Indonesian Journal of Computing, Engineering, and Design

Journal homepage: http://ojs.sampoernauniversity.ac.id/index.php/IJOCED

Understanding Man-in-the-middle-attack through Survey of Literature

A. Mallik[1,], A. Ahsan[2], M. M. Z. Shahadat[1] & J. C. Tsou[3]*

[1] Dept of Mechanical Engineering, RUET, Rajshahi-6204, Bangladesh

[2] Dept of Computer Science and Engineering, RUET, Rajshahi-6204, Bangladesh

[3] Dept of Business Administration, China University of Technology, Taipei City, Taiwan

Correspondence: E-mail: avijitme13@gmail.com

ABSTRACT

These days cyberattack is a serious criminal offense and it is a hotly debated issue moreover. A man-in-the-middle-attack (MITM) is a kind of cyberattack where an unapproved outsider enters into an online correspondence between two users, remains escaped the two parties. The malware that is in the middle-attack often monitors and changes individual/classified information that was just realized by the two users. A man-in-the-middle-attack as a protocol is subjected to an outsider inside the system, which can access, read and change secret information without keeping any tress of manipulation. This issue is intense, and most of the cryptographic systems without having a decent authentication security are threatened to be hacked by the malware named MITM. This paper essentially includes the view of understanding the term of MITM; the current work is mainly emphasized to accumulate related data/information in a single article so that it can be a reference to conduct research further on this topic at college/undergraduate level. This paper likewise audits most cited research and survey articles on MITM recorded on 'Google Scholar'. The result showed that the MITM has correlation to the user behavior, in which this must be considered and careful understood for the way how to solve this problem. The motivation behind this paper is to help the readers for understanding and familiarizing the topic 'man-in-the-middle attack'.

ARTICLE INFO

Article History:
Received 7 Nov 2018
Revised 27 Feb 2019
Accepted 5 Mar 2019
Available online 21 April 2019

Keywords:
Men-In-The-Middle,
Cryptography,
Internet Security,
Wireless Communication,
Malware.

1. INTRODUCTION

In cryptography and PC security, a man-in-the-middle attack (MITM) is an attack where the attacker furtively transfers and perhaps changes the correspondence between two parties who trust they are straightforwardly communicating with each other. A man in the middle (MITM) attack is a general term for when a culprit positions himself in a discussion between a client and an application; either to listen stealthily or to imitate one of the parties, making it show up as though an ordinary trade of information is in progress (Meyer & Wetzel, 2004). The objective of an attack is to take individual information, for example, login certifications, account points of interest and charge card numbers. Targets are normally the clients of financial applications, system in businesses, web-based business locales, and other sites where logging in is required. Information obtained during an attack could be utilized for many, purposes, including fraud, unapproved support exchanges or an unlawful watchword change. Furthermore, it can be utilized to gain a decent footing inside an anchored edge during the infiltration phase of an Advanced Persistent Threat (APT) strike.

Figure 1 portrays a schematic of MITM belief system. A MITM allows a malicious actor to intercept, send and receive data meant for someone else, or not meant to be sent at all, without either outside party knowing until it is too late (Conti et al., 2016).

One case of man-in-the-middle attacks is dynamic eavesdropping, in which the attacker makes independent associations with the victims and transfers messages between them to influence them to trust they are talking straightforwardly to each other over a private association when in certainty the whole discussion is controlled by the attacker. The attacker must have the capacity to intercept every single significant message passing between the two casualties and inject new ones. This is direct in many conditions; for instance, an attacker within gathering scope of an unencrypted wireless access point (Wi-Fi) could insert himself as a man-in-the-middle .

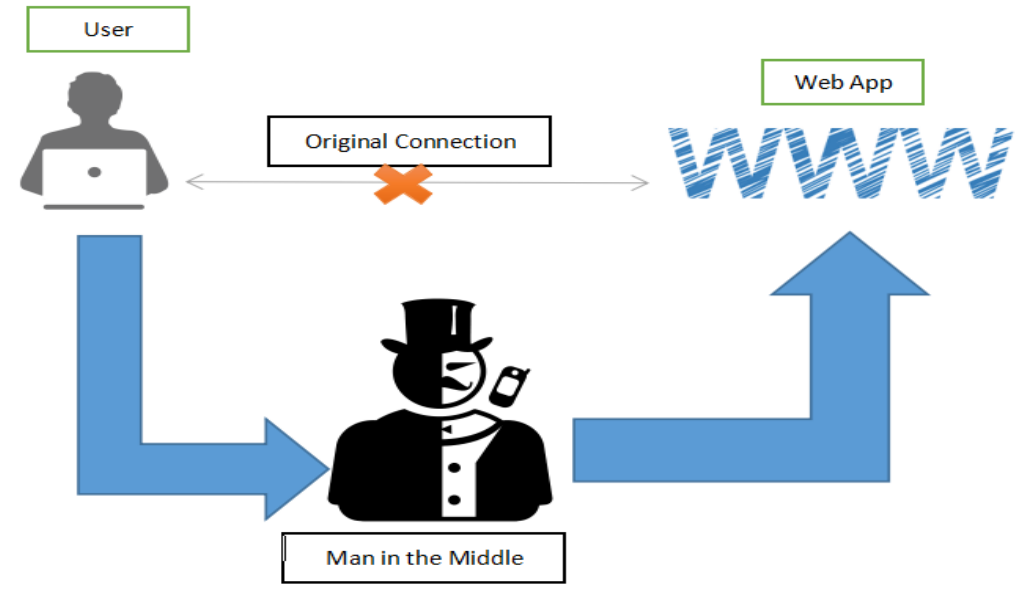

Figure 1. Men-in-the-middle attack ideology schematic.

As an attack that goes for circumventing common authentication, or scarcity in that department, a man-in-the-middle attack can succeed just when the attacker can mimic every endpoint agreeable to them not surprisingly from the genuine closures. Comprehensively speaking, a MITM attack is what might as well be called a mailman opening your bank proclamation, writing down your record points of interest and after that resealing the envelope and delivering it to your entryway. Most cryptographic conventions include some type of endpoint authentication particularly to persist MITM attacks. For instance, TLS can authenticate one or the two parties using a commonly confided in endorsement expert (Rahim, 2017).

2. METHODOLOGY

This study has been done by making surveys on several references for literature review especially in evaluating the most citation research papers. The surveys have been conducted from January to August 2018.

3. RESULTS AND DISCUSSION

3.1. Literature Survey

MITM is named for a ball game where two people play catch while a third person in the middle attempts to intercept the ball. MITM is also known as a fire brigade attack, a term derived from the emergency process of passing water buckets to put out a fire. Some researchers on 2004 (Meyer & Wetzel, 2004) presented a report on Universal Mobile Telecommunication System's (UITM) security protocol where they discussed about 'men-in-the-middle-attack' on mobile communication. Recently, some reports have been more developed (Saif et al., 2018), in which the developing method was made similar type of researches on updated version of Bluetooth networks security and discussed about new techniques to prevent MITM in two party's communication. Other developed reports (Sounthiraraj et al., 2014) conducted researches about HTTP security and those researches found MITM as a very serious threat and those also discussed the prevention techniques. A survey on MITM and its effects on the economy has also become one of the crucial issues (Conti et al., 2016). Indeed, this condition makes some researchers (Statica et al., 2017) to have a prevention of MITM mainly for Internet communication and those papers discuss several unique and effective measures on prevention of MITM from on-net communication. Other reports also showed their review reports on MITM, which mostly discusses about WLAN security for 2-way communication.

3.2. Progress of MITM

Effective MITM execution has two distinct stages: interception and decryption. The stages involve physical closeness to the intended target, and another that exclusive involves malware, known as a man-in-the-browser (MITB) attack. With a conventional MITM attack, the attacker needs access to an unsecured, or ineffectively anchored Wi-Fi switch (Sun et al., 2018). These sorts of associations are by and large found out in the open territories with free Wi-Fi hotspots, and even in a few people's homes. An attacker will check the switch using code looking for particular shortcomings, for example, default or poor secret key utilize, or security gaps because of the poor arrangement of the switch. Once the attacker has discovered the powerlessness, they will then insert their instruments in the middle of the clients' PC and the sites the client visits. A fresher variation of this attack has been gaining fame with cybercriminals because of its simplicity of execution. With a man-in-the-browser attack, every one of an attacker needs are an approach to inject malware into the PC, which will then install itself into the browser without the clients' learning and will then record the information that is being sent between the victim and particular focused on sites, for example, financial institutions, that are coded into the malware. Once the malware has gathered the particular information it was modified to gather, it then

transmits that information back to the attacker.

3.2.1. Interception

The initial step intercepts client activity through the attacker's system before it achieves its intended destination. The most well known (and easiest) method for doing this is an inactive attack in which an attacker makes free/open WiFi hotspots; accessible to general society. Commonly named in a way that relates to their area, they aren't watchword secured. Once a casualty interfaces with such a hotspot, the attacker gains full permeability to any online information trade. Attackers wishing to adopt a more dynamic strategy to interception may dispatch one of the following attacks:

- IP spoofing involves an attacker disguising himself as an application by altering parcel headers in an IP address. Accordingly, clients attempting to get to a 'url' associated with the application are sent to the attacker's site.
- ARP spoofing is the way toward linking an attacker's mac address with the IP address of a legitimate user on a local area network using fake ARP messages. Subsequently, information sent by the client to the host IP deliver is instead transmitted to the attacker.
- DNS spoofing, otherwise called DNS store poisoning, involves infiltrating a DNS server and altering a site's address record. Accordingly, clients attempting to get to the site are sent by the adjusted DNS record to the attacker's site.

3.2.2. Decryption

After an interception, any two-way SSL movement should be unscrambled without alerting the client or application. Various strategies exist to accomplish this:

- HTTPS spoofing sends an imposter endorsement to the victim's browser once the initial association demand for a safe site is made. It holds an advanced thumbprint related with the bargained application, which the browser confirms according to an existing rundown of confided in destinations. The attacker is then ready to get to any information entered by the casualty before it's passed to the application.
- SSL BEAST (browser abuse against SSL/TLS) focuses on a TLS variant 1.0 helplessness in SSL. Here, the casualty's PC is infected with pernicious JavaScript that intercepts scrambled treats sent by a web application. Then the application's Figure square chaining (CBC) is endangered in order to decode its treats and authentication tokens.
- SSL hijacking happens when an attacker passes produced authentication keys to both the client and application during a TCP handshake. This sets up what seems, by all accounts, to be a safe association when, actually, the man in the middle controls the whole session.
- SSL stripping minimizes an HTTPS association with HTTP by intercepting the TLS authentication sent from the application to the client. The attacker sends a decoded form of the application's site to the client while maintaining the anchored session with the application. In the meantime, the client's whole session is noticeable to the attacker (Valluri, 2018).

3.3. Definition MITM based on survey

MITM is a type of cryptographic attack over a communication channel by a malicious third party where he/she takes over a confidential/personal communication channel between two or legitimate communicative points or parties. In this cyberattack, the attacker can control (read, modify, intercept, change or replace) the communication traffic between victims. But by using MITM protocol the unauthenticated attacker leaves no clues/traces of his interception of this cybercrime, in short words the attacker remains invisible to the victims.

Table 1. MITM attacks on different communication channels (Dutta AK, 2018)

		MITM Types
OSI Layers	Data Links	ARP spoofing type
	Presentation	SSL decryption, CA decryption
	Transport and Networking	IP spoofing
	Applications	DHCP spoofing, BGP type, DNS spoofing
Cellular Networks	GSM	
	UMTS	FBS type

It needs a communication channel to make a MITM attack. The most used communication channels of MITM attack are namely GSM, UMTS, Long-Term Evolution (LTE), Bluetooth, Near Field Communication (NFC), Radio Frequency and Wi-Fi. The first recorded MITM attack was planned in the time of WW-II for intercepting German Military's radio communication and was done by the Royal British Intelligence (also known as MI-6) (Kozaczuk & Kozaczuk, 1984). In normal sense, there are three most possible compromises, namely Confidentiality, Integrity, and Availability; which are aimed at my MITM attack. Most of the MITM attacks now days are done in social media, because of the extensive use of human communication are done using social media (Facebook, Twitter, Yahoo Messenger and etc. (Hudaib, 2014). Decoding a MITM attack is a long process, basically this is done using three ways, namely 1) Based on impersonation methods of cyber decoding, 2) Based on Telecommunication addressing techniques and lastly 3) Based on GPS locating method of attacker and victims both (Dutta, 2018).

3.4. Present Status of MITM

Nowadays, most of the MITM attacks are performed using communication layers. Open System Intercommunication (OSI) and GSM networks are the most affected communication channels by MITM attacks. **Table 1** shows types of MITM attacks on different OSI and Cellular service networks (Dutta, 2018).

In **Table 1**, MITM attacks across OSI layers and cellular networks have been listed. Each layer enforces different approaches to provide security. Nevertheless, none of them is free from hacking attacks. (Ornaghi & Valleri, 2003) was the first to present a security system-based tracking location of the attacker and victim. He classified MITM attacks in three distinct categories: a) LAN (Local Area Network) tracking, b) LAN to Remote Network tracking and c) Remote Network track. The authors also take into consideration that STP mangling is a closed type of MITM as the attacker can only manage to decode the unmanaged traffic between two clients.

3.4.1. Spoofing: Most Common Mitm

Spoofing an impersonation technique, which is originated from 'spying'. In the middle century, European spies used to hear secret conversation by impersonating him/her to the communicative party. The same method is applied in modern cryptographic spoofing, as the attacker intercepts a confidential/personal communication between two hosts and controls over transferring data, while the hosts are not being aware of the unauthenticated attacker. Some research papers from reference (Schuckers, 2002) describe spoofing as the first step of executing MITM, not being the total of a MITM attack; while some other deliciated research papers claim spoofing as a whole MITM process.

In this paper, we will consider it as a spoofing based MITM or spoofing attack. When a

party wants to communicate with other parties over a cryptographic network then if their network is same with an unknown MAC address then the server broadcasts an address resolution protocol (ARP) request to all hosts under the same network connection. Only the specified client with announced IP (Internet Protocol) is expected to make a reply including his/her MAC (Media Access Control) address. However, having a dynamic ARP caching, cache entries can be easily managed by ARP messages, though this system does not contain proper identification and authentication service (Oh et al., 2012). In the meantime, the system saves the IP to MAC entry in its local/temporary cache, so the next time; communication can be boosted up, by avoiding any trouble.

Address Resolution Protocol has no states thus it provides very few securities to the caching system. Some top-notch researches referring from (Demuth & Leitner, 2005) shows the state-of-art (SoA) of using those security weaknesses for conducting a perfect MITM attack. Suppose, there are three networks: the attacker 'X' (IP = 10.0.x.x3, MAC = AA:AA:AA:AA:AA:X3), the first victim 'A' (IP = 10.0.x.x1, MAC = VV:VV:VV:VV:VV:X1), and the second victim 'B' (IP = 10.0.x.x2, MAC = VV:VV:VV:VV:VV:X2). The next steps for a perfect spoofing based on ARP are shown below:

1) 'X' sends an ARP Reply message to 'A', which says that IP: 10.0.x.x3 has MAC address: AA:AA:AA:AA:AA:X3. This message will update 'A''s ARP Table.
2) 'X' also sends an ARP Reply message to 'B', which says that IP: 10.0.x.x2 has MAC address: AA:AA:AA:AA:AA:X3. This message will update 'B''s ARP Table.
3) When 'A' wants to send a message to 'B', it will go to 'X''s MAC address AA:AA:AA:AA:AA:X3, instead of 'B''s VV:VV:VV:VV:VV:X2.
4) When 'B' wants to send a message to 'A', it will also go to 'X'. Schematic regarding the example stated above is given in **Figure 2**.

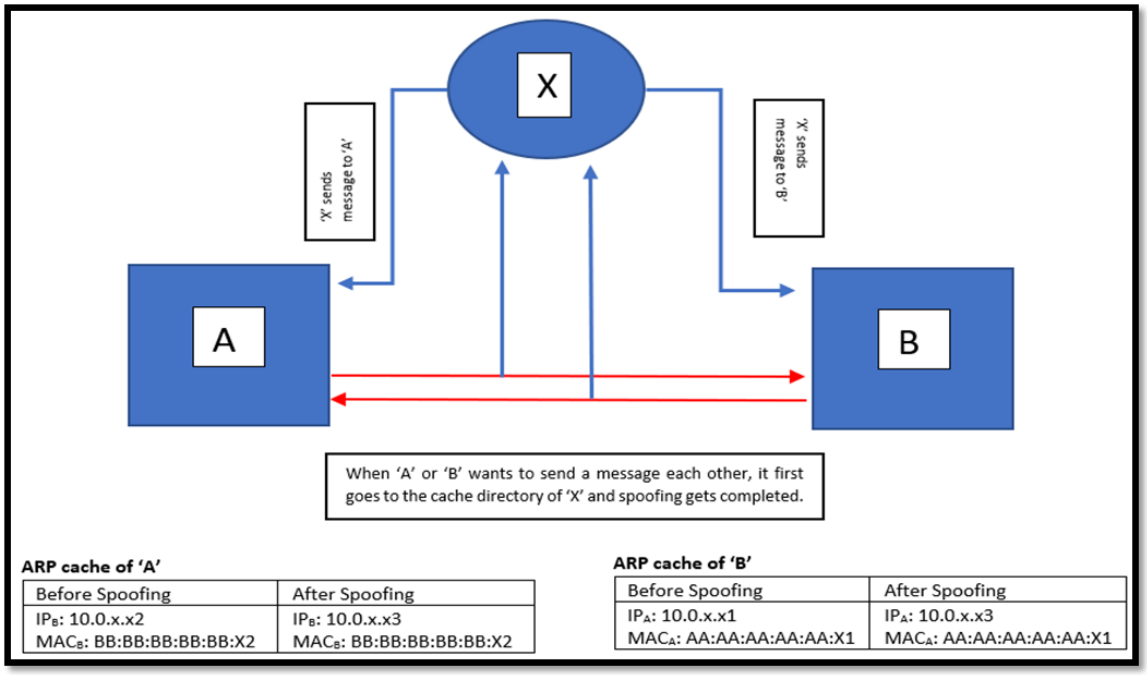

Figure 2. Spoofing method between two clients.

There are many well-researched works of literature where spoofing defending system is discussed (Philip, 2007). They introduced various well-researched techniques to prevent spoofing and make secure communication over LAN. But those Literatures doesn't concern about wireless methods of communications. **Table 2** shows a typical comparison between spoofing prevention techniques.

3.5. MITM on GSM: A Threat to Phone Communication Security

In the early 90's, the European Telecommunications Standards Institute introduced GSM as a second generation (2G) telecommunication standard. There are two basic types of services offered through GSM: telephony and data bearer. The GSM architecture consists of Mobile Stations (MSs) and Base Terminal Stations (BTS), which communicate with each other through radio links. Each BTS connects to the Base Station Controller (BSC). BSC links to the Mobile Switching Center (MSC), which is responsible for routing signals to and from fixed networks (Su et al., 2018). Home Location Register (HLR) and the Visitor Location Register (VLR) are the two major databases for each mobile service provider in the GSM architecture.

Figure 3 shows a schematic of GSM architecture. Each of GSM subscribers has the secret password, which is stored in the Subscriber Identity Module (SIM) card of the MS. The Authentication Center (AUC) has a secret key, which is shared with the subscriber and AUC. AUC generates a set of security parameters for execution of encryption and authentication.

Table 2. Comparison of various types of spoofing prevention technologies.

Medium of Communication	Protocol	Concerns
Server Based Communication	ARP	Can't work for wireless communications.
Server Based/ Host Based	ARP, DHCP	Compatible for DoS, DHCP but has a single point of failure.
Host Based	ARP	Level of importance of each host is very difficult to decide.
Host Based	ARP	Works only with Linksys routers. Static IP not supported.
Cryptographic/ Host Based	UDP/ ARP	For UDP, authentication is a must need.
Symmetric/Private-Key Cryptography	DHCP	Legitimate hosts must register in advance, adds additional message flow, hard to manage for large number of hosts.
Symmetric/Private-Key Cryptography, Rfc	DCHP, DHCP	The authors did not describe how the random value (the number, which used by the server and client to compute the session key) is determined.
Router Based	IP, ARP	Filtering-on-path method can't ensure a secure communication.
Router/ Host Based	IP, DHCP	This system is considered as the highest secured communication. But not so user friendly.

The main idea behind the attack is to impersonate same mobile network code as the legitimate GSM network to false BTS (or IMSI Cather) (Hardin, 2018) and convince the victim that this station is the valid one. Let us consider the next example: network consists of the Legitimate MS, Legitimate BTS, False BTS, and False MS. Attacker's network is a combination of the False BTS and False MS. While in standby mode the MS connects to the best received BTS. Therefore, False BTS should be more powerful than the original one, or closer to the target. If the victim is already connected, then the attacker requires to draw any present real stations. The algorithm of the FBS-based MITM attack on GSM is the following:

1) Attacker sets-up connection between False BTS and Legitimate MS.
2) False MS impersonates the victim's MS to the real network by resending the identity information, which was received from the step 1.
3) Victim's MS sends its authentication information and cipher-suites to the False BTS.
4) Attacker forwards message from step 3 to the Legitimate BTS, with changed authentication abilities of the MS to do not support encryption (A5/0 algorithm, or too weak encryption algorithm (e.g., A5/2).
5) Legitimate MS and Legitimate BTS exchange authentication challenge (RAND), and authentication response (SRES), attacker forwards them.

Figure 4 shows a graphical representation of the example stated above. Finally, the authentication is finished. All following messages between the victim and real network are going through attacker's entities, with encryption specified by an attacker, or no encryption at all. This manipulation is possible since GSM does not provide the data integrity (Chen et al., 2007) as a result, the attacker can catch, modify, and resend messages. At the designing phase of the GSM protocol, FBS seemed impractical due to costly required equipment, but currently, this kind of attack is completely applicable since costs decreased (Feher et al., 2018).

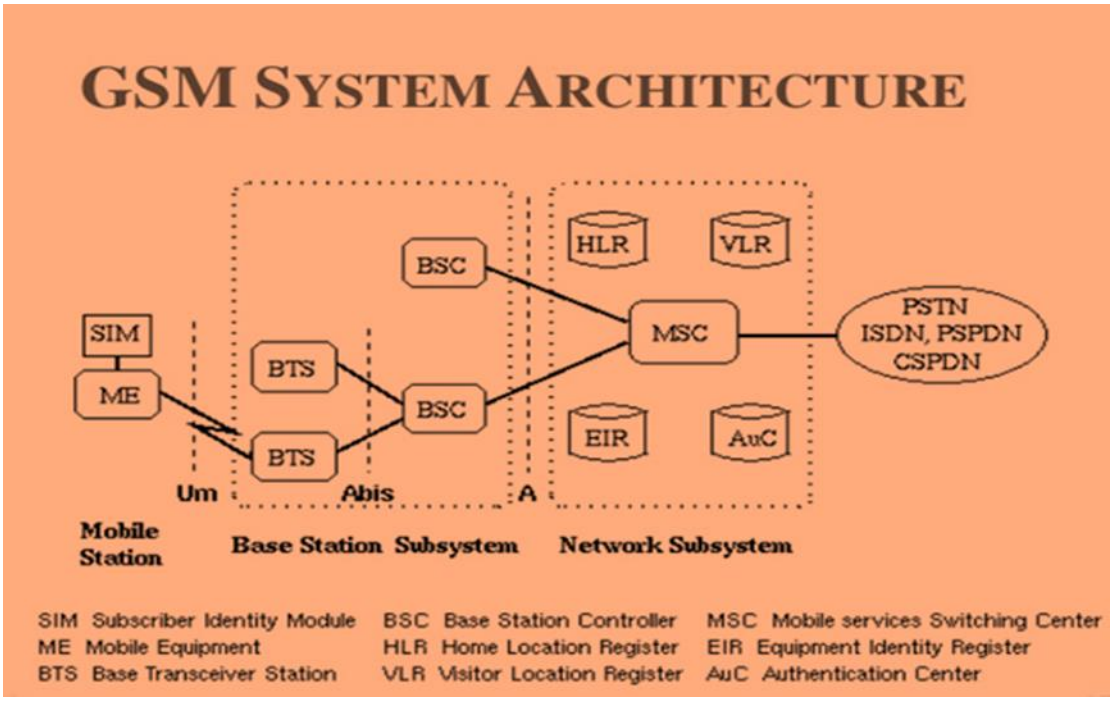

Figure 3. GSM Architecture.

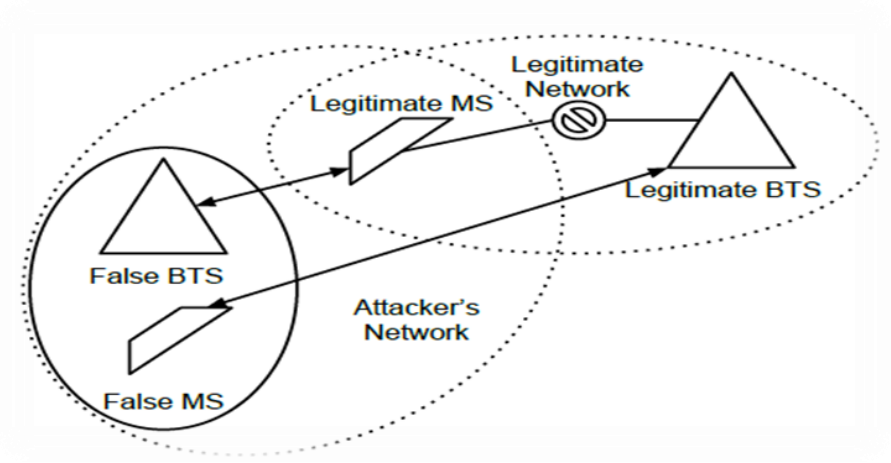

Figure 4. MITM in GSM network.

Among the reasons we can identify open-source projects and low-cost hardware. In particular, an attacker can build its own false BTS for less than $1,000. An algorithm of FBD based MITM attack on GSM network is given below in **Figure 5**.

Table 3 discusses various FBS based MITM attacks prevention approaches and different attacks with regarding references.

3.6. Statistical Analysis pf MITM Attack

For statistical analysis of the MITM attacks, we refer to the usual finite lattice of security levels, $(\mathcal{S}, \sqsubseteq_{\mathcal{S}}, \sqcap_{\mathcal{S}}, \sqcup_{\mathcal{S}}, \top_{\mathcal{S}}, \bot_{\mathcal{S}})$ and based on it define $\zeta: \mathrm{N} \to \mathrm{S}$ as a mapping from names to their security levels. Now, we can define the *name integrity* property as follows.

Property [Name integrity]

We say that a name, x, has the integrity property with respect to a ϕ_A environment if,

$$\forall n \in value_{of(\phi_A(x))}: \zeta(x) \sqsubseteq \zeta(n) \qquad \text{(i)}$$

The predicate integrity $(\mathrm{x}, \phi_{\mathrm{A}})$ indicates that x upholds the above property with respect to ϕ_A. A MITM attack is defined as an attack in which the intruder is capable of breaching the integrity of names of two processes.

Property [Man-in-the-Middle Attack]

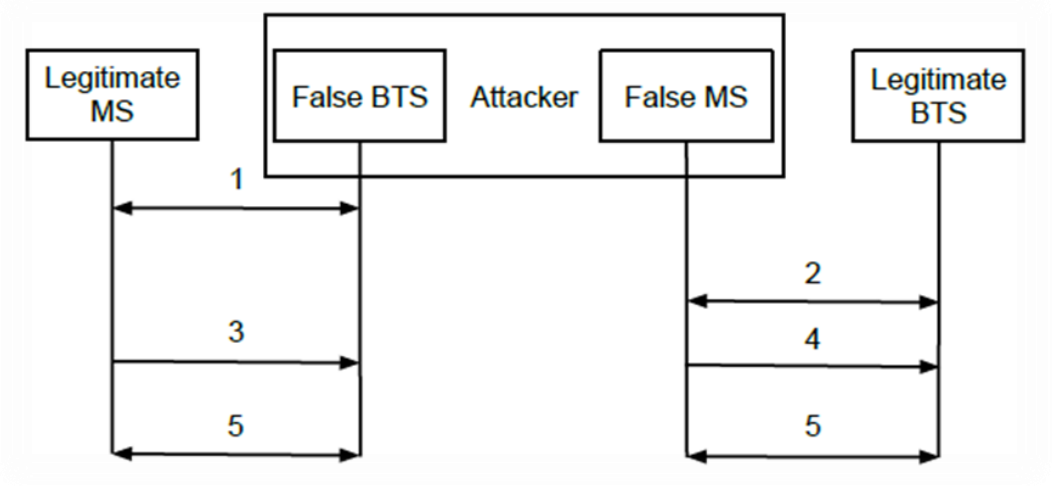

Figure 5. MITM on GSM network via FBS method.

Table 3. FBS based MITM attacks preventions

Preventions	Ou et al., 2010	Huang et al., 2011	Hwang & Gope, 2014	Chaudhari & Saxena, 2014	Saxena & Chaudhari, 2014
MITM attacks	Yes	Yes	Yes	Yes	Yes
Replay attacks	Yes	Yes	Yes	Yes	Yes
Active attack in unauthorized network	Yes	Yes	Yes	Yes	Yes
Redirection	Yes	Yes	Yes	Yes	Partially
DoS attack	No	Partially	Yes	No	Yes

A context, C (a process with a hole) succeeds in launching a MITM attack on two processes, P and Q, if the result of the abstract interpretation, $A(|C(P|Q|)\{||\}\perp_{D\perp} = \Phi_A$ proves that: $\exists_x \in bn(P), y \in bn(Q)$: $\neg(integrity(x, \Phi_A) \vee integrity(y, \Phi_A))$ (ii)

3.7. Preventing MITM

Blocking MITM attacks requires a few down to earth ventures with respect to clients, and additionally a combination of encryption and check techniques for applications. For clients, this implies:

- Avoiding Wi-Fi associations that aren't password encrypted.
- Paying consideration regarding browser warnings reporting a site as being unsecured.
- Immediately logging out of a protected application when it's not in utilize.
- Not using open systems (e.g., cafés, lodgings) when conducting sensitive financial exchanges.

For site administrators, secure correspondence conventions, including TLS and HTTPS, help relieve spoofing attacks by vigorously encrypting and authenticating transmitted information. Doing so keeps the interception of site activity and hinders the decoding of delicate information, for example, authentication tokens. It is viewed as best practice for applications to utilize SSL/TLS to anchor each page of their site and not only the pages that expect clients to sign in. Doing so helps diminishes the possibility of an attacker stealing session treats from a client browsing on an unsecured segment of a site while signed in.

Table 4. Various MITM prevention Mechanisms studied from literatures.

		Approaches				
		Detection	**Cryptography**	**Voting**	**Hardware**	**Other**
OSI	Application	BGP	BGP	DNS	DCHP	BGP
		DNS	DCHP			DNS
	Presentation	SSL/TLS	SSL/TLS	SSL/TLS	-	SSL/TLS
	Transport	-	IP	-	-	IP
	Network	-	||	-	-	||
	Data Link	ARP: [60-88]	ARP	ARP	ARP	ARP
Modular Networks	GSM	-		-	-	-
	UMTS	-		-	-	-

To counter MITM, Antivirus frameworks furnish its clients with a streamlined end-to-end SSL/TLS encryption, as a component of its suite of security administrations. Facilitated on well-known Anti-spam administrations content conveyance arrange (CDN), the authentications are ideally executed to forestall SSL/TLS compromising attacks, for example, minimize attacks (e.g. SSL stripping), and to guarantee compliance with most recent PCI DSS demands. Offered as a managed benefit, SSL/TLS arrangement is stayed up with the latest maintained by an expert security, both to stay aware of compliance demands and to counter emerging dangers (e.g. Heartbleed). Finally, with Antivirus dashboards, the client can likewise design HTTP Strict Transport Security (HSTS) arrangements to implement the utilization of SSL/TLS security over different subdomains. This furthers secure site and web application from convention minimize attacks and treat hijacking endeavours. **Table 4** gives a typical review of different types of prevention methodologies.

4. CONCLUSION

The MITMs interrupt interchanges between two frameworks, and this phenomenon takes place when the attacker is responsible for a switch along typical point of movement. The attacker in all cases is situated on a similar communicated domain as the victim stands. Indeed, in a HTTP exchange, a TCP protocol exists among the customer and the server. The attacker divides the TCP protocol into two connections – one between the victim and the attacker and the other between the attacker and the server. On intercepting the TCP protocol, the attacker goes about as an intermediary reading, altering and inserting information in intercepted correspondence. In an unsecured connection (e.g. HTTP protocol), the communication of two users can be hacked by an intruder without any difficulties. In a HTTPS connection, a single TCP protocol is attained by building two independent SSL connections. A MITM attack exploits the shortcoming in arrange correspondence convention, convincing the casualty to course movement through the attacker instead of ordinary switch and is by and large alluded to as ARP spoofing. This unethical phenomenon can affect a country's economy and may be a reason of instability between nations by stealing/modifying classified/secret defense sector data/information. So, this unethical phenomenon has to be prevented, and the necessary measures should be taken for ending. Although the paper did not focus on extensive analysis for future research directions of MITM, but a good understanding about MITM and the technologies for preventing MITM like Li-Fi were discussed briefly.

ACKNOWLEDGEMENT

The authors are grateful to the Dept. of Mechanical Engineering and Dept. of Computer Science and Engineering, RUET for providing technical and financial support to conduct this survey research.

REFERENCES

Chaudhari, N. S., & SAXENA, N. (2014). NS-AKA: An improved and efficient AKA protocol for 3G (UMTS) networks. *International Conference on Advances in Computer Science and Electronics Engineering - CSEE 2014*, 220–224. https://doi.org/10.15224/978-1-63248-000-2-74

Chen, Z., Guo, S., Zheng, K., & Yang, Y. (2007). Modeling of man-in-the-middle attack in the wireless networks. *2007 International Conference on Wireless Communications, Networking and Mobile Computing, WiCOM 2007*.

https://doi.org/10.1109/WICOM.2007.562

Conti, M., Dragoni, N., & Lesyk, V. (2016). A Survey of Man in the Middle Attacks. In *IEEE Communications Surveys and Tutorials* (Vol. 18, Issue 3). https://doi.org/10.1109/COMST.2016.2548426

DEMUTH, T., & LEITNER, A. (2005, July). Traffic Tricks. *Linux Magazine*. https://www.linux-magazine.com/Issues/2005/56/ARP-Spoofing

Dutta, A. K. (2018). Deployment of Soft-Computing for System Computing and Informatics. *American Journal of Computer Science and Information Technology*, *06*(02). https://doi.org/10.21767/2349-3917.100018

Feher, B., Sidi, L., Shabtai, A., Puzis, R., & Marozas, L. (2018). WebRTC security measures and weaknesses. *International Journal of Internet Technology and Secured Transactions*, *8*(1). https://doi.org/10.1504/IJITST.2018.092138

Hardin, N. V. (2018). UNCOVERING THE SECRECY OF STINGRAYS: What Every Practitioner Needs to Know. *Criminal Justice*, *32*(4), 20–24.

Huang, Y. L., Shen, C. Y., & Shieh, S. W. (2011). S-AKA: A provable and secure authentication key agreement protocol for UMTS networks. *IEEE Transactions on Vehicular Technology*, *60*(9). https://doi.org/10.1109/TVT.2011.2168247

Hudaib, A. A. Z. (2014). Comprehensive Social Media Security Analysis & XKeyscore Espionage Technology. In *Zare Hudaib International Journal of Computer Science and Security (IJCSS)* (Issue 8).

Hwang, T., & Gope, P. (2014). Provably secure mutual authentication and key exchange scheme for expeditious mobile communication through synchronously one-time secrets. *Wireless Personal Communications*, *77*(1). https://doi.org/10.1007/s11277-013-1501-5

Kozaczuk, W., & Kozaczuk, W. (1984). *Enigma: How the German Machine Cipher was Broken, and how it was Read by the Allies in World War Two* (C. Kasparek (ed.); 2nd ed.). University Publications of America. https://books.google.co.id/books/about/Enigma.html?id=5hJnAAAAMAAJ&redir_esc=y

Meyer, U., & Wetzel, S. (2004). A man-in-the-middle attack on UMTS. *WiSe '04: Proceedings of the 3rd ACM Workshop on Wireless Security*, 90–97. https://doi.org/https://doi.org/10.1145/1023646.1023662

Oh, M., Kim, Y. G., Hong, S., & Cha, S. (2012). ASA: Agent-based secure ARP cache management. *IET Communications*, *6*(7). https://doi.org/10.1049/iet-com.2011.0566

Ornaghi, A., & Valleri, M. (2003). Man in the middle attacks. *Blackhat Conference Europe*. https://blackhat.com/presentations/bh-europe-03/bh-europe-03-valleri.pdf

Ou, H. H., Hwang, M. S., & Jan, J. K. (2010). A cocktail protocol with the Authentication and Key Agreement on the UMTS. *Journal of Systems and Software*, *83*(2). https://doi.org/10.1016/j.jss.2009.08.019

Philip, R. (2007). *Securing wireless networks from arp cache poisoning*. San Jose State University.

Rahim, R. (2017). Man-in-the-middle-attack prevention using interlock protocol method. *ARPN Journal of Engineering and Applied Sciences*, *12*(22). https://doi.org/10.17605/osf.io/wsa8d

Saif, S., Gupta, R., & Biswas, S. (2018). Implementation of cloud-assisted secure data transmission in WBAN for healthcare monitoring. *Advances in Intelligent Systems and Computing*, *706*. https://doi.org/10.1007/978-981-10-8237-5_64

Saxena, N., & Chaudhari, N. S. (2014). Secure-AKA: An efficient AKA protocol for UMTS networks. *Wireless Personal Communications*, *78*(2). https://doi.org/10.1007/s11277-014-1821-0

Schuckers, S. A. C. (2002). Spoofing and Anti-Spoofing Measures. In *Information Security Technical Report* (Vol. 7, Issue 4). https://doi.org/10.1016/S1363-4127(02)00407-7

Sounthiraraj, D., Sahs, J., Greenwood, G., Lin, Z., & Khan, L. (2014). *SMV-HUNTER: Large Scale, Automated Detection of SSL/TLS Man-in-the-Middle Vulnerabilities in Android Apps*. https://doi.org/10.14722/ndss.2014.23205

Statica, R., Howell, C. A., & Copa, K. L. (2017). *In-band identity verification and man-in-the-middle defense* (Patent No. US 9,584,530 B1). https://patents.google.com/patent/US9584530B1/en

Su, Z., Timmermans, W., Zeng, Y., Schulz, J., John, V. O., Roebeling, R. A., Poli, P., Tan, D., Kaspar, F., Kaiser-Weiss, A. K., Swinnen, E., Toté, C., Gregow, H., Manninen, T., Riihelä, A., Calvet, J. C., Ma, Y., & Wen, J. (2018). An overview of european efforts in generating climate data records. *Bulletin of the American Meteorological Society*, *99*(2). https://doi.org/10.1175/BAMS-D-16-0074.1

Sun, D. Z., Mu, Y., & Susilo, W. (2018). Man-in-the-middle attacks on Secure Simple Pairing in Bluetooth standard V5.0 and its countermeasure. *Personal and Ubiquitous Computing*, *22*(1). https://doi.org/10.1007/s00779-017-1081-6

Valluri, M. R. (2018). Cryptanalysis of Xinyu et al.'s NTRU-lattice based key exchange protocol. *Journal of Information and Optimization Sciences*, *39*(2). https://doi.org/10.1080/02522667.2017.1368182