Chapter-#10

Man-in-the-middle (MITM) Attacks

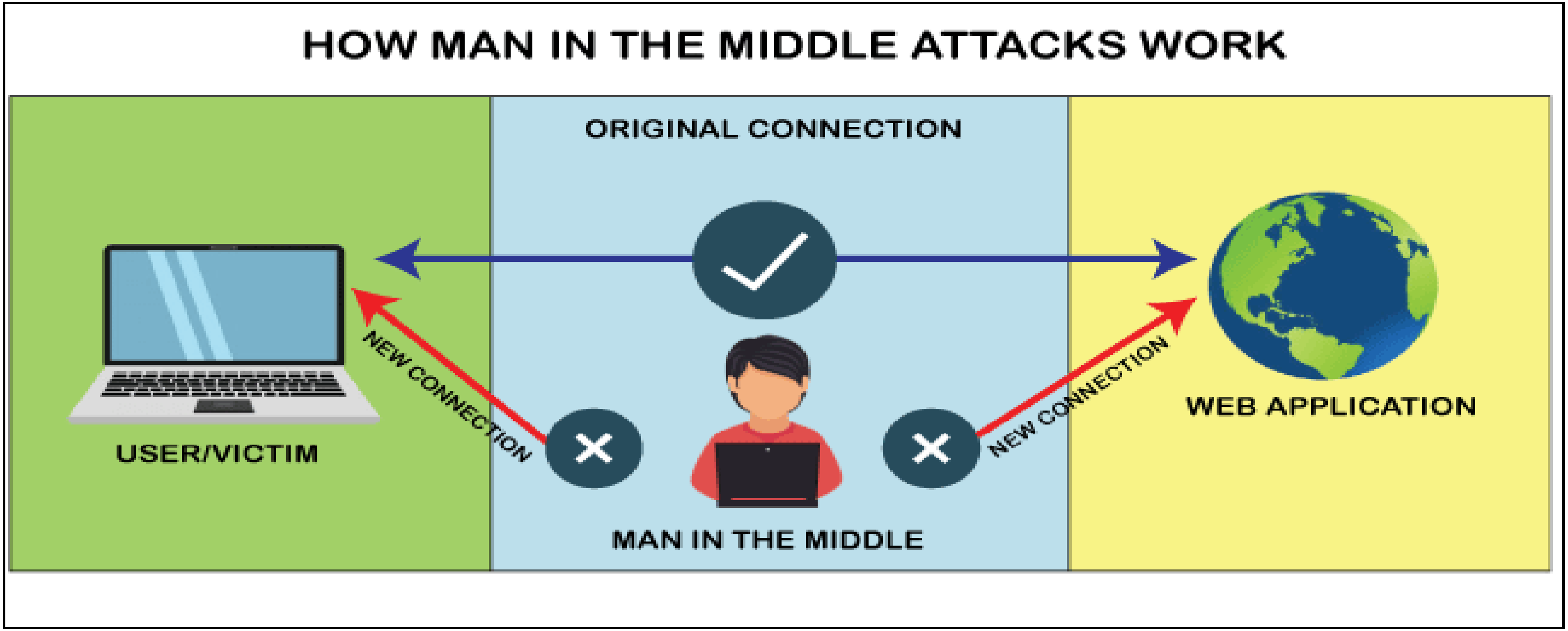
Man-in-the-middle (MITM) Attacks

- ## What is MITM Attack
- A MITM attack is a form of cyber-attack where a user is introduced with some kind of meeting between the two parties by a malicious individual, manipulates both parties and achieves access to the data that the two people were trying to deliver to each other. A man-in-the-middle attack also helps a malicious attacker, without any kind of participant recognizing till it's too late, to hack the transmission of data intended for someone else and not supposed to be sent at all. In certain aspects, like MITM, MitM, MiM or MIM, MITM attacks can be referred.
- If an attacker puts himself between a client and a webpage, a Man-in-the-Middle (MITM) attack occurs. This form of assault comes in many different ways.
- **For example**, In order to intercept financial login credentials, a fraudulent banking website can be used. Between the user and the real bank webpage, the fake site lies "in the middle."

Man-in-the-middle (MITM) Attacks

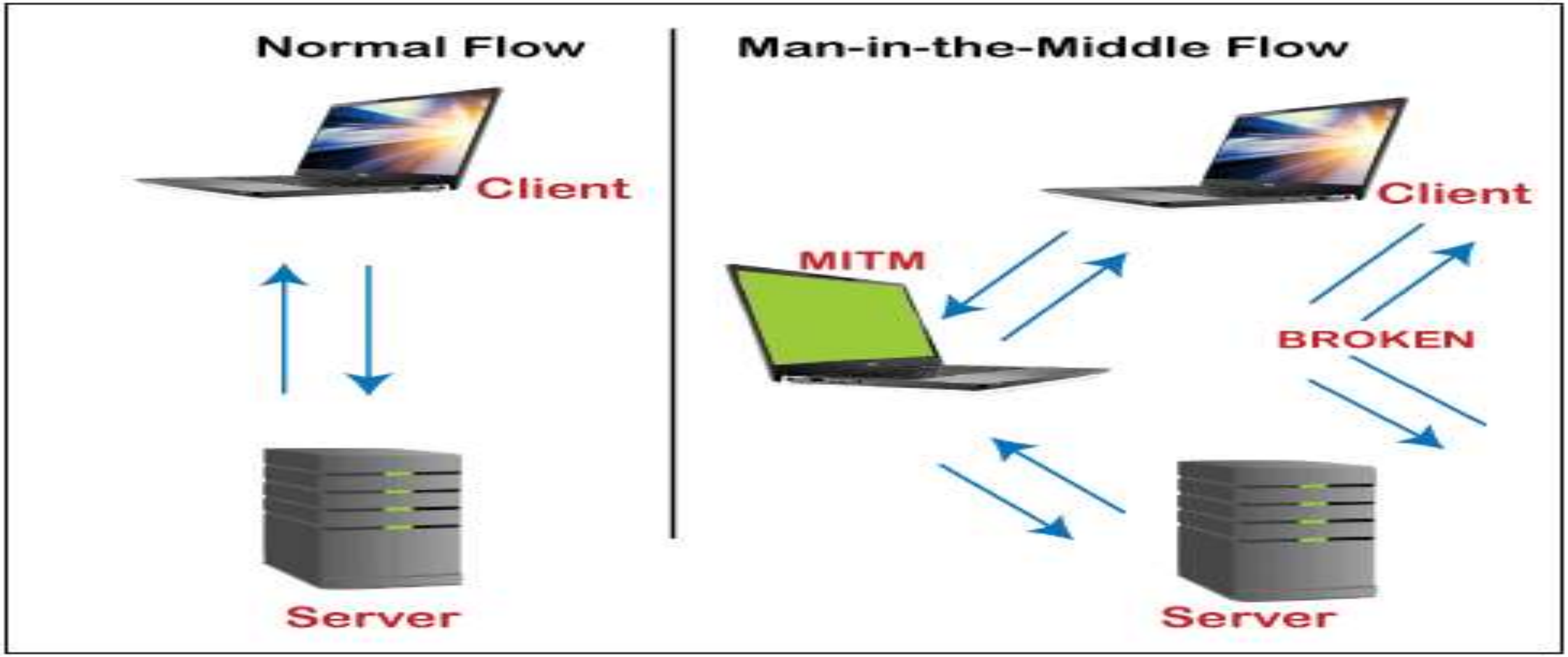
How does MITM work

- There are several reasons and strategies for hackers to use a MITM attack. Usually, like credit card numbers or user login details, they try to access anything. They also spy on private meetings, which may include corporate secrets or other useful information.
- The feature that almost every attack has, in general, is that the attacker pretends to be somebody you trust (or a webpage).



Man-in-the-middle (MITM) Attacks

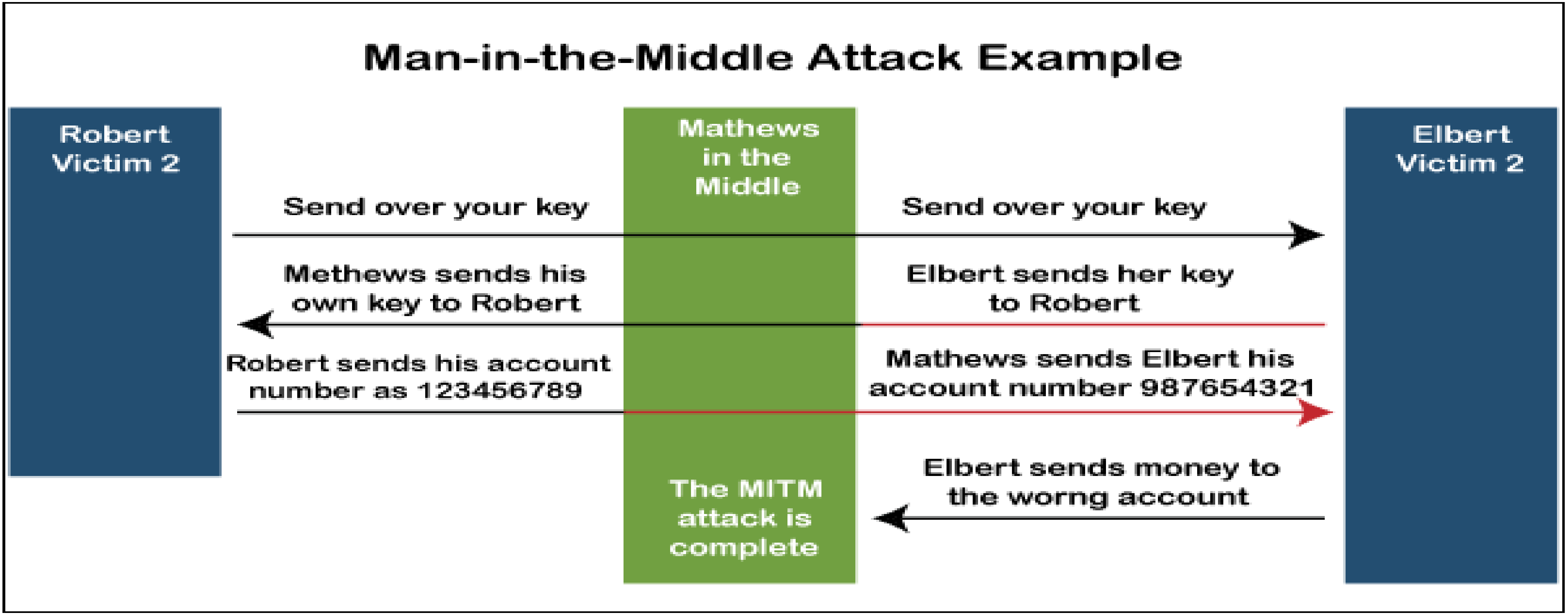
- **Real life Instances of MITM attack**



- In the above diagram, you can see that the intruder positioned himself in between the client and server to intercept the confidential data or manipulate the incorrect information of them.

Man-in-the-middle (MITM) Attacks

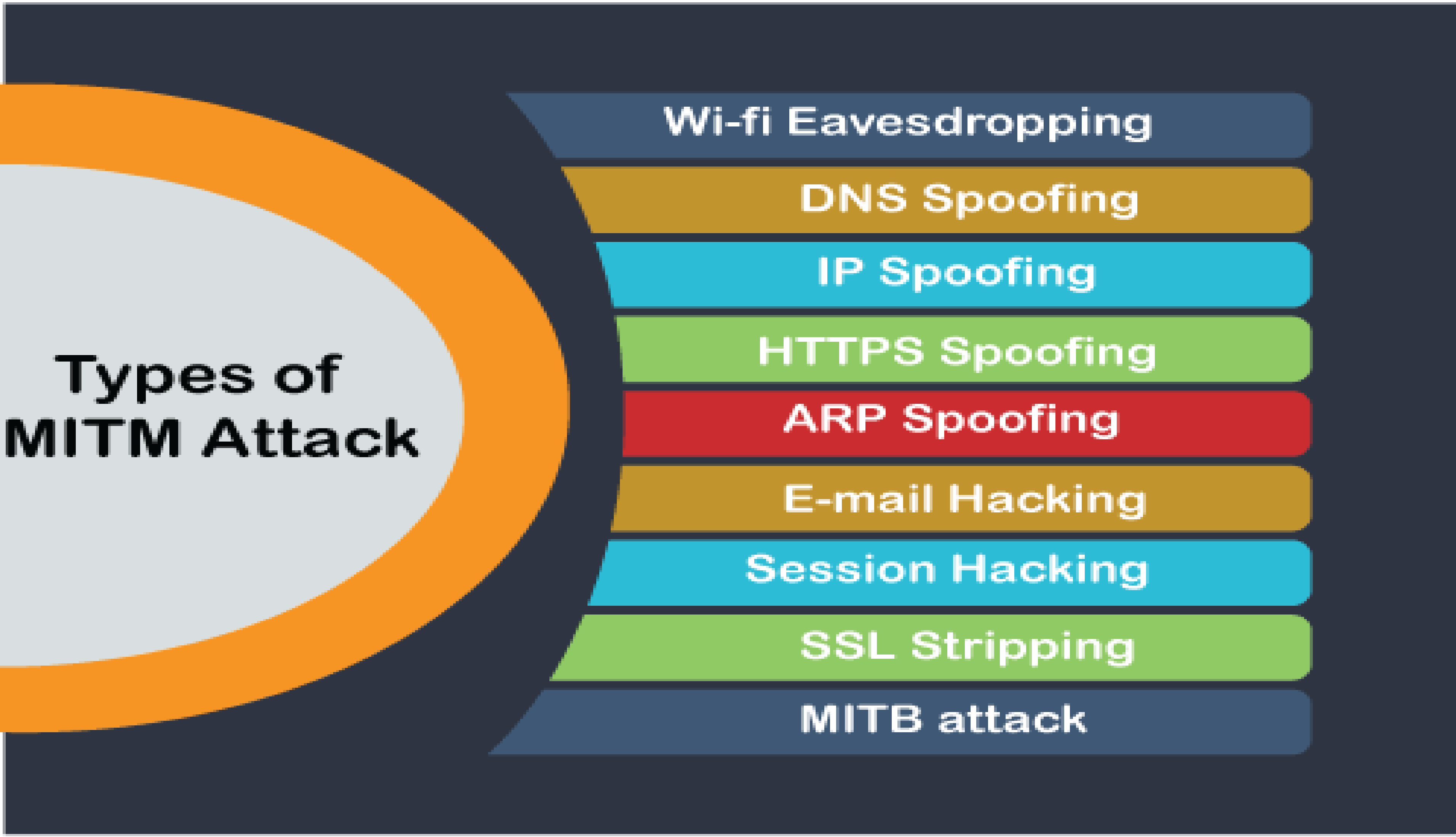
- Another Instance of MITM attack


Man-in-the-Middle Attack Example
Robert Victim 2
Mathews in the Middle
Elbert Victim 2
Send over your key
Send over your key
Methews sends his own key to Robert
Elbert sends her key to Robert
Robert sends his account number as 123456789
Mathews sends Elbert his account number 987654321
Elbert sends money to the worng account
The MITM attack is complete

- As shown in the above picture, to obtain access to banking, the attacker is trying to imitate both sides of the discussion. This instance is accurate for the client and the server discussions and also person-to-person discussions. Shown in this instance, the attacker retrieves a public key and can modulate his own passwords to manipulate the audience to accept that they are safely communicating with each other at either end.

Man-in-the-middle (MITM) Attacks

- Types of MITM Attack



Man-in-the-middle (MITM) Attacks

- Wi-fi Eavesdropping
- DNS Spoofing
- IP Spoofing
- HTTPS Spoofing
- ARP Spoofing
- E-mail Hacking
- Session Hacking
- SSL Stripping
- MITB attack

Man-in-the-middle (MITM) Attacks

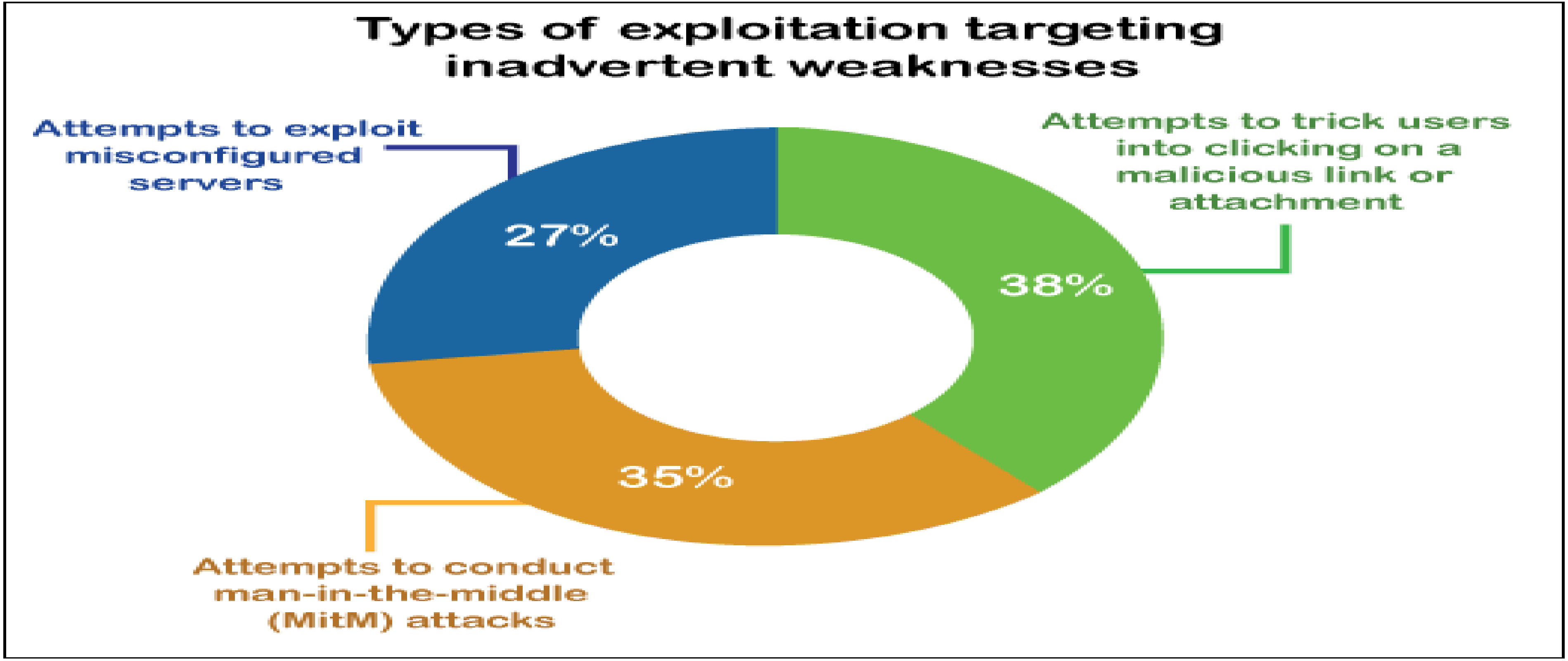
- **Wi-fi Eavesdropping**
- You may have seen a notification that suggests, "This connection is not safe," if you've used a device in a cafe. Public wi-fi is typically offer "as-is," without any promises of service quality.
- The unencrypted wi-fi networks are easy to watch. Although, it's just like having a debate in a public place-anybody can join in. You can limit your access by setting your computer to "public," which disables Network Discovery. This avoids other users on the network from exploiting the system.
- Some other Wi-Fi snooping attack occurs when an attacker establishes his own "Evil Twin" wi-fi hotspot. Attacker make the link, through the network Address and passwords, appear identical to the real ones. Users will link to the "evil twin" unintentionally or automatically, enabling the attacker to intrude about their actions.

Man-in-the-middle (MITM) Attacks

- ## DNS Spoofing
- The Site operates with numeric IP addresses like 192.156.65.118 is one of Google's addresses.
- For example, a server is used by several sites to interpret the address to a recognizable title: google.com. A DNS server, or DNS, is the server that transforms 192.156.65.118 to google.com.
- A fraudulent Web server can be developed by an attacker. The fraudulent server transports a specific web address to a unique IP address, which is termed as "spoofing."
- ## IP Spoofing
- Many devices connected to the same network contains an IP address, as we all know. Each device is equipped with its IP address in several enterprise internal web networks. In IP spoofing, the attackers imitate an approved console's IP address. For a network, it appears just as the system is authorized.
- It might be causing a network to be exploited by unauthorized access. They must stay quiet and track the actions, or a Denial of Service (DoS) attack may also be released. In a Middle-in-the-man attack, IP spoofing may also be used by placing between two devices.

Man-in-the-middle (MITM) Attacks

- **For Example,** Device A and device B assume that they communicate with each other, but both are intercepted and communicated to the attacker.
- Device A= = = = Attacker= = = = Device B
- 35 percent of the intrusion operations include hackers conducting MITM exploits, as per the IBM X-Force 's Threat Intelligence 2018 Reports. It is represented in below Pie chart.



Man-in-the-middle (MITM) Attacks

HTTPS Spoofing

- Duplicating an HTTPS webpage is not currently possible.
- A theoretical approach for circumventing HTTPS, however, has been illustrated by cyber security experts. The attacker creates an authoritative address.
- It uses letters of international alphabets rather than standard scripts. This acts as phishing emails with unusual characters that you might have used. Rolex may be written Rólex, for example.

ARP Spoofing

- ARP refers to the Protocol on Address Resolution.
- An ARP request is sent out by a client, and an attacker produces a fraudulent response. The attacker is like a computer modem in this situation, which enables the attacker to access the traffic flow. Usually, this is restricted to local area networks (LAN) that use the ARP protocol.

Man-in-the-middle (MITM) Attacks

- ## E-mail Hacking

- An attacker exploits the email system of a user in a such a kind of cyber security intrusion. The intruder also watches quietly, collecting data and eavesdropping on the discussion via email. The Attackers may have a scan pattern that searches for targeted keywords, such as "financial" or "hidden Democratic policies."

- Through Social Engineering, email hacking operates perfectly. To imitate an online friend, the attackers might use relevant data from some kind of hijacked email address. Spear-phishing can also be used to trick a user into downloading malicious apps.

- ## Session Hacking

- Usually, this form of MITM attack is often used to hack social media platforms. The webpage contains a "session browser cookie" on the victim's machine for most social media platforms. If the person steps off, this cookie is disproved. But when the session is running, the cookie offers identity, exposure, and monitoring data.

Man-in-the-middle (MITM) Attacks

- A Session Hijack happens when a configuration cookie is stolen by an intruder. Unless the victim's account is hacked with malware or application attackers, it can arise. It can occur if a user exploits an XSS cross-scripting intrusion, in which the hacker injects malicious script into a site that is commonly visited.
- ## SSL Stripping
- SSL refers to Secure Socket Layer. SSL is the security standard used if you see https:/ next to a website address, not http:/. The attacker accesses and routes data packets from a user using SSL Stripping:
- **User = = = = Encrypted website User = = = = Authenticated website**
- The user tries to link to a website that is secured. In the account of the client, the attacker encrypts and links to the secured website. Usually, a fake design is developed by the attacker to present it to the customer. The victim thinks that they have signed on to the normal website, but actually they signed in to a hacker's website. The attacker does have the SSL certificate "stripped" from the data connection of the victim.

Man-in-the-middle (MITM) Attacks

MITB attack

- This is a form of attack that leverages internet browser security flaws.
- The malicious attacks will be trojans, desktop worms, Java vulnerabilities, SQL injection attacks, and web browsing add-ons. These are commonly used to collect financial information.
- Malware steals their passwords as the user signs in to their bank account. In certain instances, malware scripts may move money and then alter the receipt of the transaction to conceal the transaction.

Detection of Man-in-the-middle attack

- It is harder to identify a MITM attack without taking the appropriate measures. A Man-in-the-middle assault will theoretically proceed unchecked till it's too late when you do not consciously need to evaluate if your interactions have been monitored. Usually, the main technique for identifying a potential-attacks are always searching for adequate page authorization and introducing some kind of temper authentication; however, these approaches may need further forensic investigation after-the-fact.

Man-in-the-middle (MITM) Attacks

- Instead of trying to identify attacks when they are operational, it is necessary to manage precautionary measures to avoid MITM attacks whenever they occur. To sustain a safe environment, being mindful of your surfing habits and identifying possibly hazardous environments can be important.

Preventions of Man-in-the-middle attack

- Here, we have discussed some prevention techniques to avoid the interactions being compromised by MITM attacks.

1. Wireless access point (WAP) Encryption

- Creating a strong protection feature on access points eliminates legitimate access just from being closer from accessing the system. A vulnerable system of protection will enable an intruder to brute-force his way into the system and start attacking the MITM.

2. Use a VPN

- Use a Virtual Private Network (VPN)
To encrypt your web traffic, an encrypted VPN severely limits a hacker's ability to read or modify web traffic.
Be prepared to prevent data loss; have a cyber security incident response plan.

Man-in-the-middle (MITM) Attacks

- Network Security
- Secure your network with an intrusion detection system. Network administrators should be using good network hygiene to mitigate a man-in-the-middle attack.
  Analyze traffic patterns to identify unusual behavior.
- 3. Public Key Pair Authentication
- MITM attacks normally include something or another being spoofed. In different layers of the protocol stack, public key pair authentication such as RSA is used to ensure that the objects you communicate with that are essentially the objects you want to communicate with.
- 4. Strong Network User Credentials
- Ensuring that the primary email login is modified is extremely important. Not only the login credentials for Wi-Fi but the password hashes for your router. When a hacker detects the wireless router login details, they can switch the fraudulent servers to the DNS servers. Or, at worst, hack the modem with harmful malware.

Man-in-the-middle (MITM) Attacks

- **5. Communication security**
- Communication security help the users to protect from unauthorized messages and provides secure data encryption.
- Enabling two-factor authentication is the most powerful way to avoid account hacking. It implies that you'll have to give another protection factor, in contrast with your login credentials. One instance is the conjunction of a login credential and a text to your device from Gmail.
- **6. Using proper hygiene for network protection on all platforms, such as smart phone apps.**
- Since phishing emails are the most popular attack vector when lookout a spam email. Analyze the references cautiously before opening.
- Just mount plug-ins for the browser from trusted sources.
- Reduce the chance of exploits to disprove persistent cookies by logging out inactive accounts.
- Avoid what you're doing and execute a security scan if you anticipate a secure link but do not have one.

Man-in-the-middle (MITM) Attacks

- **7. Avoid using public wi-fi**
- Configure your phone to require a manual link if you're using public wi-fi.
- It can be hard to identify MITM attacks as they are occurring. The easiest way to remain secure is to regularly incorporate all of the above prevention for security.
- Be conscious that such attacks are a part of social engineering. Take a couple of minutes to dig deeper if anything doesn't seem normal about social media and email.