**Related Work on Man-in-the-Middle Attack**

Student’s Name

Institutional Affiliation

Instructor

Course

Date

**Related Work on Man-in-the-Middle Attack**

**Summary of the Authors research**

Belkhouja et al. 2018 examine the lightweight solutions appropriate for defending against man-in-the-middle (MITM) attacks against implantable medical devices (IMD). From their analysis, IMDs largely rely on wireless technology for information exchange, which, in the absence of appropriate security metrics, poses a notable danger to individual patients’ health. The work proposes the creation of a signature protocol that would help to protect IMDs from MITM attacks, and that leverages fewer resources compared to the common encryption algorithms. The method is based on a chaotic generator and a signature algorithm that serves to prevent potential third-party interference.

           Ahmad et al. 2020 identify the Vehicular Ad-hoc Network (VANET) as a novel technology that is significant in the transportation industry, attributed to its potential to enhance efficiency and safety in traffic. Usually, connected vehicles, at diverse ranges propagate overly sensitive data and that must be shared through a secure environment. Nonetheless, the authors note a presence of dishonest modes, such as MITM attacks within VANET, whose presence is detrimental as they aim at distributing and sharing malicious content, ultimately polluting the networks with compromised data. The proposed solution encompasses a novel trust model, MARINE, which has the potential for identifying dishonest modes within the MITM attacks and revoking their credentials.

           Akter et al. 2020 investigates Near Field Communication (NFC), a recent development involving the widely used, and misconceived Radio Frequency Identification (RFID) technology. NFC communications necessitate close proximity between the communicating devices, which results in a false belief of the infeasibility of the MITM attacks. However, the analysis demonstrates the practical feasibility of a MITM attack on NFC communication by incorporating practical attack scenarios. As such, the authors propose a defense mechanism that exploits a time delay leading to the attacks as an effective mitigation strategy.

           A review of the MITM attack within the wireless and computer networking undertaken by Bhushan et al 2017 identifies the attacks as a notable risk of compromise of data integrity and confidentiality. A data breach can be executed through eavesdropping and by message communication, usually through communication interception. The review provides an extensive review of the MITM attacks scope, which is focused on enhancing the understanding of the prevalent diverse risky attacks. Lastly, they provide an overview of the preventative strategies that can be leveraged to halt such attacks.

           The authors, Knežević et al. 2020re-evaluates MITM attacks against particular authentication protocols to garner fresh insight on the best approach and re-evaluation. The approach embodies evaluating the HB authentication protocols. The authors unveiled that by using the OOV-MIM, notable changes are possible, which resulted in a change in prior beliefs. It leads to the conclusion that the prior stated complexity of the attack was overestimated while the complexity of the attack was underestimated.

           The review by Salem et al. 2021 aims at mitigating MITM attacks on the internet of medical things. Specifically, the attack happens by identifying the healthcare emergency of the respective monitored individuals and subsequently replaying normal physiological data as a way of preventing the system from raising an alarm. The authors also propose a system that could be leveraged to prevent the aftermath devastating effects of the alarms of the remote healthcare monitoring system.

**Advantages and Disadvantages of the Respective Studies**

|  |  |  |
| --- | --- | --- |
| Related Studies  | Advantages  | Disadvantages  |
| (Ahmad et al., 2020) | They proposed the MARINE model, a system with a potential of performing multi-dimensional plausibility checks, which provides a chance for the receiver of verifying the trustworthiness of the sender, and the data. | The risks of the system failure are high, which necessitates advanced future research in the domain. |
| (Akter et al., 2020) | The authors proposes a strategy that seeks to eliminate the identified delays that results in the MITM attacks, an attribute that would reduce the risk of MITM attacks in the NFC, which makes it an ideal defense mechanism. | At times, the identified delays fail to be solved by the strategy. |
| (Belkhouja et al., 2018) | The proposed light weight solution, unlike the common encryption and decryption algorithms uses less resources and is dynamic, which increases its efficiency in preventing IMDs against MITM attacks.Besides, the signature algorithm ensures that it can only be validated by a trusted user, a factor that increases its robustness against a myriad of threats.  | Effective care must be taken to check the reliability of the solution, failure to which, would compromise overall plan and startegies. |
| (Bushan et al., 2017) | They proposed a myriad of solution in attempts to mitigate and potentially lessen such attacks, including standardizing a BGP MITM detection. The detection technique is victim and peer-centric, and infrastructure-based, depicting its potential effectiveness in solving the challenge. | The method is depicted as having failed to incorporate appropriate fingerprinting detection method, and failed to describe the firewalls problem solving.  |
| Knežević et al. 2020 | The overviewed protocol confers leaders an opportunity to underscore and understand its role and mandate in preventing MITM attacks.  | The algorithm is identified to leverage erroneous weight approximation, which increases the risk for making an error. As such, an attacker could fail to correctly identify the weight but collectively recover their bits. |
| (Salem et al., 2021) | The authors successfully proposed an effective mitigation strategy to implement in lessening the negative impact of MITM attacks on IoMT. The approach successfully addressed critical domains, such as the privacy of the physiological data, and energy consumption.  | Using a classification model increases the risk of failure of the strategy.  |

**References**

Ahmad, F., Kurugollu, F., Adnane, A., Hussain, R., & Hussain, F. (2020). MARINE: Man-in-the-middle attack resistant trust model in connected vehicles. *IEEE Internet of Things Journal*, *7*(4), 3310-3322.

Akter, S., Chellappan, S., Chakraborty, T., Khan, T., Rahman, A., & Alim Al Islam, A. (2020). Man-in-the-Middle Attack on Contactless Payment over NFC Communications: Design, Implementation, Experiments and Detection. *IEEE Transactions On Dependable And Secure Computing*, 1-1. <https://doi.org/10.1109/tdsc.2020.3030213>

Belkhouja, T., Mohamed, A., Al-Ali, A. K., Du, X., & Guizani, M. (2018, December). Light-weight solution to defend implantable medical devices against man-in-the-middle attack. In *2018 IEEE Global Communications Conference (GLOBECOM)* (pp. 1-5). IEEE.

Bhushan, B., Sahoo, G., & Rai, A. K. (2017, September). Man-in-the-middle attack in wireless and computer networking—A review. In *2017 3rd International Conference on Advances in Computing, Communication & Automation (ICACCA)(Fall)* (pp. 1-6). IEEE.

Knežević, M., Tomović, S., & Mihaljević, M. J. (2020). Man-In-The-Middle Attack against Certain Authentication Protocols Revisited: Insights into the Approach and Performances Re-Evaluation. *Electronics*, *9*(8), 1296.

Salem, O., Alsubhi, K., Shaafi, A., Gheryani, M., Mehaoua, A., & Boutaba, R. (2021). Man-in-the-Middle Attack Mitigation in Internet of Medical Things. *IEEE Transactions on Industrial Informatics*, *18*(3), 2053-2062.