UNIVERSITI TEKNOLOGI MARA

PACKET HEADER SUPPORT USING HYBRID SECURITY APPROACH FOR SECURING TRIVIAL FILE TRANSFER PROTOCOL IN MACHINE TO MACHINE APPLICATIONS

NUR NABILA BINTI MOHAMED

Thesis submitted in fulfillment
of the requirements for the degree of
Doctor of Philosophy
(Computer Engineering)

Faculty of Electrical Engineering

September 2019

ABSTRACT

Trivial File Transfer Protocol (TFTP) is noted as one of the well-known protocols for managing data transfer in Machine to Machine (M2M) constrained embedded system due to its lightweight features and compatibility. However, the protocol provides zero support for data authentication or encryption method, also lacks of access control mechanism and no protection from Man In The Middle (MITM) attack. The security flaw should not be ignored as the attackers can easily access, modify private information and install malicious codes to interrupt the communication especially during data collection and transmission. Here in this thesis study, a feasible hybrid security extension has been incorporated into the protocol combining the Hash-based Message Authentication Code and Diffie Hellman Key Exchange (HMAC-DHKE) to enable key agreement and Advanced Encryption Standard (AES) algorithm to perform data encryption/decryption. Upon achieving the first objective, a reasonable hybrid security mechanism has been identified and ratified to perform the shared secret and data encryption/decryption in TFTP. The proof of concept of the proposed scheme and analysis study are presented to demonstrate that the proposed work can mitigate at least MITM and impersonation attacks. The second objective has been achieved by designing and reconstructing feasible security parameters to be extended in the TFTP protocol header. In this thesis study, three basic types of security schemes have been compared with the standard protocol: the protocol with single security extension (TFTP_AES256), the protocol extended with hybrid of conventional DHKE and AES encryption (TFTP_DK2048 and TFTP_DK3072) and the proposed protocol extended with hybrid of authenticated key agreement (HMAC-DHKE) and AES encryption (TFTP_AK2048 and TFTP_AK3072). Based on the result, the security overhead was approximately 35% for initial key agreement and 7% for encryption and decryption process from the overall operation. The energy usage was two times higher than the standard protocol, but only a slight delay of less than 1% has been produced when the proposed approach was compared to other secure TFTPs. The comparative performance analysis has achieved the final objective of the thesis study. Based on the findings in this thesis work, the novel secure TFTP has also accomplished several security desires which are data confidentiality, data integrity and authenticated key agreement properties. Compared to the conventional zero-security protocol which has no assurances the messages that is sent will arrive uncompromised to the intended destination, this simple security solution on TFTP would satisfy the security requirements during file transmission in M2M and IoT communication technology.

ACKNOWLEDGEMENT

Alhamdulillah, first and foremost, all praises to Almighty Allah for His blessings, for the wisdom He bestowed upon me, the strength and good health through the whole journey of completing my study and finishing this thesis. He is The One who listens to all my problems and guides me thorough my postgraduate study. I would not be able to finish my research and thesis without His endless blessings that He granted upon me.

I would like to express my deepest and sincere appreciation to my outstanding supervisor, Professor Ir Dr Habibah Hashim, for her constant supervision, patient guidance, endless support and also the time to consult my research work and progress on schedule. She is my mother, coach and supervisor for almost seven years since my master degree. She has guided me since I learnt to crawl, until I am able to run. I will forever be indebted to her, not only in the research work, but also motivations and advises to become successful person in life. Her useful critiques and suggestions throughout the work and thesis particularly have contributed to the success of my research work. In addition, my appreciation goes to my co-supervisor, Ir Dr Yusnani Mohd Yussoff for her support, feedback, encouragement and persistent help regarding this topic. Their guidance helped me in all the time of research and writing thesis. I could not have imagined having better advisors and mentors for my PhD study.

I would further express my appreciation to the Ministry of Higher Education, Universiti Teknologi MARA and Research Management Institute UiTM for the grants to fund and support my research work. I also would like to thank my fellow Information Security and Trusted Infrastructure Lab (InSTIL) mates especially Dr Anuar, Mr Syed Farid, and Dr Mohammed, who helped me a lot, also other lab members for their continuous support and co-operation. My PhD journey would be lonely without the presence of all of them.

Lastly, my deepest gratitude goes to my supportive parents, Mama [redacted] and Abah Ir Haji Mohamed Daud and also the siblings, Nur Nadia, Mohd Nabil and Nur Najwa, who never stop praying and supporting me to go on completing this thesis. I would also like to thank my beloved husband, my backbone along this journey, Mohd Syazwan Che Zakaria for his endless moral support, helping me a lot and taking care of our children, Nur Aisyah Zafirah and Muhammad Talhah during my study. Finally, to those who indirectly contributed in this research, your kindness means a lot to me.

Thank you to everyone, and Only the Almighty Allah SWT could pay back all your kindness to me.

TABLE OF CONTENTS