Survey Understanding Man-in-the-Middle (MITM) Attacks: Techniques, Tools, and Prevention in the Digital Era

Jawad Hussain[1], Irsa Talib[2]

[1]Riphah International University Lahore
[2]University of Management and Technology, Lahore

Correspondence:
Jawad Hussain: jawad.hussain@riphah.edu.pk

Article Link: https://www.brainetwork.org/index.php/jcai/article/view/14

DOI: https://doi.org/10.69591/jcai.1.2.5

Citation: Hussain, J. & Talib, I., (2023). Survey Understanding Man-in-the-Middle (MITM) Attacks: Techniques, Tools, and Prevention in the Digital Era, *Journal of Computing and Artificial Intelligence*, *1*(2), 60-71.

Conflict of Interest: Authors declared no Conflict of Interest

Acknowledgment: No administrative and technical support was taken for this research

Article History

Submitted: Sep 02, 2023
Last Revised: Oct 11, 2023
Accepted: Nov 28, 2023

Volume 1, Issue 2, 2023

Funding
No

An official Publication of
Beyond Research Advancement & Innovation Network, Islamabad, Pakistan

Survey Understanding Man-in-the-Middle (MITM) Attacks: Techniques, Tools, and Prevention in the Digital Era

Jawad Hussain[1*], Irsa Talib[2]

[1]Riphah International University Lahore

[2]University of Management and Technology, Lahore

Abstract

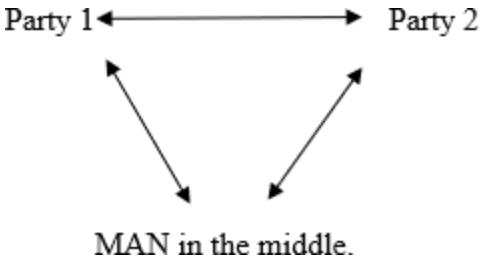
Cyber threats are increasing day by day as internet is becoming more and more popular. In current digital era, online use of banking transactions and other e-commerce activities open the door of online theft. Different types of cyber-attacks being launched keeping in mind the current digital scenario. A man in the middle attack (MITM) is the most widely held attack. MITM attack is the type of attack in which communication between two parties are interrupted either on LAN or internet without knowledge of both parties. In this survey paper, basic understanding of MITM attack and types have been discussed after reading most of the research of some past years. Introduction regarding tools for execution of MitM attack is also the part of this survey paper. Basic inspiration to write this paper is to present MITM topic in such a way that would be helpful for readers to understand and to familiarize the topic.

Keywords: man in the middle attack, mitm attack, cyber-attacks, cyber security, common attacks, cyber Threats

Introduction

A man-in-the-middle attack (MitM) is a cyber-attack where an attacker positions themselves between the communications of two parties without their knowledge [1]. This attack involves three players: the victim, the entity the victim is communicating with, and the "man in the middle" who intercepts the victim's communication. Crucially, the victim is unaware of the presence of the intermediary, allowing the attacker to eavesdrop on the communication undetected [2].

* Corresponding Author: jawad.hussain@riphah.edu.pk



MitM attacks can be classified into two categories: those aimed at reading the contents of a message, which is known as a confidentiality attack, and those aimed at altering the message or modifying communication, known as an integrity attack [3]. These attacks can take two forms: physical proximity to the target or the use of malicious software or malware [4].

The primary objective of a MitM attack is to steal information such as login credentials, debit/credit card details, or sensitive data, or to modify information for malicious purposes. Cybercriminals typically execute MitM attacks in two phases: interception and decryption [5]. Interception involves capturing encrypted data, while decryption involves decrypting this data to read and manipulate it [6].

Various techniques are employed in MitM attacks, including IP Spoofing, ARP Spoofing, DNS Spoofing, HTTPs spoofing, and SSL hijacking. These attacks often target communication layers such as the OSI and GSM networks, exploiting vulnerabilities in these channels for unauthorized access and data manipulation. [7].

Table 1

OSI Layers	Data Link	ARP Spoofing
	Presentation	SSL Decryption
	Transport and Network	IP Spoofing
	Application	DHCP Spoofing, DNS Spoofing
Cellular networks	GSM UTMS	FBS Type

Types of MitM

A. IP Spoofing

It's a type of attack in which attacker changes the IP header's source (false source IP address) to hide the identity of request sender. This type of spoofing is done for different malicious activities without detection [8].

B. ARP Spoofing

ARP spoofing uses disadvantage of ARP (Address Resolution Protocol) protocol i.e. its stateless nature. ARP protocol is used to map IP address with MAC address. ARP protocol uses its ARP cache to store this mapping. When a device wants to send message to other device, it checks its ARP cache either mac address against device IP exists or not. If MAC address exists, message sends otherwise a broadcast message is sent to all devices. All network devices check their MAC address [10]. If it does not match, message is discard. If MAC address matches, that device sends a response message to sending device that contains MAC address. In such way both devices update their ARP cache. Now these ARP messages and replies can be spoofed and there is not record maintain of ARP messages [11]. ARP Spoofing or ARP cache poisoning is a technique that forges fake ARP request or ARP reply. ARP Spoofing is a type of malicious attack in which linkage of an attacker's MAC address with the IP of target computer or server is done by sending incorrect ARP messages. With the help of ARP spoofing, an attacker disrupts data frames, modify these frames, modify network traffic or stops the traffic [12].

C. DNS Spoofing

DNS Spoofing also referred to as DNS cache poisoning. It is the act of entering false information into a DNS cache so that DNS queries return an incorrect response and users are directed to wrong websites [13].

D. Session Hijacking

A session hijacking attack occurs when an attacker gains control of your internet session while you're engaged in activities like checking your credit card balance, paying bills, or shopping online. Typically, session hijackers focus on browser or web application sessions, exploiting vulnerabilities to seize control of your ongoing online activities [14].

Research Methodology

This research material is collected for survey after evaluating the best research papers.

A. Research Objectives (RO)

The foremost goals of this study are:

RO1: Initial focus of this research is to collect understandable data about man in the middle attack and its types from different sources

RO2: How to prevent from different MitM attacks

RO3: Overview of tools used for execution of MitM attacks

B. Search Scheme

In any survey, a search plan is prepared which requires description of a search string as a main part [15].

Table 2

Search string INCLUSION and exclusion criteria

Sources	Search String	Context
IEEE Xplore, Science Direct, Springer Link, MDPI, and IGI Global	(“Cyber Security Threats” OR “Cyber Security Attacks” OR “Cyber Threats”) AND (Man in the middle attack” OR “MITM” OR “MITM attacks”) AND (“Spoofing attacks” OR “ARP spoofing” OR “IP spoofing” OR “DNS spoofing” OR “Session Hijacking”)	Security Attack

Inclusion criteria parameters

1) All papers published in Conference and Journals are included
2) All published papers included among 2012 to 2022
3) Any paper targeting to MitM attacks, ARP OR ARP Spoofing attack, DNS spoofing attacks, session hijacking etc

Exclusion criteria parameters

1) Papers published before 2012
2) Papers not written in readable format and language

MitM Prevention Techniques

A. IP Spoofing

It is very difficult to end users to detect IP spoofing. However different network monitoring tools are used to detect while detecting packet filters [13]. Some common techniques are mentioned in Table 1&2.

B. ARP Spoofing

Following different techniques are used to mitigate ARP spoofing attack. These techniques are found in different research papers. Some common techniques are mentioned in Table 1&2.

1) Stateful ARP cache and a fuzzy logic controller technique introduced by Zouhier Trabelsi et al. [2]. Similar proposal from Tripunitara et al. [3]. came in which requests and replies of ARP are maintained in separate queues.
2) S-ARP (Secure Address Resolution Protocol) technique in which each host has a public and private key pair distribution by AKD (Authoritative Key Distributor) introduced by D.Bruschi et al. [4]. To mitigate ARP Spoofing, all the messages are digitally signed by sender.
3) One Man in the middle attack solution proposed by G N Nayak and S Samaddar [6]. More than one entries against same IP and MAC address are removed from ARP table by using another secondary cache.
4) G Jinhua and Keijian introduced new scheme for ARP spoofing attack detection by using ICMP protocol [5]. This new scheme is an algorithm that uses ICMP protocol to detect malicious packets. These malicious packets perform spoofing attacks send by an attacker. The algorithm collects these ARP packets for analyzing its nature. After analysis, this algorithm replies ICMP echo request packet to check host is malicious or not according to its response packet [16].

C. DNS SPOOFING

Domain Name System Security Extensions (DNSSEC) verifies data integrity and origin. Actual DNS not capable of doing this. DNSSEC adds a cryptographic signature to the entries [17].

D. SESSION HIJACKING

Use VPN for mitigation of session hijacking. Some common techniques to avoid also this type of attack is mentioned in Table 1&2.

Table 3

Common MitM Prevention Techniques

1	Avoid Public wifi or all other wifis that are not password protected
2	Install reputable security software on your devices and make sure to update it on regular intervals
3	Avoid clicking on any malicious link about which you are not sure to be safe. Session hijackers may send emails that contain different links to click
4	Be ware of site security. Reputable institutions, companies and banks properly monitor their websites security
5	Avoid to browse / download data from non secure website i.e. Use only https website.
6	Immediately logging out of a protected applications specially banking/emails etc when it's not in use
7	Not use open sysems like cafes,lodgings when conducting sensitive financial exchanges.
8	Using SSL encryption to establish a secure connection channel.
9	For Site administrator, includes TLS, HTTPS schemes, antivirus frameworks furnishes its clients with a streamlined end-to-end SSL/TSL encryption as component of its suite of security administrations.

Tools for Launching MitM Attacks

Ettercap

It is very comprehensive tool for packet sniffing and ARP cache poisoning. It can perform different functions including MAC and IP based

sniffing, launches DoS attack, intercepts and modifies packets, decrypts passwords etc. It is also used to capture passwords and other personal sensitive information. Ettercap has a good GUI interface with command line interface also. Emulation of Man in The Middle Attack, credentials capturing, ARP Spoofing, DNS spoofing and DoS attack possible with the help of Ettercap**.** Ettercap is available with Linux and Unix-variant operating systems such as RHEL, CentOS, Ubuntu, Kali, Debian, Fedora, NetBSD and Solaris etc [18].

Dnsniff

Dsniff tool is also used for network traffic and analysis with strong penetration testing. This tool monitors a network for accessing credentials such as passwords, emails, files etc. arp spoofing, dns spoofing and mac spoofing let the attacker sniff through the network traffic with out knowledge of the user about it [19].

Ssstrip

In this scenario, the attacker compels a victim's browser to communicate with them in plaintext over HTTP, intercepting and altering the content from HTTPS servers. This is achieved through a process known as SSL stripping, where the attacker modifies HTTPS URLs to HTTP URLs, allowing them to intercept and manipulate the victim's communications. [20].

Mitmproxy

It's an interactive console tool designed for analyzing and reconfiguring user HTTP traffic [21]. What sets it apart from mitmdump is its capability to retain the flow of HTTP traffic in memory for sample testing [22,23].

Table 4

MitM Types and Their Defenses (Summary)

Type	Defenses
ARP Spoofing	Secured LAN
	Static ARP Cache
	Third Party ARP traffic monitoring System
DNS Spoofing	Secured LAN
	IDS/IPS
	DNSSEC (Domain Name System Security Extensions)
Session Hijacking	SSL encryption of secure a connection channel
	Logout functionality for session termination
	Passing authenticated cookies over a secure HTTPS connection
	Regeneration session IDs for every successful login

Conclusion

This survey paper presented a discussion of MitM attacks, its types and different techniques through which we can save ourself from different MitM attacks. Although complete saving from MitM attack is not possible however our discussed points will help to minimize the threat of such attacks.

References

[1] J. Singh, S. Dhariwal, and R. Kumar, "A detailed survey of ARP poisoning detection and mitigation techniques," *Int. J. Comput. Technol. Appl.*, vol. 9, no. 41, pp. 131–137, 2016.

[2] Z. Trabelsi and W. El-Hajj, "Preventing ARP attacks using a fuzzy-based stateful ARP cache," in *2007 IEEE international conference on communications*, IEEE, 2007, pp. 1355–1360. Available: https://ieeexplore.ieee.org/abstract/document/4288899/

[3] M. V. Tripunitara and P. Dutta, "A middleware approach to asynchronous and backward compatible detection and prevention of ARP cache poisoning," in *Proceedings 15th Annual Computer Security Applications Conference (ACSAC'99)*, IEEE, 1999, pp. 303–309. Available: https://ieeexplore.ieee.org/abstract/document/816040/

[4] D. Bruschi, A. Ornaghi, and E. Rosti, "S-ARP: a secure address resolution protocol," in *19th Annual Computer Security Applications Conference, 2003. Proceedings.*, IEEE, 2003, pp. 66–74. Available: https://ieeexplore.ieee.org/abstract/document/1254311/

[5] G. Jinhua and X. Kejian, "ARP spoofing detection algorithm using ICMP protocol," in *2013 international conference on computer communication and informatics*, IEEE, 2013, pp. 1–6. Available: https://ieeexplore.ieee.org/abstract/document/6466290/

[6] G. Nath Nayak and S. Ghosh Samaddar, "Different flavours of Man-In-The-Middle attack, consequences and feasible solutions," in *2010 3rd International Conference on Computer Science and Information Technology*, Jul. 2010, pp. 491–495. doi: 10.1109/ICCSIT.2010.5563900.

[7] M. Data, "The defense against arp spoofing attack using semi-static arp cache table," in *2018 International conference on sustainable information engineering and technology (SIET)*, IEEE, 2018, pp. 206–210. Available: https://ieeexplore.ieee.org/abstract/document/8693155/

[8] P. Arote and K. V. Arya, "Detection and prevention against ARP poisoning attack using modified ICMP and voting," in *2015 International conference on computational intelligence and networks*, IEEE, 2015, pp. 136–141. Available: https://ieeexplore.ieee.org/abstract/document/7053817/

[9] V. Rohatgi and S. Goyal, "A detailed survey for detection and mitigation techniques against ARP spoofing," in *2020 fourth international conference on I-SMAC (IoT in social, mobile, analytics and cloud)(I-SMAC)*, IEEE, 2020, pp. 352–356. Available: https://ieeexplore.ieee.org/abstract/document/9243604/

[10] D. Srinath, S. Panimalar, A. J. Simla, and J. Deepa, "Detection and Prevention of ARP spoofing using Centralized Server," *Int. J.*

Comput. Appl., vol. 113, no. 19, 2015, Available: https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=b188cbb71682c863ab44f216360bac84cb15bcf9

[11] M. N. Ahmed and M. Hussain, "A Study and Model to protect Sophisticated Eurograbber attack," *Int. J. Grid Distrib. Comput.*, vol. 9, no. 6, pp. 63–70, 2016.

[12] D. Raviya Rupal, D. Satasiya, and M. H. Kumar, "A comprehensive survey of ARP Poisoning Remedies". Available: https://www.researchgate.net/profile/Rupal-Raviya/publication/303588133_A_comprehensive_survey_of_ARP_Poisoning_Remedies/links/57495f5608ae5f7899b9e38d/A-comprehensive-survey-of-ARP-Poisoning-Remedies.pdf

[13] A. Mallik, "Man-in-the-middle-attack: Understanding in simple words," *Cyberspace J. Pendidik. Teknol. Inf.*, vol. 2, no. 2, pp. 109–134, 2019.

[14] M. Conti, N. Dragoni, and V. Lesyk, "A survey of man in the middle attacks," *IEEE Commun. Surv. Tutor.*, vol. 18, no. 3, pp. 2027–2051, 2016.

[15] http://www.thoughtcrime.org/software/sslstrip

[16] https://mitmproxy.org

[17] https://www.cloudflare.com/learning/dns/dns-cache-poisoning/

[18] R. Petrović, D. Simić, S. Stanković, and M. Perić, "Man-In-The-Middle Attack Based on ARP Spoofing in IoT Educational Platform," in 2021 15th International Conference on Advanced Technologies, Systems and Services in Telecommunications (TELSIKS), Oct. 2021, pp. 307–310. doi: 10.1109/TELSIKS52058.2021.9606392.

[19] U. O. Obonna et al., "Detection of Man-in-the-Middle (MitM) Cyber-Attacks in Oil and Gas Process Control Networks Using Machine Learning Algorithms," Future Internet, vol. 15, no. 8, Art. no. 8, Aug. 2023, doi: 10.3390/fi15080280.

[20] R. Goenka, M. Chawla, and N. Tiwari, "A comprehensive survey of phishing: mediums, intended targets, attack and defence techniques and a novel taxonomy," Int. J. Inf. Secur., vol. 23, no. 2, pp. 819–848, Apr. 2024, doi: 10.1007/s10207-023-00768-x.

[21] I. Alodat, "Protection of Nurse-Sys Platform from Man-In the Middle Attacks," in 12th International Conference on Information

Systems and Advanced Technologies “ICISAT 2022,” M. R. Laouar, V. E. Balas, B. Lejdel, S. Eom, and M. A. Boudia, Eds., Cham: Springer International Publishing, 2023, pp. 146–155. doi: 10.1007/978-3-031-25344-7_14.

[22] O. Pospisil, R. Fujdiak, K. Mikhaylov, H. Ruotsalainen, and J. Misurec, “Testbed for LoRaWAN Security: Design and Validation through Man-in-the-Middle Attacks Study,” Appl. Sci., vol. 11, no. 16, Art. no. 16, Jan. 2021, doi: 10.3390/app11167642.

[23] M. B. Muzammil, M. Bilal, S. Ajmal, S. C. Shongwe, and Y. Y. Ghadi, “Unveiling Vulnerabilities of Web Attacks Considering Man in the Middle Attack and Session Hijacking,” IEEE Access, vol. 12, pp. 6365–6375, 2024, doi: 10.1109/ACCESS.2024.3350444.