New York Institute
of Technology

TERM PROJECT PROPOSAL

A Discussion and Practical Implementation of Man in the Middle Attack

19th Oct 2022

By

Kamran Adil-1319615
Lalit Manohar-1318737
Mysura Reddy Kuchuru-1317900
Sai Milind-1320979

Professor- Dr. Ziqian Dong

Table of contents

Objective of the Project

The objective of this project is to do an in-depth discussion of the Man-in-the-middle attack (MITM), it's different types, along with the prevention techniques. We have approximately more than 3 billion internet users around the globe and 640TB of data is being transferred every minute. Hence there is a lot of communication going on and essential data is being shared among one another [1]. MITM attacks are a form of cyberattack that involves gaining control of a network relay between two parties on a network, usually a host and a server, which allows hackers to intercept and modify the data or communications traveling between them. MITM attacks commonly steal login information, allowing hackers to gain access to users' confidential accounts.

Hackers may also steal personal information for the purposes of identity theft or redirect financial transactions in order to steal money [2].

In this paper, we will discuss how the intruder performs the (MITM) attack using the open-source Ettercap tool in the Kali Linux environment. Ettercap is a sniffing tool available in the Kali Linux operating system. It is used to perform sniffing, ARP snooping in MITM attacks, and other attacks like DDOS attacks, packet filtering, DNS spoofing, etc [3]. This paper attempts to implement this attack for instructional use in an academic setup.

Related Work

MITM attacks have become progressively numerous over the past few years, below

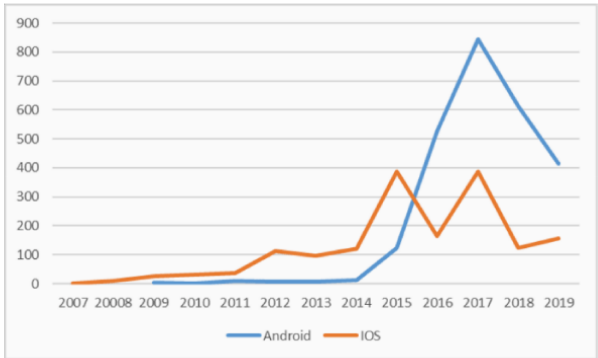

Fig-1 Vulnerability Trends of MITM attack [5]

figure represents the vulnerability trends over the years 2007 to 2019 on two types of mobile platforms. This is just a tiny portion of the data, and one type of MITM attack, in reality, the number is huge.

In order to identify these attacks based on different characteristics, a classification system has been developed. However, the majority of this classification system is either too broad to classify MITM attacks or overly specific to focus on one cyber attack [7].

One example of the classification system is the computer and network system taxonomy

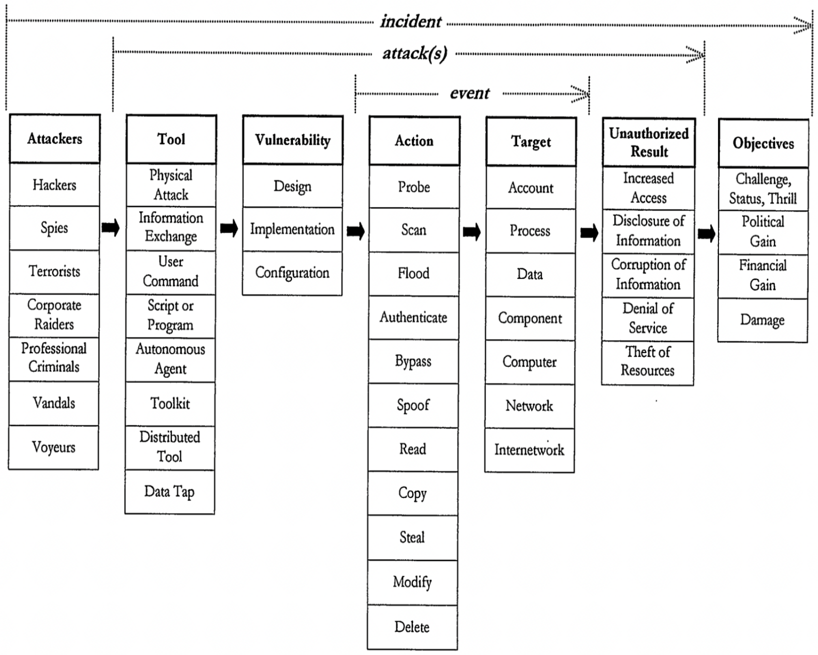

Fig 2- Computer and Networks Incident Taxonomy [6]

developed by John D Howard and Thomas A Longstaff, see figure above
Although these taxonomies provide a good framework for classifying a variety of attacks they are limited by their capability to identify specific attack characteristics.[7]

These related works provide the basis for the differentiation of MITM attacks. There are multiple prevention techniques that have been implemented in the past, and based on the type of MITM attacks, the solution varies too. For example past related work talks about prevention techniques in a wireless network, in fog computing, in IPV6 networks, in switched ethernet LANs, and many more. All these diverse types of attacks and their prevention surely create a basic plot for our project, although they remain out of scope for this paper, confining this paper to simulate MITM attack using Kali Linux environment and implement its defense using the same.

Proposed Deliverable

The team will deliver a final term paper with the contents of the Abstract, Introduction, and Objective of how prevalent and versatile MITM attacks are along with modern techniques to stop them. The Main body, Discussions and Evaluations, and Conclusion and Bibliography.

The primary task of the team is to create testbed that performs MIMT attacks for academic purposes. This will utilize Kali Linux environment. The major tool that our team will be using for performing our task is Ettercap. This tool allows us to do versatile network manipulation, it can perform character injection, packet filtering, kill any connection, etc., apart from the man-in-the-middle attack. Once Ettercap places itself in the middle of a switched connection, it can acquire and analyze all the communication happening between the two victim hosts, and then the attacker can take advantage of the situation[3].

We make sure that every person on the team has a clear understanding of setting an environment to perform MITM attack, understanding the various methods involved like character injection, packet filtering, HTTPS (Hypertext transfer protocol secure), killing the connection, ARP Poisoning (Address recall protocol) which is performed using Ettercap to know the mac address of the host systems.

Milestones

1. Setting up a common meeting time for the project group.
2. Divide the topics and start with basic research to develop ideas.
3. Understanding advanced concepts through research papers and saving citations.
4. Understanding tools like Kali Linux, EtterCap, WireShark, and Responders.
5. Install the tools on the system based on the roles decided above.
6. Perform MITM attack simulation.

7. Understand prevention techniques and install the same on the system.
8. Re-perform the MITM attack and test the prevention technique.
9. Finalize the step-by-step guide and Term paper.

Task Assignment

Task	***Assigned Member***	***Start Date***	***End Date***
Setting common meeting time	Kamran	10-05-22	10-05-22
Topic division and basic research	All Team	10-06-22	10-12-22
Understanding advanced topics and managing citations	All Team	10-12-22	11-08-22
Understanding of Tools	All Team	11-10-22	11-18-22
Start putting together term paper	Kamran	11-20-22	
Install attacking tools	Kamran and Mysura	11-21-22	11-21-22
Install prevention tools	Lalit and Milind	11-21-22	11-21-22
Perform Attack Simulation	Kamran and Mysura	11-25-22	11-25-22
Perform Prevention Simulation	Lalit and Milind	11-30-22	11-30-22
Re-Perform Attack Simulation	All Team	12-05-22	12-05-22
Finalize the paper and steps	Mysura	12-10-22	12-10-22

Bibliography

[1] H. Shah, H. Dudhat, H. Gogri, and K. Dani, “Man in the Middle Attack: Implementation using Kali Linux and Defense Mechanism.” Accessed: Nov. 01, 2022. [Online]. Available: https://web.archive.org/web/20180409220955id_/http://www.ijritt.org/paper/IJRITTV1IS010002.pdf

[2] Biscontini, Tyler. n.d. “Man-in-the-middle attack (MITM).” Research Starters (Salem Press Encyclopedia of Science, 2020. 2p.). https://search-ebscohost-com.arktos.nyit.edu/login.aspx?direct=true&db=ers&AN=141669474&site=eds-live&scope=site.

[3] B. Pingle, A. Mairaj and A. Y. Javaid, "Real-World Man-in-the-Middle (MITM) Attack Implementation Using Open Source Tools for Instructional Use," 2018 IEEE International Conference on Electro/Information Technology (EIT), 2018, pp. 0192-0197, doi: 10.1109/EIT.2018.8500082.

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

[5] qKhelif Mohamed Amine, L. Jordane, and R. Olivier, “Hardware Man-in-the-Middle Attacks on Smartphones,” Forensic Science Today, vol. 6, no. 1, pp. 012–015, Apr. 2020, doi: 10.17352/fst.000016.

[6] J. D. Howard and T. A. Longstaff, “A common language for computer security incidents,” www.osti.gov, Oct. 01, 1998. https://www.osti.gov/biblio/751004

[7] S. Stricot-Tarboton, S. Chaisiri, and R. K. L. Ko, "Taxonomy of Man-in-the-Middle Attacks on HTTPS," 2016 IEEE Trustcom/BigDataSE/ISPA, 2016, pp. 527-534, doi: 10.1109/TrustCom.2016.0106.