September 17, 2024

“What Happens During a Hijacking?”

Foundations of Cybersecurity - CYBS 3213

Christopher Freeze, Ph.D.
Assistant Professor, Cybersecurity
OU Polytechnic Institute

OU Tulsa
SCHUSTERMAN CENTER

Checking In

Last time we looked at “Who Are You?” (Identity and Access Management)

1. **Different Authentication Factors**: Something you know (password), have (smart card or phone), or are (biometrics).
2. **Multi-Factor Authentication (MFA)**: Single-factor authentication (SFA), two-factor authentication (2FA), and multi-factor authentication (MFA).
3. **Authentication Protocols and Methods**: Password Authentication Protocol (PAP), Challenge Handshake Authentication Protocol (CHAP), and Kerberos, RADIUS.
4. **Access Control Models**: Role-Based Access Control (RBAC), Mandatory Access Control (MAC), and Discretionary Access Control (DAC), approaches for managing permissions.

Checking In

- What have been the most important concepts that you learned in the last classes?
- What have been the muddiest (most unclear) poinst during the last classes?

https://www.popularmechanics.com/flight/a45639586/who-was-db-cooper/


NETFLIX
OFFICIAL
TRAILER

hijacking

crime

hijacking, the illegal seizure of a land vehicle, aircraft, or other conveyance while it is in transit.

https://www.britannica.com/topic/hijacking

Denial-of-Service:

- DoS is an attack against a network resource that aims to prevent, disrupt, or delay authorized users from accessing the network resource.

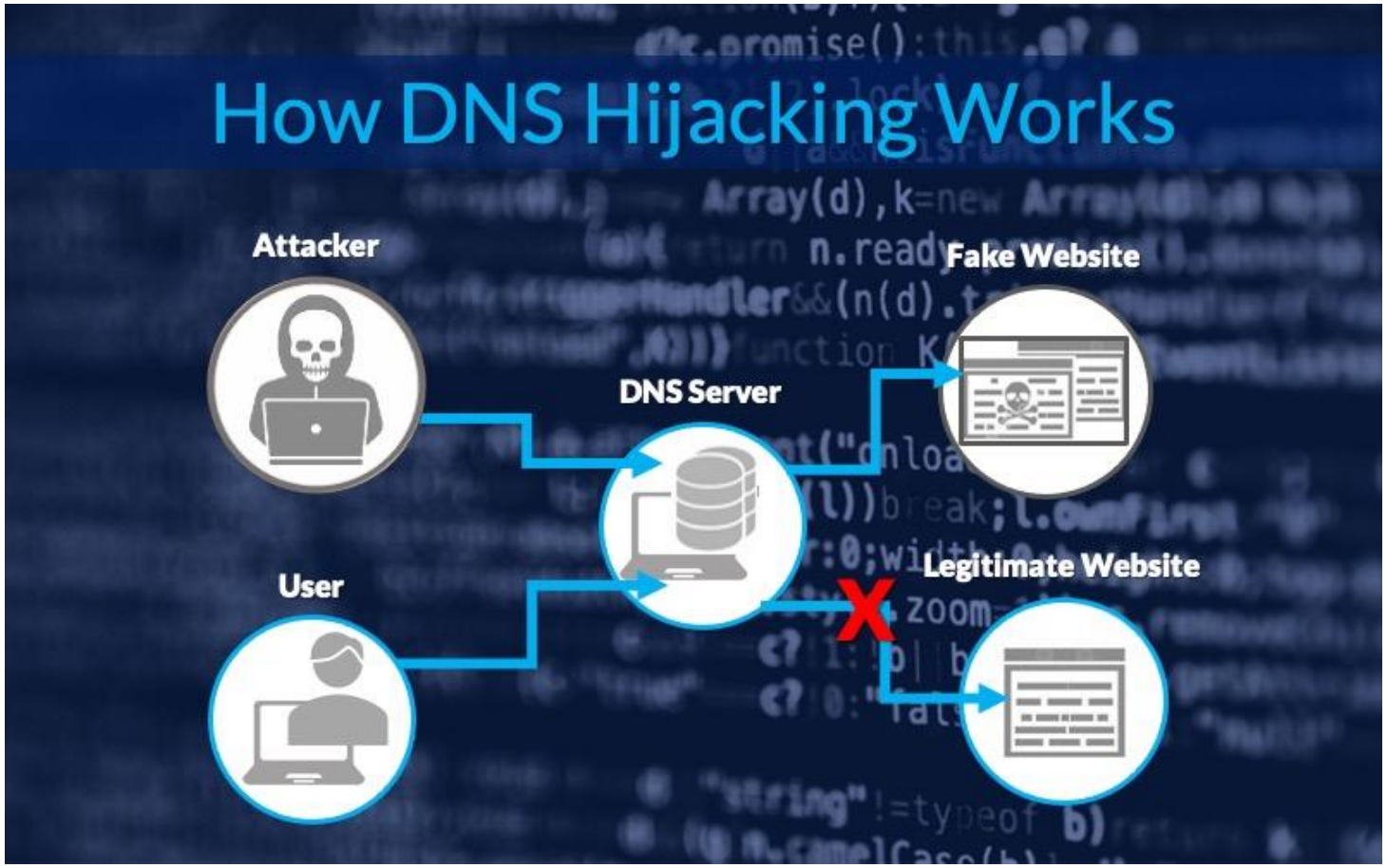
Distributed Denial-of-Service

- DDoS attack is a DoS attack that is simultaneously launched from multiple systems.

Domain Name System (DNS)

Domain hijacking - act of taking control of a website's domain without the knowledge or consent of the domain owner.

DNS poisoning, also known as DNS cache poisoning, or DNS spoofing, is an attack tricks a DNS server into sending users to the wrong website, often a malicious one, instead of the legitimate site they were trying to visit.

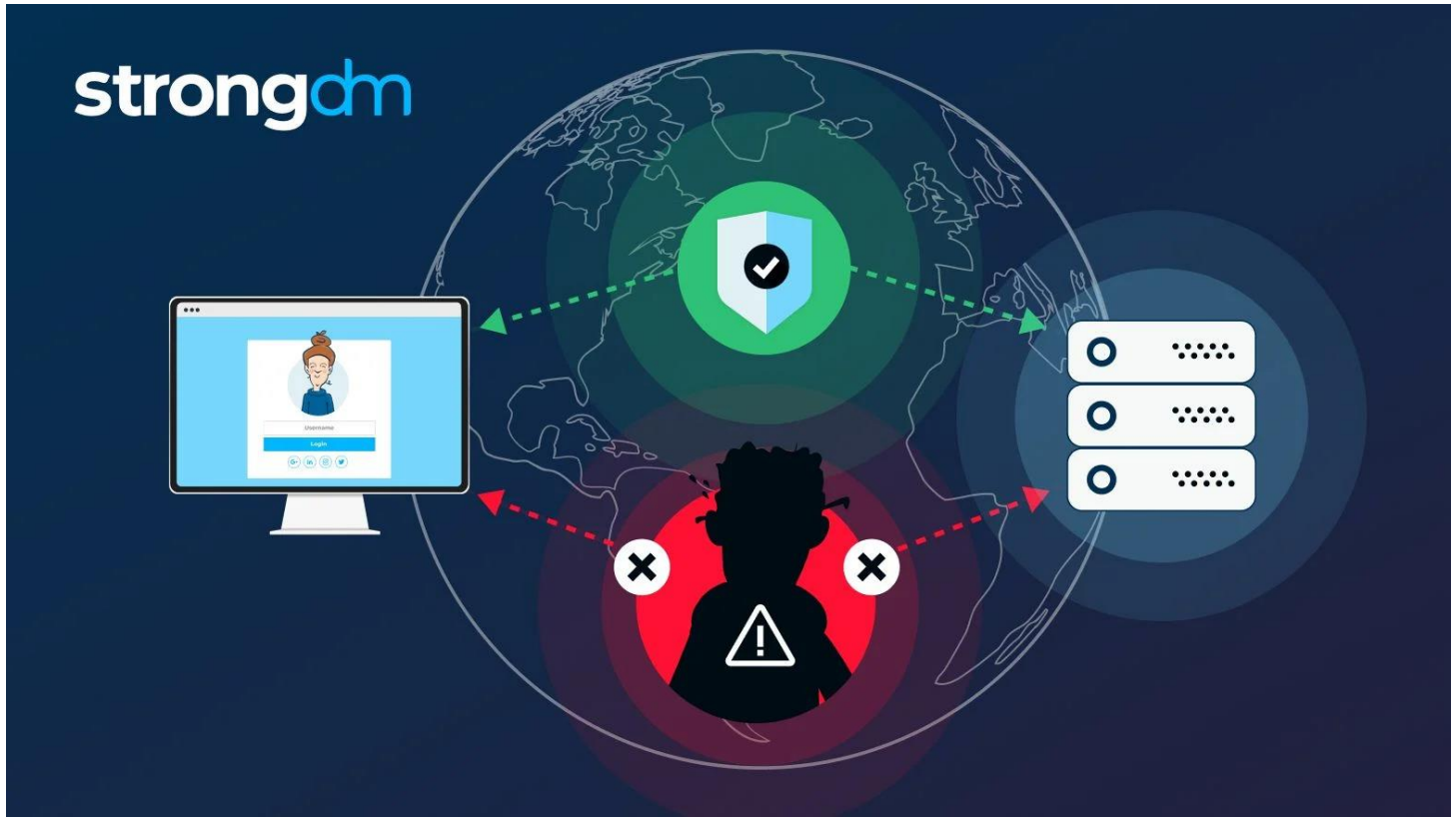


Address resolution protocol (ARP) poisoning sends fake ARP messages on a local network, making a device associate the attacker's **MAC address** (permanent) with the IP address of a legitimate device (like a PC or server). This allows the attacker to intercept and potentially modify or steal data intended for the legitimate device.

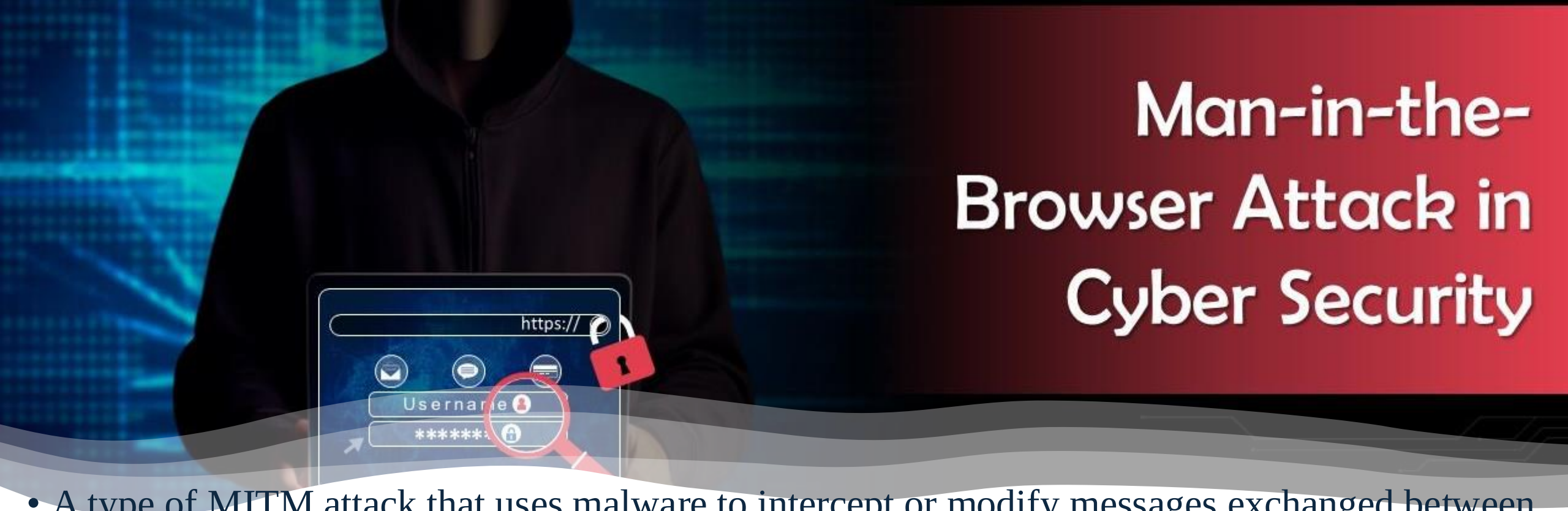
https://www.riskcrew.com/2021/01/how-to-mitigate-dns-hijacking/

https://www.strongdm.com/blog/man-in-the-middle-attack

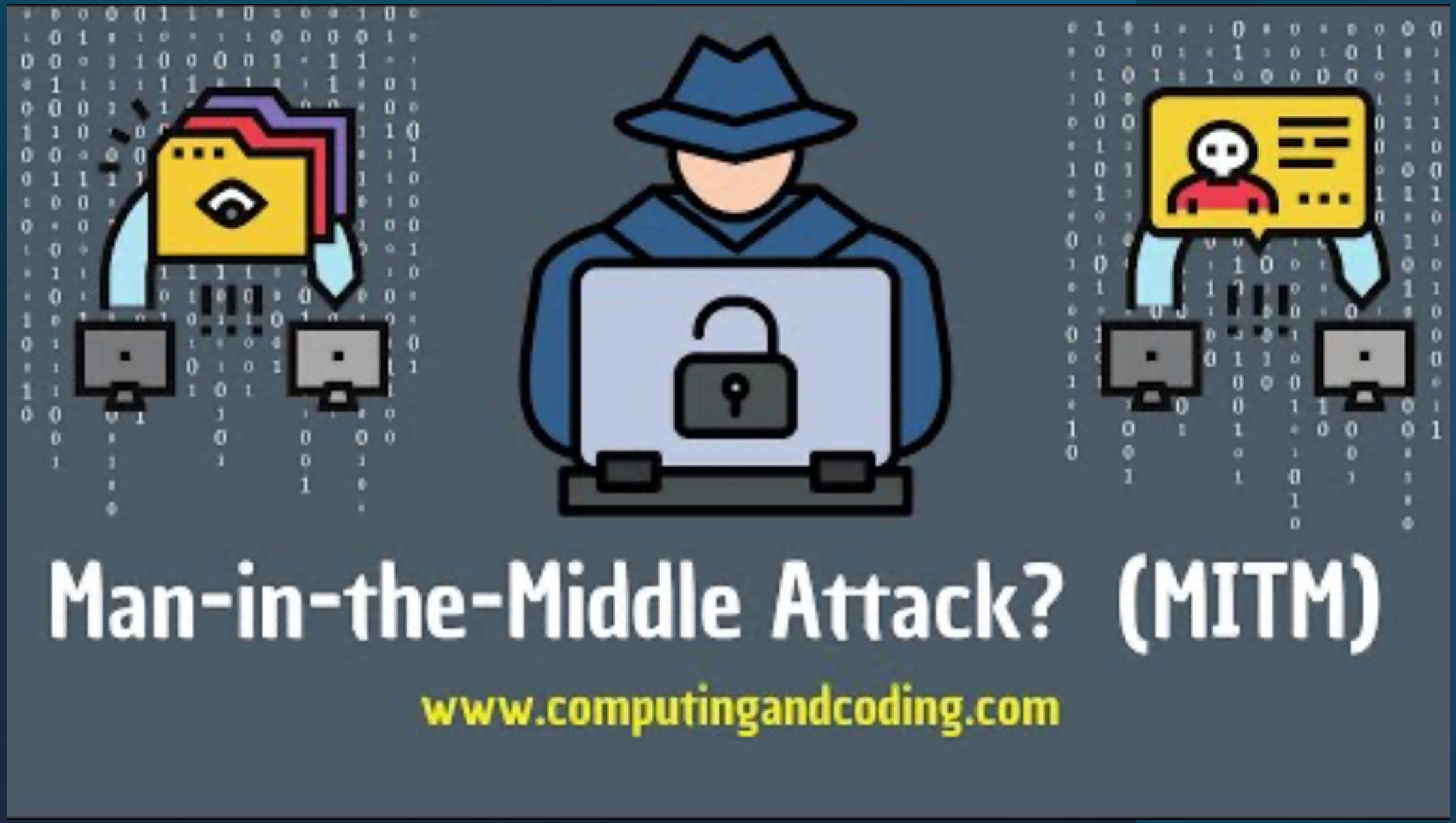
Man-In-The-Middle



- A threat actor is positioned in a communication pathway between two endpoints.
- The goal of the attack is to either eavesdrop on the conversation or impersonate one of the parties.
- A DNS poisoning attack that redirects a user to a malicious website by modifying the user's DNS query is a MITM attack.



- A type of MITM attack that uses malware to intercept or modify messages exchanged between a web browser and a web server. Often used in attacks on banking/shopping websites.
- A web browser vulnerability is exploited by a Trojan horse. The malware is an extension or plugin in the web browser. When a user enters the URL of a site, the extension checks to determine if this is one of the sites that was targeted for attack (steal credentials)
- MITB software resides exclusively within the web browser, making it difficult for standard anti-malware software to detect it. (What might defeat this attack?)


Man-in-the-Middle Attack? (MITM)
www.computingandcoding.com


ABC2 INVESTIGATORS
INSIDE A HACKER'S MIND
THE PRICE YOU COULD PAY FOR "FREE" HOTEL WI-FI
abc 2

The organization that Mike works in finds that one of their domains is directing traffic to a competitor's website. When Mike checks, the domain information has been changed, including the contact and other administrative details for the domain. If the domain had not expired, what has most likely occurred?

a. DNS spoofing

b. An on-path hijacking

c. Domain hijacking

d. A zero-day exploit

Network Protocols

- Established set of rules that determine how data is transmitted between different devices in the same network.
- Network protocols take large-scale processes and break them down into small, specific tasks or functions.
- Examples include **HTTP** for websites, **TCP/IP** for internet communication, and **Wi-Fi protocols** for wireless connections

Security Protocols

- Sets of rules that ensure data is **protected** when it's being transmitted over a network. They provide privacy, integrity, and safety by encrypting data and verifying the identity of users or devices.
- Encryption, Entity Authentication (verifies identity of user), Transportation (securely transmitted)
- Examples: HTTPS; SSL/TLS; IPsec

POPS, IMAPS, and S/MIME (Network Protocols)

POPS:

- SMTP – technical standard; mail delivery
- POP3 – mail retrieval, but not sending; downloads to device

IMAP

- IMAP4 – email retrieval, but not secure.
- Cross-platform

S/MIME

- MIME – internet standard; enhances SMTP
- S/MIME – standard for signing and encrypting data; provides CIA

SMTP vs POP3 vs IMAP: What is the difference?

mailtrap


KEYTOS
What Are
S/MIME
Certificates?

SSL/TLS, SSH, FTPS, and SFTP (Security Protocols)

SSL/TLS:

- Secure Socket Layer/Transport Layer Security;
- Provides authentication through cryptography

SSH

- Secure shell protocol uses cryptography to operate on an insecure network.

FTPS & SFTP

- FTPS – file transfer protocol using SSL/TLS.
- SFTP – uses SSH for file transfer on a network.

SSL/TLS

- **What it is**: SSL and its successor TLS are protocols used to **secure data** being transmitted over a network, usually between a browser and a web server.
- **What it does**: They **encrypt** the data to prevent it from being intercepted and understood by unauthorized parties.
- **Difference**: TLS is an updated, more secure version of SSL.
- **Example**: When you see a padlock in your browser’s address bar (like on a banking site), it means SSL/TLS is being used to secure the connection.

SSH (Secure Shell)

- **What it is**: SSH is a protocol for **securely accessing and managing remote servers** over an unsecured network.
- **What it does**: It encrypts commands and data sent between a user's computer and the server to prevent attackers from intercepting sensitive information (like passwords).
- **Difference**: Unlike SSL/TLS, which secures connections between browsers and servers, SSH is specifically used for secure remote login and system administration.
- **Example**: System administrators use SSH to securely log in to and manage remote servers.

FTPS (File Transfer Protocol Secure)

- **What it is**: FTPS is a **secure version of FTP**, the protocol used to transfer files over the internet.
- **What it does**: It adds SSL/TLS encryption to protect the data being transferred, ensuring that files can’t be intercepted or modified during transmission.
- **Difference**: While FTP sends data in cleartext (unsecured), FTPS secures the file transfers using SSL/TLS.
- **Example**: A company may use FTPS to securely transfer sensitive documents between a client and a server.

HTTPS

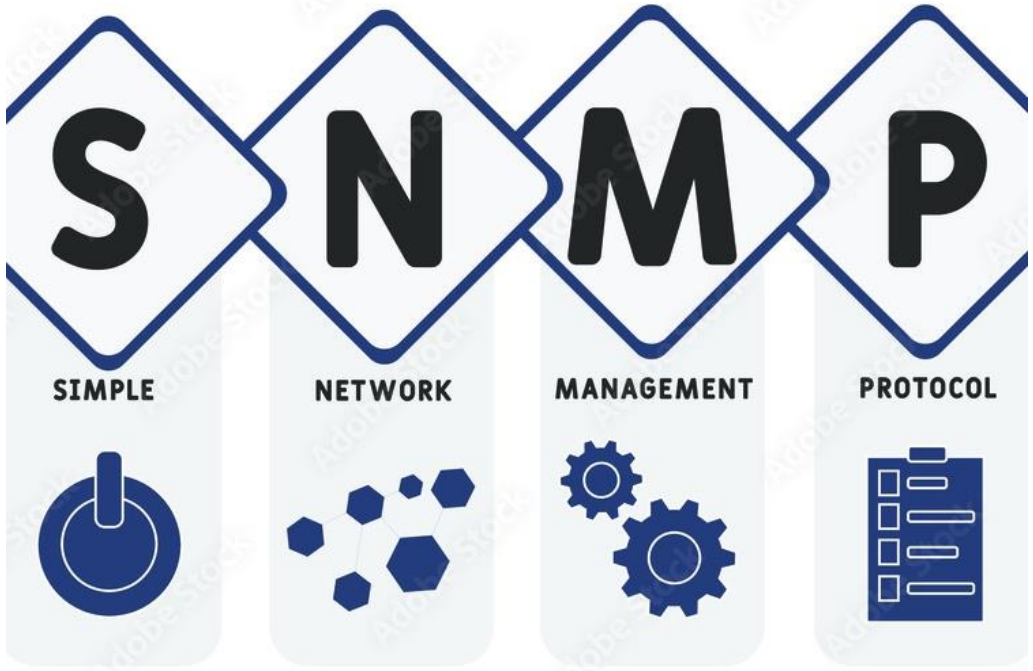
- Hypertext Transfer Protocol Secure, used to send and receive web pages
- Uses SSL/TLS to encrypt the data exchanged between a user’s browser and a website.
- Uses digital certificates. protecting things like login credentials, payment information, and personal data
- Protects against MITM and eavesdropping and tampering of data.

ttps://www.onelogin.com/blog/advanced-authentication-the-way-forward

SNMP helps different devices on a network—such as routers, switches, and servers—share information regardless of their hardware or software. It allows network administrators to monitor and manage these devices efficiently.

Key Components of SNMP:

1. **Managers (Servers)**: These are the central systems that gather, analyze, and control information from various devices on the network.
2. **Agents (Clients)**: These are the devices connected to the network—like computers, switches, printers, or phones—that provide the manager with data about their performance and status.



https://stock.adobe.com/images/snmp-simple-network-management-protocol-acronym-business-concept-background-vector-illustration-concept-with-keywords-and-icons-lettering-illustration-with-icons-for-web-banner-flyer-landing-p/476419386

Internet Protocol Security (IPSec)

IPSec is a set of protocols designed to secure data sent over an IP network, such as the internet. It ensures that data is authenticated, protected from tampering (integrity), and kept private (confidentiality). Key Components of IPSec:

- Authentication Header (AH):
  - What it does: AH ensures that the data sent has not been altered (integrity) and that it came from the correct sender (authentication). Protects against replay.
- Encapsulating Security Protocol (ESP):
  - What it does: ESP provides the same authentication and integrity protections as AH but also encrypts the data to ensure privacy (confidentiality).
  - How it works: Unlike AH, ESP only authenticates the IP payload (the data inside the packet) and not the IP header itself. It also protects against replay attacks.

https://www.enterprisenetworkingplanet.com/standards-protocols/what-is-tunneling/

Internet Protocol Modes

Transport Mode:

- **What it is**: In transport mode, only the **data (payload)** inside the IP packet is authenticated and encrypted, not the packet's header.
- **When it’s used**: This mode is commonly used for **end-to-end communications**, like between a client and a server or between two computers.

Tunnel Mode:

- **What it is**: In tunnel mode, the **entire IP packet** (both the header and the payload) is authenticated, encrypted, and then wrapped (or “encapsulated”) in a new IP packet.
- **When it’s used**: This mode is commonly used in **VPNs** (Virtual Private Networks), where secure communication between two networks is needed.

https://www.enterprisenetworkingplanet.com/standards-protocols/what-is-tunneling/


Professor Messer
Secure Protocols
©2022 Messer Studios LLC

Which of the following is the more recent and advanced electronic email system?

a. Simple Mail Transfer Protocol (SMTP)

 b. Internet Mail Access Protocol (IMAP)

c. Post Office Protocol (POP)

d. Transmission Control Protocol (TCP)

You are a security administrator for Acme Corporation. You have discovered malware on some of your company's machines. This malware seems to intercept calls from the web browser to libraries, and then manipulates the browser calls. What type of attack is this?

- [x] a. Man-in-the-browser
- [ ] b. On-path attack
- [ ] c. Man-in-the-middle
- [ ] d. Session hijacking

Prepare Media Article and Presentation

- Relevance to class topic (20%):
- Understanding of the issue (30%):
- Clear and organized summary (30%)
- Engagement with class (20%):
- IMPORTANT: Upload your article before the next class and provide a few sentences to answer each of the first three questions.

https://midas-pr.com/five-ways-get-public-speaking-opportunities-even-youre-new/