International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Role of Man in the Middle Attack in Business Process

*Matta Nageswararao**

GMR Institute of Technology Razam, Kinneravada, Thogiri, Saravakota, Srikakulam, Andhra Pradesh, PIN-532427, India.

ABSTRACT

For social media, cyber security has become essential. Evil actors have attacked social media networks that house sensitive and valuable data. It is made to prevent theft and damage to all types of knowledge. Without a cyber security plan, your social media accounts are at risk of criminal actors who will view them as an easy target because they are unable to defend themselves against online attacks. The Man-in-the-Middle (MitM) attack is one of the most significant attacks. Users and devices automatically believe they are in direct communication with the target system's server when they access a foreign system via the internet. Attackers disprove this presumption in a MitM attack by standing between the user and the target server. As soon as an attacker has captured communications, once communications have been intercepted, the attacker will be able to steal sensitive information, compromise user credentials, and return various answers to the user. Session hijacking, replay attacks, IP spoofing, eavesdropping assaults, and Bluetooth attacks are examples of MitM attacks. When communicating owners use the Diffie-Hellman key exchange for mutual authentication, the EECDH algorithm precludes the MITM attack, ensuring that confidentiality is preserved when sharing data in the cloud. Elliptic Curve Digital Signature Algorithm and Enhanced Elliptic Curve Diffie-Hellman (EECDH) key exchange protocol (ECDSA).

Keywords: Multi-owner, MitM (Man-in-the-Middle),Diffie-hellman key exchange protocol, Elliptic curve digital signature algorithm, Enhanced elliptic curve diffie hellman Algorithm.

1. Introduction

The world has recently been trending toward sharing knowledge that is widely accessible worldwide. As a result, hackers become even more interested in stealing consumers' personal data from the Internet. In this research, we identified multiple MITM attacks that exhibit a range of behaviour, including message tampering, message delaying, and message dropping[2]. Basketball players that attempt to intercept the ball while two other players are attempting to pass it are known as "Man-In-the-Middle"[2][3]. In this situation, the MITM attacker jeopardises communication and modifies data shared on social media by real people. This kind of assault could have a catastrophic effect on network connectivity, especially if the material provided contains sensitive data about profiles and personal information.The following two conditions must be met for an opponent to launch an MITM attack: I the misbehaving user must receive data, including important data; and (ii) the adversary must have the ability to comprehend the data's content. This kind of attack typically takes advantage of network security flaws, such as unprotected public WiFi, to place oneself in between a visitor's device and the network. The problem with this kind of assault is that it can go undetected for a long time because the victim believes the data is going somewhere legitimate. The Diffie-Hellman key exchange for mutual authentication with the EECDH algorithm safeguards against the MITM attack by requiring communication owners to authenticate themselves before sharing their keys.

2. Literature Review

- The Diffie-Hellman key exchange for mutual authentication used in the proposed EECDH algorithm protects against the MITM attack by requiring communicating owners to authenticate themselves before giving their keys in order to maintain privacy when sharing data in the cloud. [1]. The system is resilient because it combines identity- and attribute-based access rules. In addition to having the key, the information user also needs to comply with the attribute-based access policy in order to decode the message. [1]
- Reliably tying a public key to its owner is crucial for many applications. The current solution is to fulfil this assignment by signing the certificate for the general public key after validating its owner using the well-known Public Key Infrastructure (PKI), as represented by a trusted certificate authority (CA) [2].
- [2] Cecoin prevents the chance of a communication attack like the MitM in addition to avoiding the registration and distribution of fake certificates. The security of the plan has been thoroughly examined, and in a real network environment, this plan foils a MitM attack.
- The ability of the Vehicle Ad-Hoc Network (VANET) to improve traffic management and safety makes it a crucial component of Intelligent Transportation Systems (ITS). According to the literature, different Man-In-The-Middle (MITM) attacks were identified during this paper[3] with a variety of characteristics such message tampering, message stalling, and message dumping.
- Although communication-based train control (CBTC) systems are crucial to the effective and consistent functioning of urban rail transits, their

high level of network penetration leaves them vulnerable to Man-in-the-Middle (MitM) attacks[4]. Results from the Asynchronous Advantage Actor-Critic (A3C) algorithm demonstrate that the suggested strategy performs admirably while fighting off MitM attacks.

- Blocking MITM attacks requires several practical steps on the a part of users, further as a mix of encryption and verification methods for applications.
  - Avoiding such WiFi connections that are not password protected.
  - Paying more attention to browser notifications reporting an internet site as being unsecured.
  - Immediately do logging out of a secure application when it’s not in use.
  - Not using public networks (e.g., coffee shops, hotels) when conducting sensitive transactions like online payment, internet banking etc

Methodologies

Elliptic Curve Diffie-Hellman Key Exchange (ECDH) is an anonymous key agreement mechanism that enables two parties to create a shared secret across an unsecured channel and each have an elliptic-curve public-private key pair. Elliptic Curve Diffie-Hellman Key Exchange is an anonymous key agreement mechanism that enables two parties to create a shared secret across an unsecured channel and each have an elliptic-curve public-private key pair. [2] Algorithm for Enhanced Diffie-Hellman Key Exchange One of the major threats, the MITM attack, is intended to be avoided by the proposed EECDH algorithm in order to preserve data integrity and confidentiality. A network assault is a classic MITM attack in which the attacker deceitfully passes information between two owners who believe they are directly speaking with one another and may even change it.The primary goal of the proposed EECDH algorithm is to enhance privacy, confidentiality, and authentication in single-owner and multi-owner situations using cloud storage. EECDH stands for elliptic curves over finite fields, an algebraic structure used in public key cryptography. Elliptic-curve cryptography is used in the Elliptic Curve Digital Signature Algorithm (ECDSA), a variation of the Digital Signature Algorithm (DSA) [3]. A MITM attack detection and localization approach utilising cross-layer information is proposed in Cross-Layer Consistency-Based MITM Attack Detection and Localization [4]. These findings demonstrate the effectiveness of the proposed technique in detecting MITM attacks, with location errors often smaller than 0.53 m..Users must take the required precautions to protect themselves against MitM because the assaults are silent and undetectable to the targeted user. [5] The application developer is likewise accountable for making sure that their programme is impervious to MitM attacks. Users could occasionally not be able to stop a man-in-the-middle attack because of the way an application is programmed. Here are some ways to avoid being a target of a MitM attack. In some cases, users would be unable to prevent a man-in-the-middle attack due to the way an application is coded. Some methods to prevent becoming a victim of a MitM attack:

- Use two-factor authentication on email accounts
- Use traffic analytical tools on the network.
- Use certificate pinning on mobile apps
- Use VPN on public Wi-Fi network
- Educate employees about the dangers of phishing.
- Integrate email security.
- Never connect to an unknown Wi-Fi hotspot.

Results

PAPER	AUTHOR	METHOD	RESULT	ACCURACY
[1]	Anand, S., & Perumal, V.	Elliptic Curve Diffie–Hellman Key Exchange Algorithm	The author discovers the effective algorithms that have been suggested for safe data sharing between various owners. The EECDH technique is suggested for secure key exchange and preserving the integrity of shared data across several owners. The suggested EECDH algorithm is created alongside the EECDS method to safeguard the owners' data from the MITM attack. Before sharing their keys with one another, the communicating owners use the Diffie-Hellman key exchange to verify their identities.	99%
[2]	Qin, B., Huang, J., Wang, Q., Luo, X., Liang, B., & Shi, W. Luo, X., Liang, B., & Shi, W.	Elliptic Curve Diffie–Hellman Key Exchange Algorithm Enhanced Elliptic Curve Diffie–Hellman Key Exchange Algorithm	In this paper, The authors provided a secure enhanced structure of PKI named Cecoin which distributively blockchain-based. The scheme processes the guarantee of consistency to prevent from false certificates. Besides, it provides practical services of multi-certificates and identity assignment. The scheme are achieved in prototype with a desirable efficiency.	99.9%

[3]	Al-shareeda, M. A., Anbar, M., Manickam, S., & Hasbullah, I. H.	Elliptic Curve Digital Signature Algorithm (ECDSA)	This paper represent the survey of existing schemes to prevent MITM attacks in VANET. This ECDSA scheme encourage the batch verification method. To migrate the computation complexity, they utilize one-way hash. Digital signature and certificate is the only way in VANET to far from MitM attack.	90%
[4]	Raich, A., & Gadicha, V.	Cross-Layer Consistency-Based MITM Attack Detection and Localization	The experiments introduced in this paper results that the model based on the physical layer information is correct and feasible. The performance of the MITM attack detection and localization algorithm based on cross-layer information is better to protect the system.	90%
[5]	Shajina Anand, P. Varalakshmi	MITM ATTACK Prevention Technique	The authors suggested some prevention techniques to prevent the MITM attack. These techniques easily prevent the attack.	----

Discussions

According to [1], proposed EECDH performs better than conventional ECDH in terms of data exchange and mutual authentication. The ECDSA scheme processes the consistency guarantee to avoid fake signatures in [2]. Additionally, it offers useful services for assigning identities and multiple certificates. This plan was implemented in a prototype with admirable effectiveness. Due to the high mobility of vehicles on the road and the numerous security assaults, such as MITM attacks, the VANET still faces numerous difficulties in [3]. Although the algorithm described in this paper can detect and locate the MITM attack, the complexity and timeliness of the algorithm are still the constraints of the method they were discussed in [4]. The algorithm's still has limits due to its complexity and timeliness. This review article demonstrates the continued necessity to address security-related issues.

Conclusion

I studied the effective algorithms put forward for safe data sharing among numerous proprietors. For secure key exchange and to guarantee the integrity of shared data among several owners, the EECDH algorithm is suggested. The proposed EECDH algorithm is offered in addition to the EECDS method to protect data owners from MITM attacks. Before sharing their keys, the communicating owners use the Diffie-Hellman key exchange to authenticate themselves. To guarantee the confidentiality of the data, all the active owners exchange a secret key and independently verify themselves using their public and private keys. The integrity of the shared data among owners is assured by improving these algorithms. The suggested EECDH framework decreases time complexity and increases the speed of encrypting and decrypting data.The suggested EECDH framework minimises temporal complexity and increases the speed at which data can be encrypted and decrypted. When it comes to data sharing and mutual authentication, the EECDH performs better than the conventional ECDH. The system processes the consistency guarantee to guard against bogus certificates. The plan is implemented in the prototype with a desired level of efficiency. The algorithm will be improved in the future successfully to minimise complexity. The technique will also become more realistic with the addition of dynamic MITM attack detection and location.

References

1. Anand, S., & Perumal, V. (2019). EECDH to prevent MITM attack in cloud computing. Digital Communications and Networks, Hyper cluster computing,P.no: 276-287.

2. Qin, B., Huang, J., Wang, Q., Luo, X., Liang, B., & Shi, W. (2020). Cecoin: A decentralized PKI mitigating MitM attacks. Future Generation Computer Systems, 107, 805-815.

3. Al-shareeda, M. A., Anbar, M., Manickam, S., & Hasbullah, I. H. (2020). Review of prevention schemes for man-in-the-middle (MITM) attack in vehicular ad hoc networks. International Journal of Engineering and Management Research, 10.

4. Raich, A., & Gadicha, V. (2021, October). Various Threats and Challenges to Information Security via Active and Passive Attack. In 2021 International Conference on Smart Generation Computing, Communication and Networking (SMART GENCON) (pp. 1-5). IEEE.

5. Shajina Anand, P. Varalakshmi Madras Institute of Technology Department of Computers[2022], Springer Cluster Computing, [ONLINE]

Website: https://www.researchgate.net/publication/336793622_EECDH_to_prevent_MITM_attack_in_cloud_computing.

6. Al-shareeda, M. A., Anbar, M., Manickam, S., & Hasbullah, I. H. (2020). Review of prevention schemes for man-in-the-middle (MITM) attack in vehicular ad hoc networks. International Journal of Engineering and Management Research, 10.

7. Li, Y., Zhu, L., Wang, H., Yu, F. R., & Liu, S. (2020). A cross-layer defense scheme for edge intelligence-enabled CBTC systems against MitM attacks. IEEE Transactions on Intelligent Transportation Systems, 22(4), 2286-2298.

8. Sebbar, A., Zkik, K., Baddi, Y., Boulmalf, M., & Kettani, M. D. E. C. E. (2020). MitM detection and defense mechanism CBNA-RF based on machine learning for large-scale SDN context. Journal of Ambient Intelligence and Humanized Computing, 11(12), 5875-5894.

9. Stute, M., Heinrich, A., Lorenz, J., & Hollick, M. (2021). Disrupting Continuity of Apple's Wireless Ecosystem Security: New Tracking,{DoS}, and {MitM} Attacks on {iOS} and {macOS} Through Bluetooth Low Energy,{AWDL}, and {Wi-Fi}. In 30th USENIX Security Symposium (USENIX Security 21) (pp. 3917-3934).

10. Maikol, S. O., Khan, A. S., Javed, Y., Bunsu, A. L. A., Petrus, C., George, H., & Jau, S. (2021). A novel authentication and key agreement scheme for countering MITM and impersonation attack in medical facilities. International Journal of Integrated Engineering, 13(2), 127-135.

11. Kondracki, B., Azad, B. A., Starov, O., & Nikiforakis, N. (2021, November). Catching Transparent Phish: Analyzing and Detecting MITM Phishing Toolkits. In Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security (pp. 36-50).

12. Lahmadi, A., Duque, A., Heraief, N., & Francq, J. (2020, September). MitM attack detection in BLE networks using reconstruction and classification machine learning techniques. In Joint European Conference on Machine Learning and Knowledge Discovery in Databases (pp. 149-164). Springer, Cham.

13. Lahmadi, A., Duque, A., Heraief, N., & Francq, J. (2020, September). MitM attack detection in BLE networks using reconstruction and classification machine learning techniques. In Joint European Conference on Machine Learning and Knowledge Discovery in Databases (pp. 149-164). Springer, Cham.

14. Bao, Z., Guo, J., Shi, D., & Tu, Y. (2021). MITM meets guess-and-determine: further improved preimage attacks against AES-like hashing. Cryptology ePrint Archive.

15. Almon, L., Krause, A. M., Fietze, O., & Hollick, M. (2021, November). Desynchronization and MitM Attacks Against Neighbor Awareness Networking Using OpenNAN. In Proceedings of the 19th ACM International Symposium on Mobility Management and Wireless Access (pp. 97-105).

16. Kponyo, J. J., Agyemang, J. O., & Klogo, G. S. (2020). Detecting end-point (EP) man-in-the-middle (MITM) attack based on ARP analysis: A machine learning approach. International Journal of Communication Networks and Information Security, 12(3), 384-388