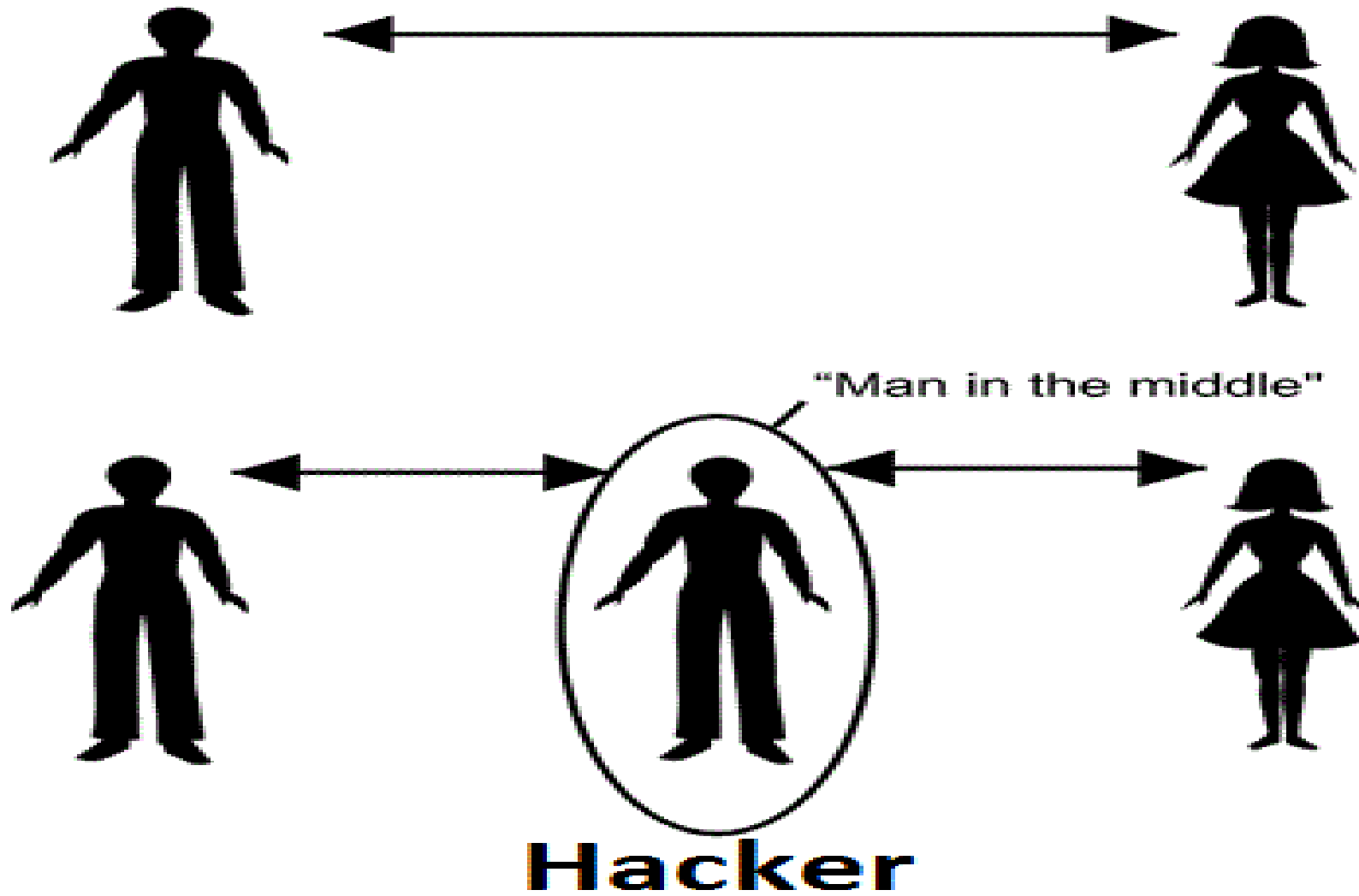


Man In-The Middle Attack

MITM



What is MITM ?

- ▶ A man-in-the-middle (MITM) attack is a form of eavesdropping where communication between two users is monitored and modified by an unauthorized party. Generally, the attacker actively eavesdrops by intercepting a public key message exchange and retransmits the message while replacing the requested key with his own.

MITM attack is also known as:

- ▶ Bucket-brigade attack
- ▶ Fire brigade attack
- ▶ Monkey-in-the-middle attack
- ▶ Session hijacking
- ▶ TCP hijacking
- ▶ TCP session hijacking

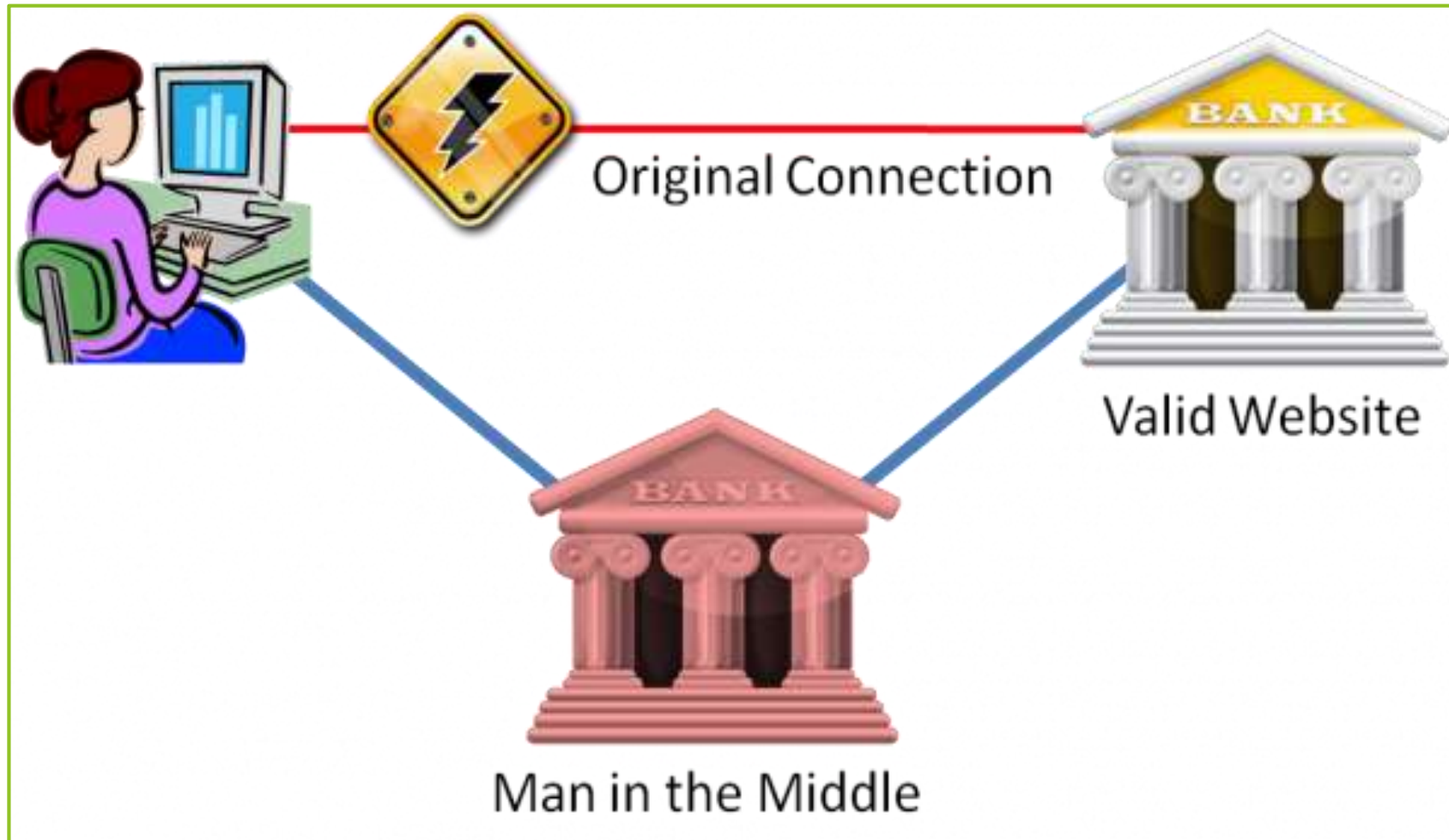
Name Origin:

- ▶ The name "Man-in-the-Middle" is derived from the basketball scenario where two players intend to pass a ball to each other while one player between them tries to seize it. MITM attacks are sometimes referred to as "bucket brigade attacks" or "fire brigade attacks." Those names are derived from the fire brigade operation of dousing off the fire by passing buckets from one person to another between the water source and the fire.

How Does It Work?

- ▶ Man in the middle is known most to others as "session hijacking" and to general public as "hijacking". These hackers are primarily targeting specific data about the transactions on computers. This can be anything from an email to a bank transaction that said the hackers begin their investigation of the party of interest.

A BASIC ILLUSTRATION



What is wireless

- More or less it is a radio signal that carries a digital signal.



Sender (Router)

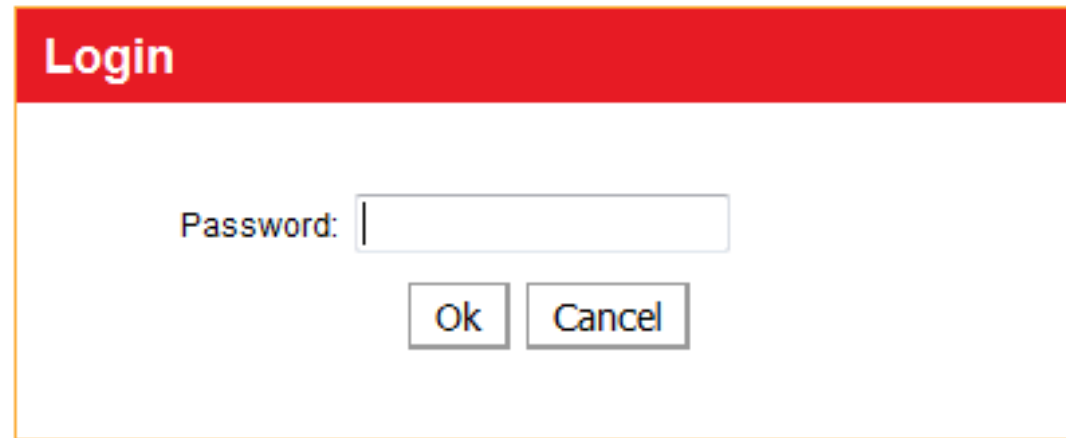
Receiver

Project Description

- ▶ Configure a wireless network
- ▶ Perform a Man-in-the-Middle (MITM) attack over a wireless network
 - ▶ **MITM** is an attack in which an attacker is able to read, insert and modify at will, messages between two parties without either party knowing that the link between them has been compromised. (Wikipedia)

Log in to The Router Admin

- Using IE we connected to the gateway(IP Address:192.168.1.1) and entered the default password

A screenshot of a web browser login dialog box. The dialog has a red header bar with the word "Login" in white. Below the header, the text "Password:" is followed by a text input field. At the bottom of the dialog, there are two buttons: "Ok" and "Cancel".

Login

Password:

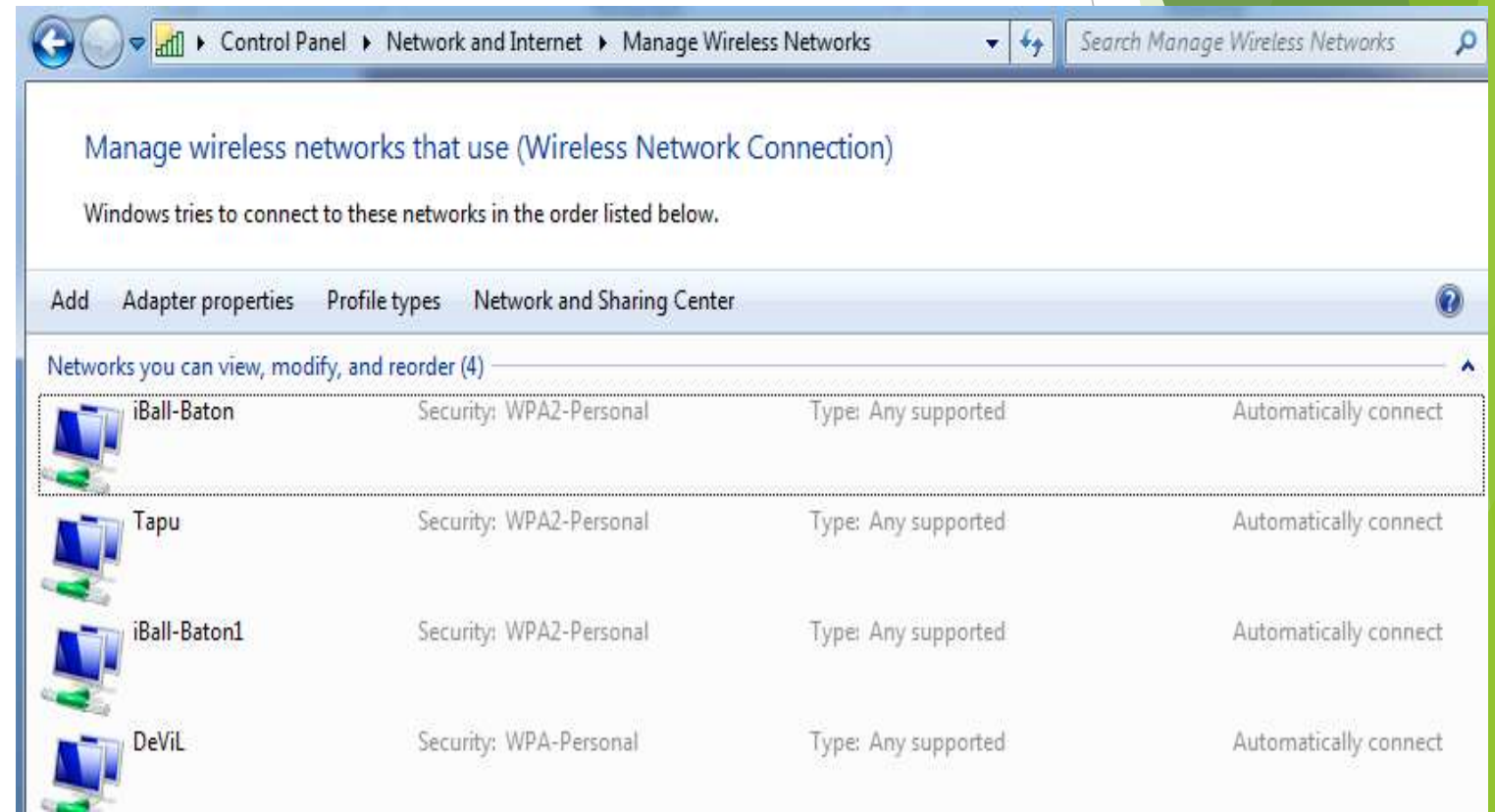
Ok Cancel

WEP Configuration

- ▶ Changed SSID, changed default username and password to log in and enabled WEP with one key.
- ▶ Channel 6 was used instead of 11 because the router was firmware routed to number 6 only.

Securing Our Wireless Network

- We are then able to see and connect to the network we have configured



MAC Filtering

- ▶ Turned on MAC filtering and cloned the known computer and only allowed it

MAN IN THE MIDDLE

How It Works?

- ▶ The MitM poisons the ARP cache of the victim and the server/gateway/switch
- ▶ So the victim computer then thinks the hacker's ARP address is the gateway's.
- ▶ The gateway thinks the hacker's ARP address is the victim computer's.
- ▶ All data is redirected through the listening system.

MAN IN THE MIDDLE

Basic Attacks

- ▶ Read all clear text information passed between the hosts (i.e., browser requests, username/passwords)
- ▶ Log/trap all data packets
- ▶ Packet injection

(all these attacks can be performed through traffic dumps and setting your NIC to promiscuous mode)

MAN IN THE MIDDLE

Advanced Attacks

- ▶ Traffic Blocking
 - ▶ Web page denied - 404 error even though the page works fine
- ▶ Filters
 - ▶ Listen for any signature and change it
- ▶ Break Encryption
 - ▶ Crypto rollbacks and de-authorization

Similar Attacks

- ▶ HostAP can be used to create a rogue access point that clients will authenticate with, much like ARP poisoning, but it's more obvious to admin's.
- ▶ Other MITM attacks can use HostAP to deauthenticate a client and force it to re-authenticate with themselves on a different channel.

Protections

- ▶ SSL connections *may* prevent you from connecting through the MITM.
- ▶ Read certificates carefully (https pass through) before connecting.
 - ▶ File-Encrypt (Other encrypted files) any file you don't want intercepted.
- ▶ WEP won't work at all because the hacker can tumble your data and find the Key. With the key, all traffic can be decrypted on-the-fly, as if it's clear text.

Sniffing

- ▶ It is the easiest attack to launch since all the packets transit through the attacker.
- ▶ All the “plain text” protocols are compromised (the attacker can sniff user and password of many widely used protocol such as telnet, ftp, http)

Hijacking

- ▶ Easy to launch
- ▶ It isn't blind (the attacker knows the sequence numbers of the TCP connection)

Injecting

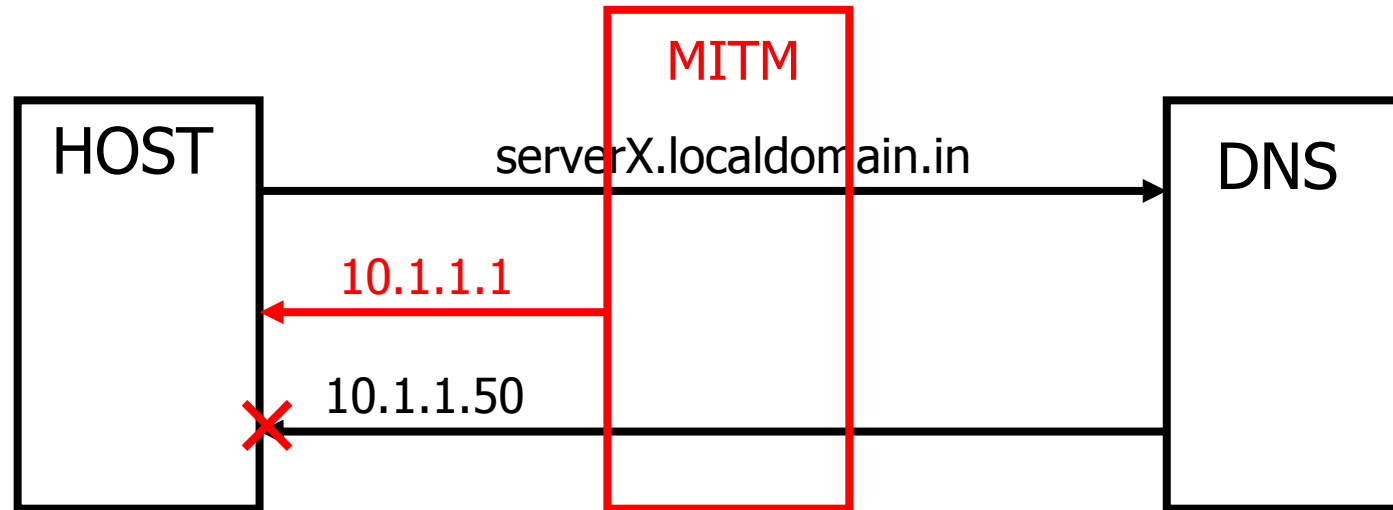
- ▶ Possibility to add packets to an already established connection (only possible in full-duplex connection (only possible in full-duplex mitm)).
- ▶ The attacker can modify the sequence numbers and keep the connection synchronized while injecting keep packets.
- ▶ If the mitm attack is a “proxy attack proxy attack” it is even it easier to inject (there are two distinct connections).

Filtering

- ▶ The attacker can modify the payload of the packets by recalculating the checksum.
- ▶ He/she can create filters on the fly.
- ▶ The length of the payload can also be changed but only in full-duplex (in this case the seq has to be adjusted).

DNS spoofing

- ▶ If the attacker is able to sniff the ID of the DNS request,
- ▶ he/she can reply before the real DNS server



THANK
YOU