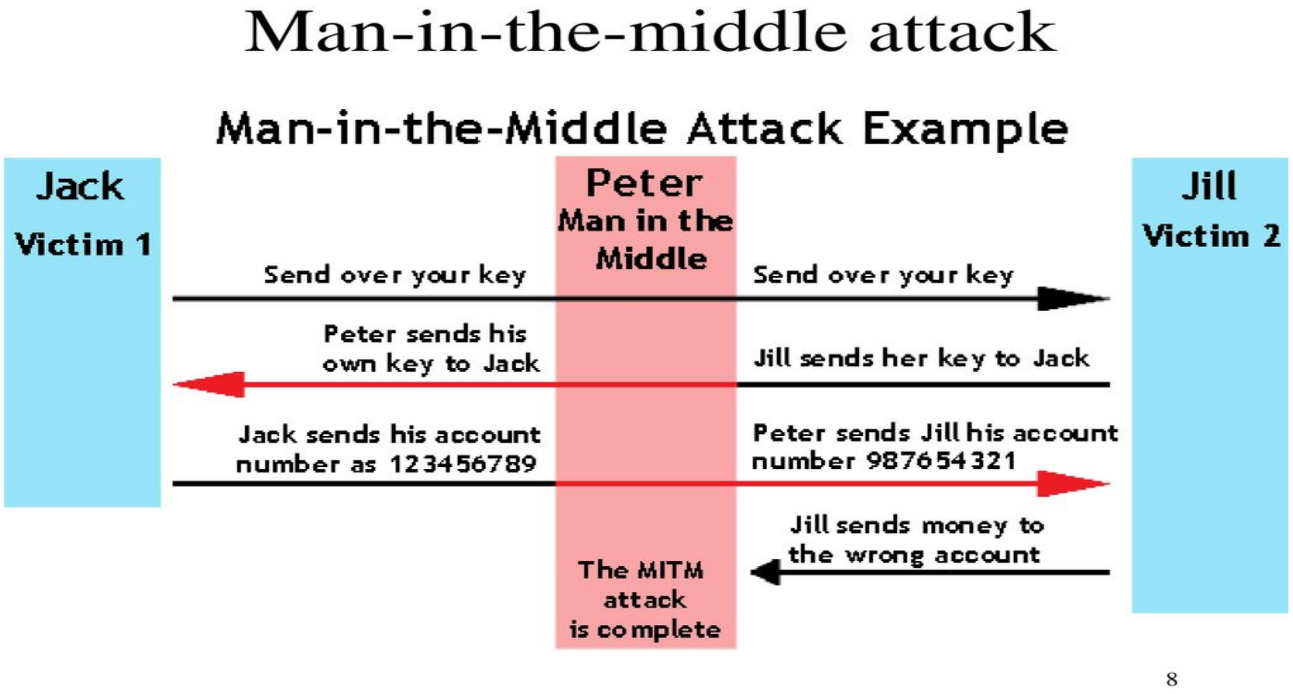
Man in the Middle attack

Introduction

What is MITM?

In cryptography and computer security, a Man-In-The-Middle Attack (MITM) also known as “Hijacking” is an attack where the attacker secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other.

Simple Scenario



Man-in-the-middle attack

Man-in-the-Middle Attack Example

Jack

Victim 1

Peter

Man in the Middle

Jill

Victim 2

Send over your key

Send over your key

Peter sends his own key to Jack

Jill sends her key to Jack

Jack sends his account number as 123456789

Peter sends Jill his account number 987654321

Jill sends money to the wrong account

The MITM attack is complete

8

Types of MITM attacks

- **ARP Spoofing**
- **DNS Poisoning**
- **DHCP Spoofing**
- SSL stripping
- Rogue Access Point
- IP Spoofing
- Email Hijacking
- HTTPS Spoofing

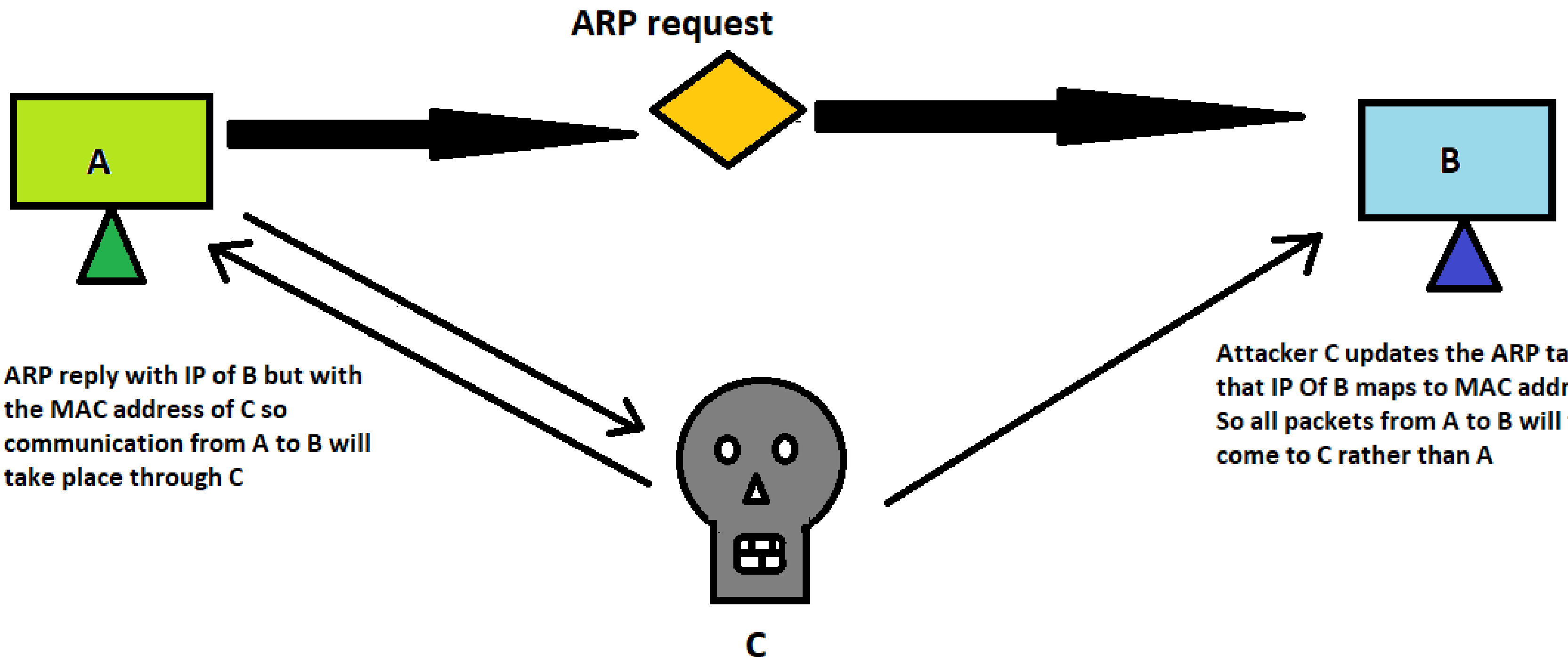
ARP Spoofing

ARP: ARP stands for **Address resolution protocol**. It is basically a protocol used by the IP, specifically IPv4 to map IP addresses to MAC address used by a data link protocol.

Every System has an ARP table where they store information about what IP address is associated with what MAC address. While sending a packet to an IP, the system will first check the ARP table to see if it has MAC address associated with that IP. If it is not present then it will broadcast the IP address across the network asking for it's corresponding mac address. Now the IP packet can be transferred successfully as source IP, MAC and Destination IP, MAC is known.

Command to check the arp table: **arp –a**

ARP Spoofing



ARP reply with IP of B but with the MAC address of C so communication from A to B will take place through C

Attacker C updates the ARP table of A that IP Of B maps to MAC address of C. So all packets from A to B will first come to C rather than A

ARP Spoofing

System A can send IP packets to B as the ARP Table of A has the IP address of B assigned to MAC address of B. So communication would take place.

But if the attacker C gives an ARP reply with the IP address of B but with the MAC address of itself (i.e. MAC address of C) and as ARP has no authentication mechanism, the A’s ARP table will be updated that the IP address of B maps to MAC address of attacker C.

So A on sending any packet to B, the packet will go to C. Now C can assign a forwarding mechanism that will forward the same packet from C to B thus initiating a Man in the middle attack where C will be in the middle and see all the requests.

ARP Spoofing

MITIGATIONS

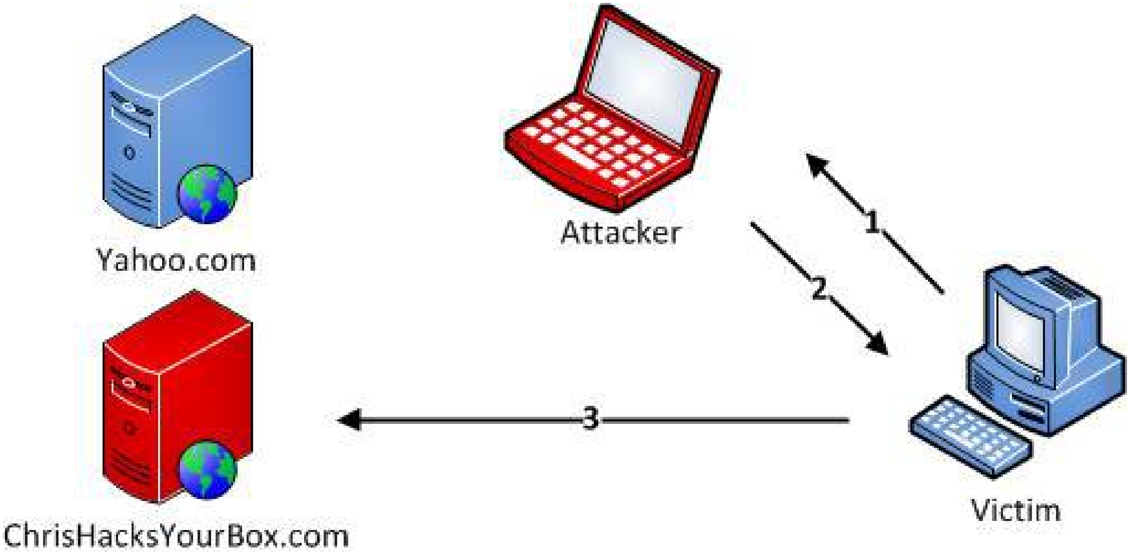
- Use a static ARP table
- Always use a Virtual Private network while connecting to public Wifi

DNS Poisoning

DNS: The **Domain Name System** (DNS) is a central part of the Internet, providing a way to translates human readable domain names (for example, theblocksec.com) to machine readable IP addresses (for example, 51.80.12.44).

DNS poisoning/spoofing is a MITM technique used to supply false DNS information to a host so that when they attempt to browse, for example, www.bankofamerica.com at the IP address 52.78.90.43 they are actually sent to a fake www.bankofamerica.com residing at IP address 192.168.0.2 which an attacker has created in order to steal account information from unsuspecting users.

DNS Poisoning



1. Legitimate DNS Request Destined for DNS Server
2. Fake DNS Reply from Listening Attacker
3. Victim begins communicating with malicious site as a result

DNS Poisoning

DNS Poisoning can be achieved in many ways but one of the most common methods is to use the Arp spoofing method to achieve DNS spoofing where in the attacker first conducts an arp spoof attack between the victim machine and the network gateway so that all the requests will travel via the attacker.

In a typical scenario, when the victim types in example.com it will first query the DNS server for DNS name translation but since it will go through the attacker, the attacker machine sends a fake DNS reply that the example.com maps to 192.168.0.2(IP address of the attacker).

This will eventually open the page hosted by the attacker in it’s own machine.

DNS Poisoning

MITIGATIONS

- **Use IDS:** An intrusion detection system, when placed and deployed correctly, can typically pick up on most forms of ARP cache poisoning and DNS spoofing.

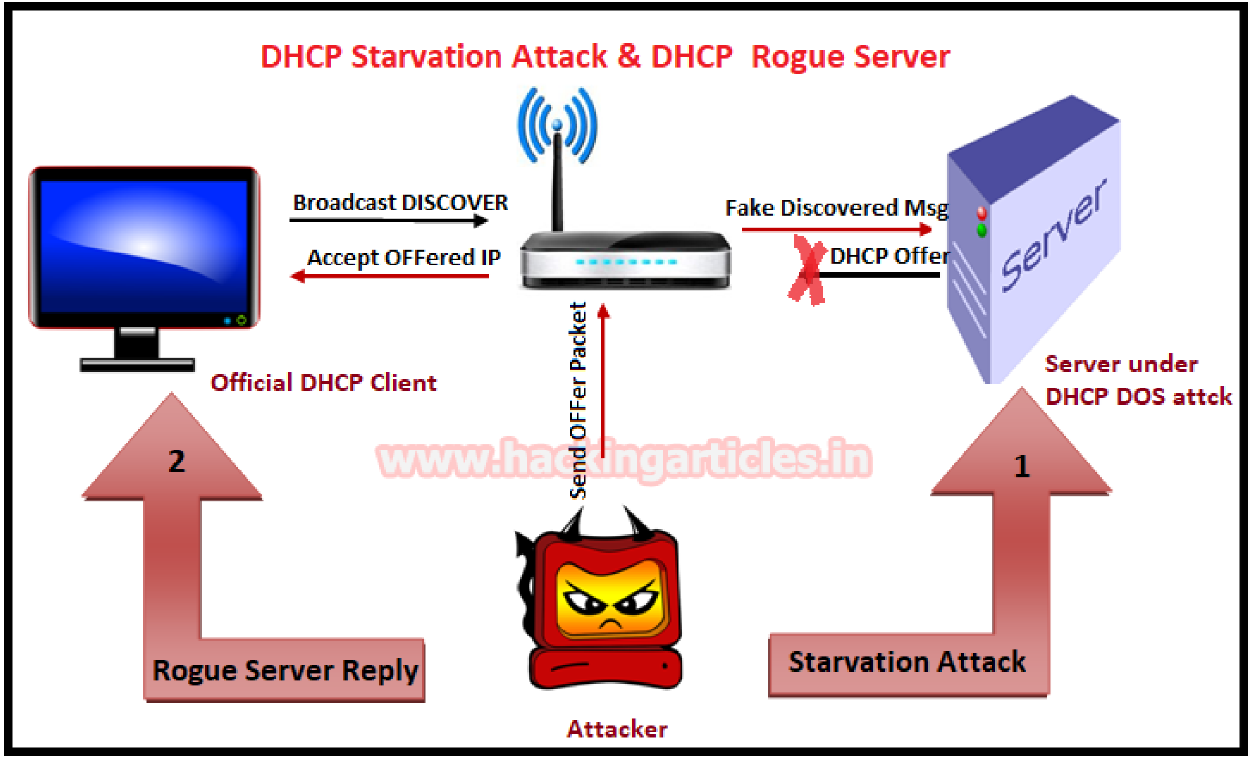
- **Use DNSSEC:** DNSSEC is a newer alternative to DNS that uses digitally signed DNS records to ensure the validity of a query response. DNSSEC is not yet in wide deployment but has been widely accepted as "the future of DNS".

DHCP Spoofing

DHCP: The **Dynamic Host Configuration Protocol** (**DHCP**) is a network management protocol used on UDP/IP networks whereby a DHCP server dynamically assigns an IP address and other network configuration parameters to each device on a network so they can communicate with other IP networks

DHCP spoofing occurs when an attacker attempts to respond to DHCP requests and trying to list themselves (spoofs) as the default gateway or DNS server, hence, initiating a man in the middle attack.

DHCP Spoofing



www.hackingarticles.in

DHCP Spoofing

DHCP spoofing is usually achieved by a combination of both DHCP starvation and spoofing attack.

DHCP Starvation Attack:

In a DHCP starvation attack, an attacker broadcasts large number of DHCP REQUEST messages with spoofed source MAC addresses. If the legitimate DHCP Server in the network start responding to all these bogus DHCP REQUEST messages, available IP Addresses in the DHCP server scope will be depleted within a very short span of time.

DHCP Spoofing

DHCP Spoofing Attack:

After a DHCP starvation attack, a rogue DHCP server is set wherein the attacker can start distributing IP addresses and other TCP/IP configuration settings to the network DHCP clients. TCP/IP configuration settings include Default Gateway and DNS Server IP addresses. Network attackers can now replace the original legitimate Default Gateway IP Address and DNS Server IP Address with their own IP Address.

Once the Default Gateway IP Address of the network devices are is changed, the network clients start sending the traffic destined to outside networks to the attacker's computer. The attacker can now capture sensitive user data and launch a man-in-the-middle attack

DHCP Spoofing

MITIGATIONS

- **Port security**: The techniques that mitigate CAM table flooding also mitigate DHCP starvation by limiting the number of MAC addresses on a switch port. You would use the port-security command to set the MAC address of a valid DHCP server on a switch port to prevent any other device from connecting to that trusted port.

- **DHCP snooping**: DHCP snooping is a security feature that filters untrusted DHCP messages and builds and maintains a DHCP snooping binding table.

Conclusion

MITM is really a difficult type to tackle and hence should be taken seriously by IT management. It can result in data theft causing severe reputational and monetary losses to the corporate firms.

As a bottom-line, having a correctly defined security perimeter defense design, server and network component's hardening, implementing robust patch management system and following best security practices can help fix MITM attacks.

Since this attack may not be visible, being vigilant in terms of network problems and performance always helps detect it, before a data theft can occur.

Thank You