UNIVERSITI TEKNOLOGI MARA

WIRELESS SECURITY ASSESSMENT ON THE FTMSK2 BUILDING

ZAINURZAMAN B. MAH SANGIT @ KASMAT
2004617776

Bachelor of Science (Hons) Data Communication and Networking
Faculty of Information Technology And
Quantitative Science

Dec 2007

DECLARATION

I hereby certify that this thesis and the research to which it refers are the produce of my own and any parts, ideas, or quotes from the research or work which belongs to any other people that will be cited here in this research hereafter will be acknowledged in full accordance of the discipline and the standard of referring practices.

DEC 2007 ……..…….

ZAINURZAMAN B. MAH SANGIT @ KASMAT

2004617831

ACKNOWLEDGEMENT

بِسْمِ اللَّهِ الرَّحْمَٰنِ الرَّحِيمِ

Bismillah Ar-Rahman Ar-Rahim

(In the name of God, Most Gracious, Most Merciful)

First and foremost I would like to express my highest gratitude to Allah S.W.T, the Almighty for granting me the will and strength to finish this research on time. Without His blessing and permission, this research could not have been completed.

Secondly, I would like to express my gratitude to all my family members, who never fails to give me strength and untiring help during my difficult moments.

I am deeply indebted to my supervisor Puan Nurshahrily Idura Binti Hj. Ramli for her detailed review, constructive criticism and excellent advice during the preparation of this thesis.

I also would like to express my deep and sincere gratitude to my coordinator, Encik Adzhar Bin Abdul Kadir for his guidance, support and constructive comments throughout this research.

Last but not least, I wish to extend my warmest thanks to all of the respondents for the feedback given and not to forget my friends who are always there for me. Thanks for inspiring me in such a means that could not be written in words.

ABSTRACT

Many university information services departments have been gradually extending their wireless local area network (WLAN) coverage in order to provide wireless access to students, staff, and faculty throughout their campuses. There is a growing concern about security risks inherent with a wireless data network, such as loss of confidentiality, loss of integrity and loss of network availability. Numerous flaws have been discovered in WEP, and studies have shown that many wireless LANs are installed with their default settings.

This thesis explores security vulnerabilities in Wireless-Fidelity (Wi-Fi) networks. A thorough description about WLAN and critical security holes is briefly described. First a guide to the necessary equipment and how to set it up as an attack platform is provided. Tools and techniques for measuring IEEE 802.11 WLANs also included giving the reader a greater insight into how computer systems are utilized by hackers, and eventually enable the design of more secure systems. The tools are all open-source software available for download and the techniques all use open-source software and off-the-shelf hardware components.

Later it is demonstrated the tools' utility in monitoring traffic at FTMSK2 building and show how the lack of security may aid a malicious hacker to exploit interesting targets beyond the realm of Wi-Fi. Our tool captures only packets of interest for optional storage and further analysis, thus greatly reducing resource requirements. The preliminary results obtained from these measurements are presented.

TABLE OF CONTENTS