A Review of Man in the Middle Attacks in M2M Communications and Attack Handling Mechanisms

Sabitha Banu.A
Avinashilingam Institute for Home Science and Higher Education for Women
sabi.banu@gmail.com

Abstract

The increase of interconnected objects through Machine to Machine Communication (M2M) is unpredictable. The researchers have predicted that in forth coming days, around fifty billion objects throughout the world will be connected with each other with the help of internetwork of smart objects. As the network grows the number of cyber Threats are also increases. Among all cyber threats MITM attack is one of the major threats against network security .Man-In-The-Middle (MITM) is a kind of attack where a malicious third party secretly takes control of the communication channel between two or more endpoints. The MITM attacker can intercept, modify, change, or replace target victims' communication traffic. Moreover, victims are unaware of the intruder, thus believing that the communication channel is protected. The attack targets not only the actual data that flows between endpoints, but also the confidentiality and integrity of the data itself. 95% of HTTPS are vulnerable to MITM attacks. In this paper taxonomy of MITM attack is discussed based on several parameters.

Introduction

Machine-to-Machine (M2M) communications is an emerging communication paradigm that provides ubiquitous connectivity between devices along with an ability to communicate autonomously requiring no human intervention. It is often used for remote monitoring. M2M communications acts as an enabling technology for the practical realization of Internet-of-Things (IoT). The IoT is envisioned as `a global network of connected devices having identities and virtual personalities operating in smart spaces and using intelligent interfaces to communicate within social, environmental, and user contexts. This vision of IoT represents a future where billions of everyday objects and surrounding environments will be connected and managed through a range of communication networks and cloud-based servers.

Today, almost each aspect of our life may be associated with the usage of Internet or cellular networks. For instance, we use online home banking, online entertainment and shopping, social networks, and so on. All these online services store or transfer user's sensitive information, which represents a key target for hackers. Besides individuals, hackers target enterprises and organizations, leading to big economical loss. In this new world of "people and things always connected" by means of the Internet, it is very common to daily read about successful attacks to connected things and online services.There are many number of cyber attacks in machine to machine communications emerging in this real world which affects all kinds of businesses.

Machine to Machine Networks are likely to encounter several types of cyber attacks and it is shown in the Fig 1 as follows:

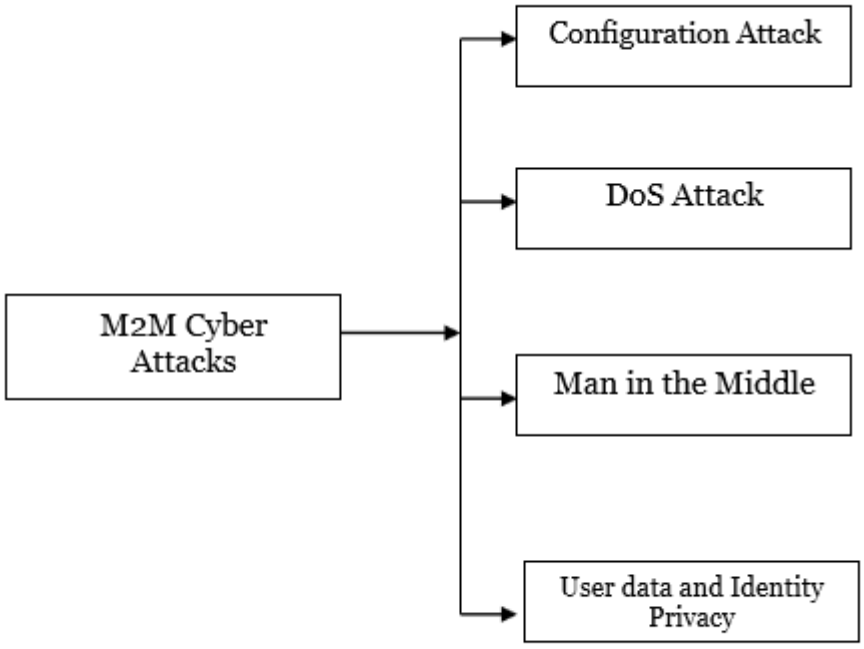

Figure 1.Cyber Attacks in Machine To Machine Communications

Among those most successful attacks is Man-In-The-Middle (MITM), which results in gaining control over end-users' transferred data.

A. MITM Risks

Wired Networks: When a man-in-the-middle attack is conducted in a wired network it requires knowing how nodes on a network create a representation of the network, and how the nodes are spoofed.A MITM attack can be carried out in a wired network via ARP spoofing, DNS spoofing, IP spoofing, ICMP spoofing, DHCP spoofing

Wireless Networks: Essentially, everyone in the mobile enterprise is a potential target, but the most vulnerable are those in senior or executive positions in business and government.

Hackers are on the lookout for anyone who deals with sensitive information particularly those who might have access to trade secrets or financial data. Anyone who works in R&D or product development should also be cautious.

It's been estimated that nearly three quarters of the top 1,000 free apps in Google Play don't check server certificates, and nearly three quarters of those ignore any SSL errors that pop up when they communicate with the app server.

And before we start wagging fingers too vigorously at Android, Apple iOS devices seem to be just as MITM prone. A vulnerability discovered in April 2015 affected how approximately 1,500 iOS apps established their secure connections to servers. It meant that anyone intercepting data from an iPhone or iPad could access logins and other personal information transmitted via HTTPS.

B. Contribution of the Paper

In this paper we provide a detailed survey about various types of cyber attacks or threats encountered in machine to machine communications. Among those cyber threats Man in the Middle is considered as one of the major threat. Man in the Middle is categorized in to three based on several parameters which is impersonation, communication channel and location of the target. MITM based on the impersonation which is nothing but spoofing is divided into Spoofing ,Man in the Browser spoofing, Border Gateway Protocol Spoofing ,STP Mangling ,Port Stealing.

Spoofing includes ARP,DNS,ICMP,IP,DHCP where researchers have studied some detection and prevention attack handling mechanisms of ARP and IP Spoofing are consolidated in this paper.

C. Organization

The remaining part of this paper is organized as follows Section II defines MITM attack and three different MITM categories, namely based on location of an attacker in the network, nature of a communication channel, and impersonation techniques. Section III ,IV and V focus on the different types spoofing based MITM attacks. Section VI reviews few prevention and detection attack handling mechanisms suggested by authors. Section VII gives few Mitigation strategies so that we can prevent our device from different MITM attacks. Section VIII defines some machine to machine communication security risks and Section IX concludes that MITM is one of the biggest threats.

MAN IN THE MIDDLE

A man-in-the-middle refers to a piece of software that sits anywhere between the victim and their intended destination. This software can spy on the communication and in some cases even modify it. A MITM attack can only succeed when the attacker can impersonate each victim to the satisfaction of the other. Most cryptographic protocols include some form of endpoint authentication specifically to prevent MITM attacks.

Figure 2.Man in the Middle

One way to prevent MITM attacks is to authenticate both the client and server. The Taxonomy of MITM attacks are

- Eavesdropping
- Masquerading
- Message Modification
- Replaying
- Denial of Service
- Exploiting flaws in design ,implementation or Operation.

MITM compromises all the Confidentiality, Integrity and Authenticity.

MITM is categorized in to various categories based on the parameters. They are

a) MITM based on the impersonation Techniques .
b) MITM based on the communication channel in which attack is executed.
c) MITM based on the Location of the attacker and target in the network.

Let us see those categories in detail:

A . MITM based on the impersonation techniques:

It is also called as Spoofing which means the attacker pretends to be legitimate user for the purpose of stealing the information. MITM attacks are again divided in to subcategories based on the impersonation. They are as follows.

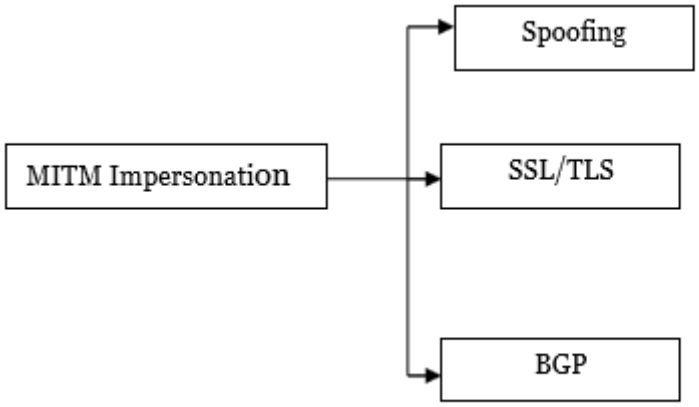

Figure 3. MITM impersonation Attacks

B. MITM based on the communication channel

MITM attacks which occurs in different layers of the OSI model are given below figure 3

OSI Model	APPLICATION	BGP MITM,DHCP Spoofing based MITM,DNS Spoofing based MITM
	PRESENTATION	SSL/TLS MITM
	TRANSPORT	IP-Spoofing based MITM
	NETWORK	
	DATALINK	ARP based Spoofing MITM

Figure3. MITM attacks in different layers of OSI

C. MITM based on the location of attacker and target in the network

They are divided into which is shown in the Figure 4.

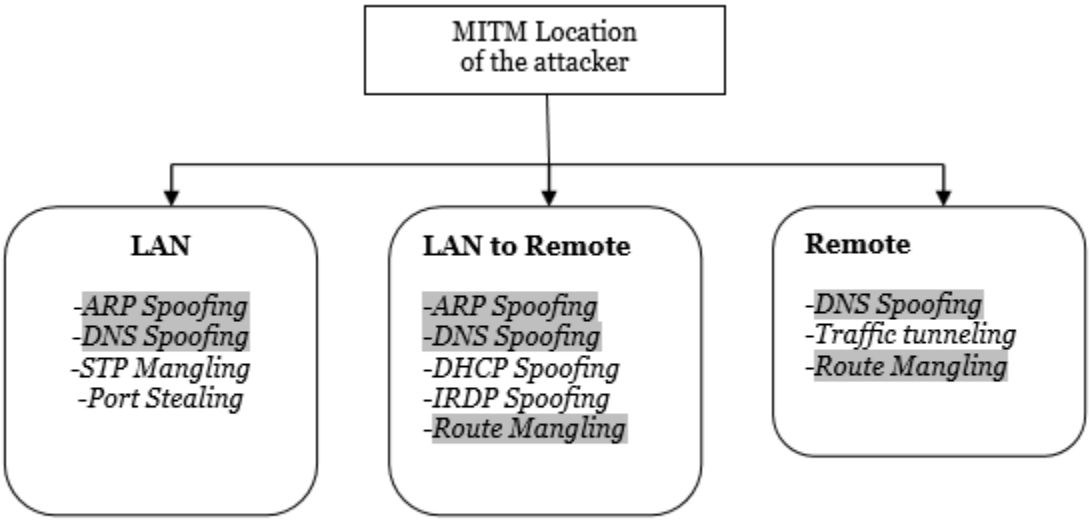

Figure 4.MITM attacks based on the location

SPOOFING BASED MITM

Spoofing refers tricking or deceiving computer systems or other computer users. This is typically done by hiding one's identity or faking the identity of another user on the Internet. This involves masking the IP address of a certain computer system. By hiding or faking a computer's IP address, it is difficult for other systems to determine where the computer is transmitting data from. Because spoofing makes it difficult to track the source of a transmission, it is often used in denial-of-service attacks that overload a server. This may cause the server to either crash or become unresponsive to legitimate requests. Fortunately, software security systems have been developed that can identify denial-of-service attacks and block their transmissions. Common types of MITM Spoofing are as follows:

1. ARP spoofing based MITM attack

Network devices use ARP protocol to map network addresses to Media Access Control (MAC) addresses. ARP is crucial in LAN communications, because each frame that leaves a host must contain a destination MAC address. ARP is a trusted protocol and was not designed to cope with malicious hosts by modifying victims' local ARP cache table (adding, updating cache entries), the attacker can associate a malicious host's MAC address with IP of a target host. Consequently, the attacker can launch DoS attack, perform MITM attack and gain access to confidential information. ARP spoofing attack may be divided into two types: cheating the gateway, and cheating the host of the internal network.

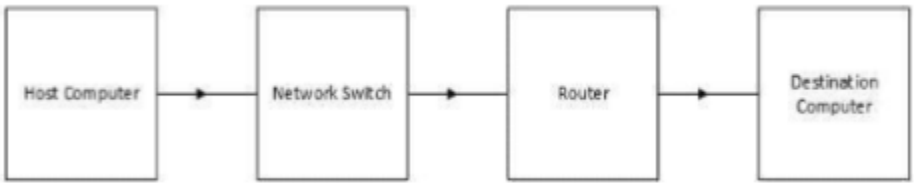

Figure 4. ARP Spoofing based MITM

B. DNS Spoofing Based MITM ATTACK

A domain name system server translates a human-readable domain name (such as example.com) into a numerical IP address that is used to route communications between nodes. Normally if the server doesn't know a requested translation it will ask another server, and the process continues recursively. To increase performance, a server will typically remember (cache) these translations for a certain amount of time. This means if it receives another request for the same translation, it can reply without needing to ask any other servers, until that cache expires.

When a DNS server has received a false translation and caches it for performance optimization, it is considered poisoned, and it supplies the false data to clients. If a DNS server is poisoned, it may return an incorrect IP address, diverting traffic to another computer (often an attacker's).DNS Spoofing is shown in the Below Figure 5.

One of the most prominent and dangerous attacks against DNS is DNS spoofing, which is executed via cache poisoning (DNS spoofing quite often named as DNS poisoning). DNS service uses cache system for improving performance, but it has various weak sides. DNS spoofing results in storage by DNS resolver the invalid or malicious mappings between symbolic names and IP addresses. DNS spoofing may be categorized into:

- hijacking or sniffing packets in the process of queryresponse (between the recursive DNS andauthoritative DNS).
- cache poisoning through the birthday attack.
- hacking on authorized DNS.

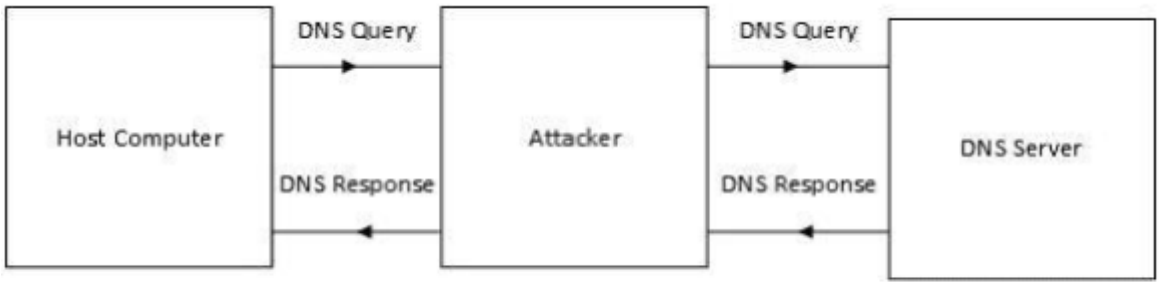

Figure 5 DNS Spoofing based MITM

C. IP Spoofing-Based MITM Attack

IP is the primary protocol in the Internet, which operates at the network layer of the OSI model. It has the task of delivering packets from the source host to the destination host solely based on the IP addresses in the packet headers. IP defines packet structures that encapsulate the data to be delivered. It also defines addressing methods that used to label the datagram with source and destination information. IP uses a connectionless model, meaning there is no information regarding the transaction state, which is used to route packets in a network. Moreover, IP specifies no method for validating the authenticity of a packet's source. This implies that the attacker could forge the source address to be any it desires. IP spoofing-based MITM is an attack where a malicious party intercepts a legitimate communication between two non-malicious parties. The malicious entity controls the flow of communication and can eliminate or alter the information sent by one of the original participants, without the knowledge of either of original endpoints. To achieve such results, attackers can use a number of IP spoofing techniques, which may be classified as follows:

1) *Blind and Non-Blind Spoofing:* The difference betweenthese two types is that in Non-Blind spoofing the attacker is in the same subnet as a victim, which opens opportunity to sniff on sequence and acknowledgement numbers.Blind spoofing requires an attacker to firstly send requests to a network, and then be able to analyse the transmission sequence.

2) *ICMP Spoofing:* IP uses ICMP to send one-way messagesto implement various error-reporting, feedback and testing capabilities. ICMP has Redirect messages, which are typically used to notify routers of a better route. These messages may be abused for execution of the MITM attack, since ICMP does not provide authentication mechanisms. The attacker spoofs ICMP Redirect messages to route the victim's traffic through its router, where it can be eavesdropped and modified.

3) *TCP Sequence-Number prediction:* TCP is a connection-oriented protocol, which means that before communication begins a connection link should be build. This is achieved using three-way handshake:

SYN, SYN-ACK, ACK. TCP uses sequence numbers for data acknowledgment. These numbers help protocol to reduce data loss and determine out-of-order packets in same way ensure reliability. Numbers are generated in Pseudo-random way in a manner known to both parties. The idea of Sequence-Number Prediction is to find the algorithm of sequence numbers generation, and then use that knowledge to intercept an existing session (often referred to as Hijacking an authorized session attack).

D. STP Mangling

STP (Spanning-Tree Protocol) mangling refers to the technique used for the attacker host to be elected as the new root bridge of the spanning tree. The attacker may start either by forging BPDUs (Bridge Protocol Data Units) with high priority assuming to be the new root, or by broadcasting STP Configuration/Topology Change Acknowledgement BPDUs to get his host elected as the new root bridge. By taking over the root bridge, the attacker will be able to intercept most of the traffic.

E. Port Stealing

This technique is useful to sniff in a switched environment when ARP poisoning is not effective (for example where static mapped ARPs are used).It floods the LAN with ARP packets. The destination MAC address of each "stealing" packet is the same as the attacker's one (other NICs won't see these packets), the source MAC address will be one of the MACs of the victims. This process "steals" the switch's port of each victim. Using low delays, packets destined to "stolen" MAC addresses will be received by the attacker, winning the race condition with the real port owner. When the attacker receives packets for "stolen" hosts, it stops the flooding process and performs an ARP request for the real destination of the packet. When it receives the ARP reply it's sure that the victim has "taken back" his port, so ettercap can re-send the packet to the destination as is. Now we can re-start the flooding process waiting for new packets.

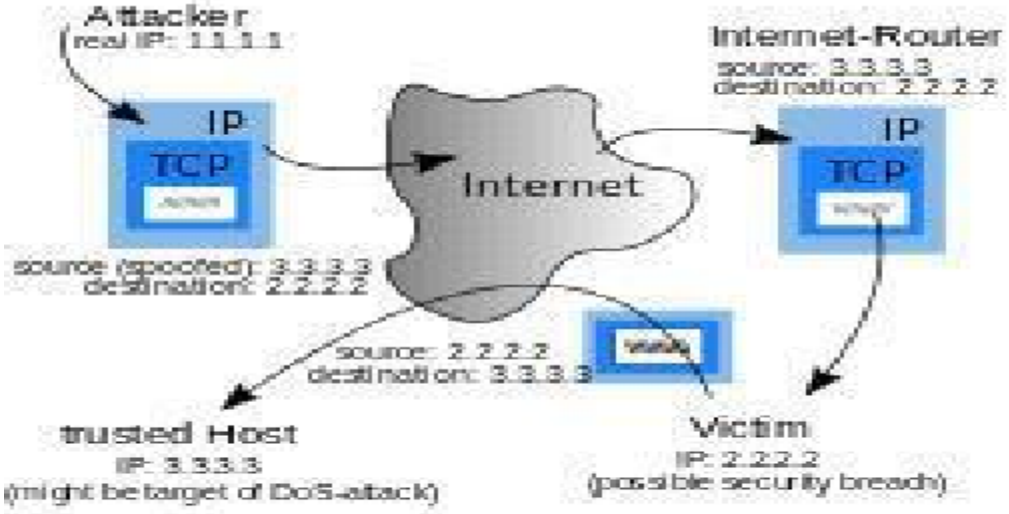

Figure 6.IP Spoofing based MITM

SSL/TLS BASED MITM ATTACK

The security guarantees offered by SSL/TLS depend on the validation of the certificate. Consequently, one of the attack's objectives is to hijack, or to forge the certificate. The following are the categorization of the SSL/TLS MITM attacks:

MITM+certificate:

(i)Attacker holds a valid certificate to the target web server. This case is possible if the attacker compromises a CA, or is able to force it to issue such certificate.

(ii)Attacker holds an invalid certificate. In this scenario the attacker may succeed if the victim will ignore the security warnings, which is a common phenomenon.

MITM+key: attacker has a private key to legitimate server.

A. Secure Socket Layers

One needs to provide security while communicating with network devices which can be obtained with the help of Secure Socket Layers (SSL) or Transport Layer Security (TLS) by using encryption methodology. One uses this protocol with other protocols for secure implementation of the services that the protocol provides. HTTPS is the most commonly used protocol and most of the online banking services and email services use it to ensure security between their servers and your web browser.

In order to understand how exactly this protocol works consider the following example. Suppose the host PC wants to connect to yahoo mail account then the communication process starts as stated below:

1. Using HTTP port 80, the client web browser will connect to http://mail.yahoo.com.
2. The web server will process this request and redirects the client to the HTTP version of this website using HTTP code.

3. The client will now connect to https://mail.yahoo.com using port 443.
4. The server will provide a certificate to the host PC to verify the identity of the website using the digital signature.
5. The host PC will now verify this certificate with the list of certificates it has.

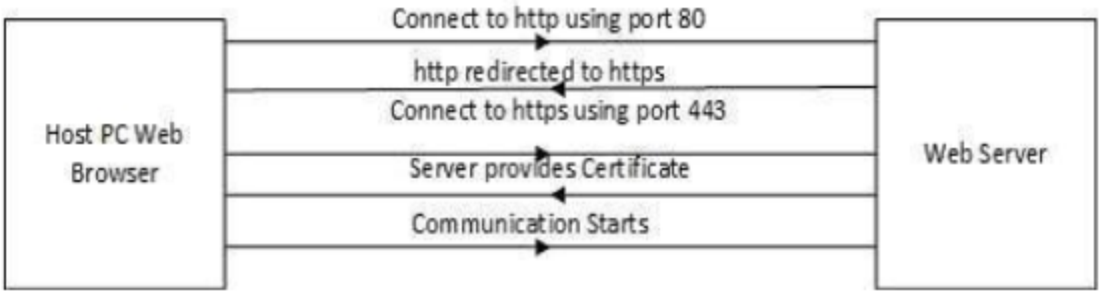

Figure 7.SS/TLS based MITM attack

B. SSL protocol communication

If the certificate doesn't match with the list of certificates of the host PC then we say that the website has failed to verify its identity so the host PC will get a certificate validation error. Even after we get this error we can proceed to connect to the website but it might be risky because we won't know whether it is the actual website we need to connect to.

BORDER GATEWAY PROTOCOL(BGP) BASED MITM ATTACK

BGP is a protocol used to exchange routing information between networks on the Internet. It is used to determine the most efficient way to route data between independently operated networks, or Autonomous Systems. As such, BGP is commonly used to find a path to route data from ISP to ISP. It is important to note that BGP is not used to transfer data, but rather to determine the most efficient routing path. The actual transfer is accomplished using whatever protocol is necessary, likely another member of the TCP/IP suite. In technical terms, a collection of IP prefixes operated by the same entity is referred to as an Autonomous System. Autonomous Systems are each assigned an Autonomous System Number (ASN) by the Internet Assigned Numbers Authority (IANA).

Since BGP determines how data travels from its Source to its destination ,security is a concern. By manipulating BGP,data can be rerouted in an attackers favor allowing them to intercept or modify traffic in internet level.

BGP hijacking is performed by configuring an edge router to announce prefixes that have not been assigned to it.if the malicious announcement is more specific than the legitimate one or claims to offer a shorter path the traffic may be directed to the attacker.attackers will frequently target unused prefixes for hijacking to avoid attention from the legitimate owner.by broadcasting false prefix announcements the compromised router may poison the routing information base(RIB) of its peers,as shown in the Fig 8.After poisoning one peer ,the malicious routing information could propogate to other peers to other autonomous ystems , and on to the broader internet.

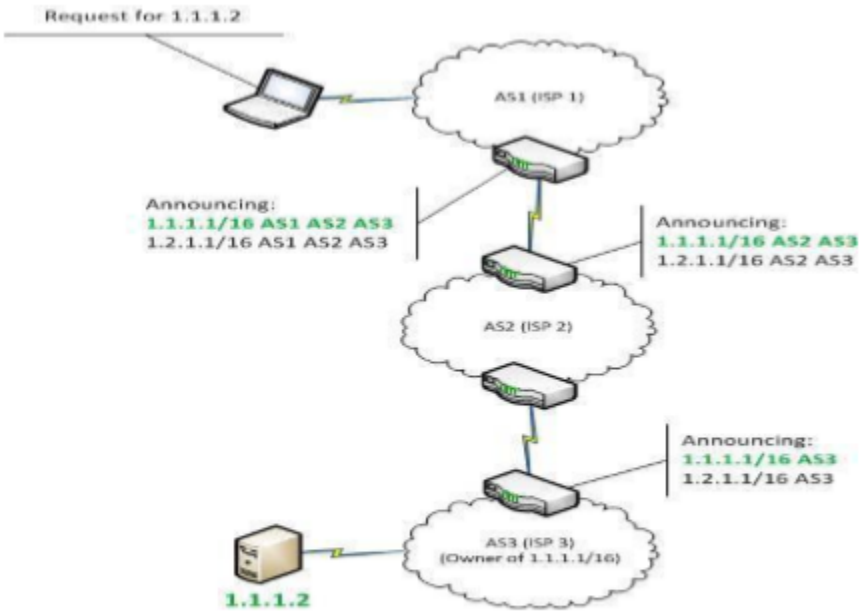

Figure8.BGP based MITM attack

LITERATURE SURVEY

ARP Spoofing based MITM attack Detection & Prevention Mechanisms are given in Table 1 & 2.

Table 1.ARP Spoofing Detection Mechanisms

Authors	Mechanisms	Limitations
Carnut et.al	Architecture based on Switched networks	Attackers hide behind the volume traffic and undetected for long period.
Online	ARP Guard, ARP Defender system	Used in LAN
	ARPwatch	Monitor Ethernet traffic, maintains database of IP& MAC Pairing.difficult to differentiate between non malicious and ARP spoofing attacks.
Hou et.al	ARP Watch	IDS Snort.
Belenguer et.al	Low-cost IDS Prototype	Detect and prevent ARP Spoofing but required to be plugged in to hub or switch.
Ramachandran et.al	Active IDS	ARP Spoofing detected by mismatch of ARP Request/Response and (IP,MAC) pairing .ARP DoS attacks generated to probe the networks eates heavy traffic on LAN.
Trabelsi et.al	Improvised switched network architecture	Detection has 2 phases : Enabling IP Packet Routing for finding the suspicious packets and Target host traffic is tested for ARP Spoofing .
Kalajdzie&Patel	Reverse ARP Poisoning with active IP Probing and IP Proing with CAM table	Instead of using test host,every host detects by itself,but contain MITM attacks are not detected and accuracy depends on the size of probing.
Barbhuiya et.al	Digital Signature	ARP requests and ARP Replies are verified by using the digital signature to identify the ARP Origin.
Song et.al	DS-ARP	Routing trace ,cache table is been under survillence and if IP,MAC pair in the cache table changes spoofing is detected .ARP Spoofing attacks are Prevented by changing the link type from dynamic state to a static state.

Table 2.ARP Spoofing Prevention Mechanisms

Authors	Mechanisms	Limitations
D.Brusc hi,A.Orn aghi & E.Rosti	S-ARP Public Key cryptography	when transmitting the ARP replies it is authenticated by AKD to prevent ARP Spoofing
Gouda et.al	Installed Security Server which has 2 protocols Invite-accept, request -reply	Security is enhanced ,single point of failure obvious target of DoS attacks
Goyal et. al	Enhanced S-ARP with low computational costs. Combination of digital signatures ,OTP and hash chain.	To avoid additional computations same digital signatures used for many ARP replies. To connect client with untrusted server OTP is shared for security and still uses AKD because it has single point of failure.
Lottah et.al	T-ARP	used for reducing computational cost of S-ARP by generating tickets for each (IP,MAC) pair .LTA(local ticket Agent) and key management server (KMS) to issue public key.
		Performance overhead ,replay attacks.
Y.I.Jersc how, C.Loche rt, B.Scheu rmann	Cryptographic Link Layer(CLL) in law used public key cryptography	Host authenticate each other by exchanging the cryptographic parameters
P.Limm aneewic hid & W.Lilaki atsakun	P-ARP ,nonce, hash function HMAC	over all network throughput to an DoS, Slows down the acceptable level

Table 3.IP Spoofing Defence Mechanisms

Authors	Mechanisms	Drawbacks
	Ingress Filtering Egress Filtering	Filtering on path using ACL(Access control List) and uRPF(unicast Reverse Path Forwarding). Ingress Filtering & Egress Filtering is deployed at router level.
Yao et.al Z.Duan,X.Yuan & J.Chandrashekar	DPF(Distributed Packet Filtering) IDPF(Inter domain Packet Filter Extension of	If packets are transmitted in unexpected route they are dropped Builds inter domain filtering rules based on the valley free feature of inter domain routing and

	DPF	BGP announcement filtering rules .
A.Bremler-Barr & H.Levy	Spoofing Prevention method	Autonomous systems tag is inserted with the data packet specifying the key(S,D).up on receiving in the destination key is verified and removed.
X.Liu,A.Li, A.Yang & D.Wetherall	Packet Passport System	Symmetric Cryptography & hash algorithms. Does not provide protection against spoofing.
H.Wang,C.Jin,and K.G.Shin	HFC(Hop Count Filtering) HOST based solutions	Checks the validation of the source prefix based on the binding between prefix and hop count value. Produces false negatives.HCF bypassed by Attackers.
A.Yaar,A.Perrig and D.Song	Stack Path identifier(Pi) (Host and Router based Solution	Each router uses IP identification field for marking. Packets travelling on the same path have same markings. even if the pi mark receive attack packets it is forced to drop valid packets

MITIGATION STRATEGIES

MITM attacks in machine to machine communications can be mitigated by the following strategies.

A. Strong WEP/WAP Encryption on Access Points

Having a strong encryption mechanism on wireless access points prevents unwanted users from joining your network just by being nearby. A weak encryption mechanism can allow an attacker to brute-force his way into a network and begin man-in-the-middle attacking. The stronger the encryption implementation, the safer.

B. Virtual Private Network

VPNs can be used to create a secure environment for sensitive information within a local area network. They use key-based encryption to create a subnet for secure communication. This way, even

if an attacker happens to get on a network that is shared, he will not be able to decipher the traffic in the VPN.

C. Force HTTPS

HTTPS can be used to securely communicate over HTTP using public-private key exchange. This prevents attacker from sniffing the data. Hyper Text Transfer Protocol Secure (HTTPS) is the secure version of HTTP, the protocol over which data is sent between your browser and the website that you are connected to. The 'S' at the end of HTTPS stands for 'Secure'. It means all communications between your browser and the website are encrypted. HTTPS is often used to protect highly confidential online transactions like online banking and online shopping order forms.

D.Public Key Pair Based Authentication

MITM attacks typically involve spoofing or sniffing. Public key based authentication like RSA can be used in the various layers of the stack to help ensure whether the things you are communicating with are actually the things user want to be communicating with.

The following things can be followed to prevent MITM attacks. They are

- Avoiding WIFI connections that are not password protected
- Paying attention to browser notifications reporting a website as being unsecured. Immediately logging out of a secure application when it is not in use.
- Not using public networks (eg coffee shops, hotels, when conducting sensitive transactions.
- There are two kinds of attack vectors: attack over communication channels, physical attack on devices.
- Never trust the communication channel.
- Always use encryption and Authentication.
- For website operators secure communication protocols, including TLS and HTTPS help mitigate spoofing attacks by robustly encrypting and authenticating transmitted data. It helps to prevent the interception of site traffic and blocks of decryption of sensitive data ,such as authentication tokens.

M2M SECURITY RISKS

Privacy

- Personal data relating to an individual should be accessed only to authorized parties
- Local processing by devices reduces exposure (send anonymous data)
- Ensure identification and authentication of involved parties.

Fraud

- Unattended devices deployed in unsecured environments are open to attackers.
- Restrict access and services to essential channel only configure APN.
- Do not transmit ID, password ,APN on unprotected channels.
- Use Physical or logical pairing between M2M device.

CONCLUSION

Most types of cyber attacks encountered in machine to machine communications are discussed .The major threat against network security in machine to machine communications is MITM . It is important to note that MITM attacks are possible in the critical networking components as well as new technologies. Routers and managed switches can be spoofed to create a higher security impact, and also the firewalls can be fooled to deliver legitimate traffic to a rough machine. we have analyzed MITM attacks based on the impersonation techniques ,communication channel and based on the location of the attacker . MITM is really a difficult type to tackle and hence should be taken seriously by IT management. It can result in data theft causing severe reputational and monetary losses to the corporate firms. As a bottom-line, having a correctly defined security perimeter defense design, server and network component's hardening, implementing robust patch management system and following best security practices can help fix MITM attacks. Since this attack may not be visible, being vigilant in terms of network problems and performance

always helps detect it, before a data theft can occur. Few authors have suggested some detection and prevention mechanisms .so we can conclude that 95% of HTTPS are vulnerable to MITM attacks.

References

R. Wagner(2001), "Address resolution protocol spoofing and man-in-themiddle attacks," The SANS Institute, Bethesda, Maryland, USA.Available: https://www.ida.liu.se/~TDDC03/literature/dnscache. pdf

A. Ornaghi and M. Valleri(2003), "Man in the middle attacks," in Proc. Blackhat Conf. Eur., [Online]. Available: http://www.blackhat. com/presentations/bh-europe-03/bh-europe-03- valleri.pdf

V. Ramachandran and S. Nandi(2005), "Detecting ARP spoofing: An active technique," in Information Systems Security. New York, NY, USA: Springer, pp. 239–250 M. Carnut and J. Gondim(2003), "ARP spoofing detection on switched Ethernet networks: A feasibility study," in Proc. 5th Symp. Seguranca Inf., [Online]. Available: ftp://www.linorg.cirp.usp.br/pub1/SSI/ 2003/A25.pdf

V. Goyal and R. Tripathy(2005), "An efficient solution to the ARP cache poisoning problem," in Information Security and Privacy. New York, NY, USA: Springer, 2005, pp. 40–51.

W. Lootah, W. Enck, and P. McDaniel(2007), "TARP: Ticket-based address resolution protocol," Comput. Netw., vol. 51, no. 15, pp. 4322–4337.

A. P. Ortega, X. E. Marcos, L. D. Chiang, and C. L. Abad(2009), "Preventing ARP cache poisoning attacks: A proof of concept using OpenWrt," in Proc. Int. Conf. Latin Amer. Netw. Oper. Manage. Symp. (LANOMS), pp. 1–9. [26]

N. Hubballi et al(2010)., "An active intrusion detection system for LAN specific attacks," in Advances in Computer Science and Information Technology. New York, NY, USA: Springer, pp. 129–142

K. Kalajdzic and A. Pate(2011)l, "Active detection and prevention of sophisticated ARP-poisoning man in-the-middle attacks on switched Ethernet LANs," in Proc. 6th Int. Workshop Digit. Forensics Incident Anal. (WDFIA'11), 2011, p. 81.

S. Y. Nam, S. Jurayev, S.-S. Kim, K. Choi, and G. S. Choi(2012), "Mitigating ARP poisoning-based man-in-the-middle attacks in wired or wireless LAN," EURASIP J.Wireless Commun. Netw., vol.no. 1, pp. 1–17, 2012.