UNIVERSITI TEKNOLOGI MARA

PROFILING AND MITIGATING BRUTE FORCE ATTACK IN WIRELESS LAN

MOHAMMAD HAFIZ B MOHD YUSOF

Dissertation submitted in fulfillment
of the requirements for the degree of
Master of Science in Computer Networking

Faculty of Computer and Mathematical Sciences

Jan 2015

ABSTRACT

Brute force is another dangerous type of cyber-attack meant for cracking wireless LAN WPA/WPA2 password. It preludes with several other attacks' attempts namely DeAuthentication, packet sniffing (`airodump`) and finally `aircrack`. The successful of a brute force attack is so determined by these attempts. This study will analyze DeAuthentication attack traffic pattern, sniffing and aircrack activity and propose two mitigation techniques which are 1) increase beacon time interval 2) mapping user's MAC address and finally evaluate its performance using normal distribution model. Experimental result shows that deployment of mitigation techniques is efficient to stop these activities and mitigate the brute force attack and in terms of performance it shows great number of processing time above mean value.

ACKNOWLEDGEMENT

Thanks to almighty Allah and Prophet Muhammad peace and blessings be upon him.

Immeasurable gratitude and immense appreciation for the support, guidance and help are conveyed to the following personnel who in a way or another have contributed in the completion of this thesis.

Dr. Fakariah Hani bt. Mohd Ali, my research supervisor, security expert and crypto doctorate for her support, advice, guidance, valuable comments, suggestions and provisions that helped me a lot in the completion and success of this paper.

Assoc. Prof. Dr. Mazani b. Hj. Manaf, my lecturer in Research and Methodology, for his review on my research, guidance in research methodological framework and structure and endless comments to correct this paper.

En. Abdul Hamid @ Hamid Othman, my lecturer in Advanced Network Security, for his technical support, unlimited enthusiasm in knowledge sharing, openness and support in lending the necessary reading materials needed in the accomplishment of this study.

To **my wife, my daughter**, both my parents for your unlimited love, pray and support.

Table of Contents

CHAPTER 1

INTRODUCTION

Chapter 1 discusses some elementary foundation of the paper such as background, problems statements, the research objectives, research scope and limitation, and significance of the research.

1.0 BACKGROUND OF RESEARCH

Wireless Local Area Network (WLAN) has gained popularity due to its mobility and portability; however this technology is prone to security threats like spoofing. This is due to unguided medium (i.e air space) used by WLAN technology to propagate information is ranged in open public access. Due to its widespread deployment areas, WLAN security network becomes more and more severe (Dong et. al ,2010).

Earlier stage of WLAN, uses Wired Equivalent Privacy (WEP) in their security feature was not sufficient as more and more flaws discovered and nowadays were replaced by Wi-Fi Protected Access (WPA) and WPA2 technologies (Petiz et. al ,2013) however this techniques still vulnerable to DoS and brute force attacks.

WLAN has been the target for a large number of attacks (Laishun et. al ,2010) and amongst them is brute force attack. Brute force WLAN attack in this study is to exhaust PSK (Phase Shift Keying) information extracted from any particular Access Point (AP) against wordlist database created from various available open source Pentest