A STUDY OF SECURITY WEAKNESSES OF IEEE 802.11b AND A SOLUTION TO IMPROVE ITS SECURITY

A PROJECT REPORT PRESENTED BY

H.M. ANURA BANDARA

to the Board of Study in Statistics and Computer Science of the

POSTGRADUATE INSTITUTE OF SCIENCE

in partial fulfillment of the requirement
for the award of the degree of

MASTER OF SCIENCE IN COMPUTER SCIENCE

of the

UNIVERSITY OF PERADENIYA

SRI LANKA

2004

A STUDY OF SECURITY WEAKNESSES OF IEEE 802.11b AND A SOLUTION TO IMPROVE IT'S SECURITY

H.M. Anura Bandara

Wireless Local Area Networks (LANs) offer a lot of solutions to network infrastructure problems that were previously unable to be solved by cumbersome wired technologies. Wireless networks are proliferating as the cost of the technology has fallen and as new uses for them are found.

However, Security concerns have become the most visible challenge to Wireless LAN growth in the enterprise market. One of the most insecure features of wireless networks turns out to be its Wired Equivalent Privacy (WEP) protocol that is intended to bring the security level of wireless systems closer to that of wired ones. Unfortunately WEP falls short in accomplishing its security goals.

This report will attempt to identify particular flaws and the corresponding attacks as well as discuss how security principles were violated in the creation of this protocol. The report will also make a few recommendations as to potential improvements that could be made to increase WEP's security level and integrity. Furthermore this paper tries to propose improvements that can be done for the existing 802.11b protocol and introduce a example security protocol for wireless networks.