NATIONAL UNIVERSITY OF SCIENCE AND TECHNOLOGY

FACULTY OF APPLIED SCIENCES

DEPARTMENT OF COMPUTER SCIENCE

MITIGATING SMARTPHONE ROGUE ACCESS POINTS USING BEACON FRAME MANIPULATION

STUDENT NAME: SIQABUKILE SIHWA

STUDENT NUMBER: N011 9185J

NAME OF SUPERVISOR: MR. T. NYATHI

NAME OF CO-SUPERVISOR: MRS. S. S. DUBE

JUNE 2013

This dissertation is submitted to the National University of Science and Technology, Computer Science Department, in partial fulfillment of the requirements of the Master of Science Degree in Computer Science

ABSTRACT

The ubiquity introduced by the advent of smartphones has expounded the need for human beings to remain connected. However, mobile connectivity has also introduced further vulnerabilities associated with the use of wireless technology. The use of wireless devices to access corporate network resources is now part of the norm within corporate environments. When wireless users need to connect to a network they hardly question the source of their connectivity, that is, the wireless network access controller. Network access, including Internet, for mobile and wireless devices is usually facilitated by an access controller which is usually an access point or a wireless router. Mobile phones, particularly smartphones, are equipped with a web browser (micro browser) to allow users to access network resources. Most users take advantage of the mobility aspect, while for some micro browsers are the only option for online access. These harmless looking wireless devices can be a source of major threats if configured to be so. The Internet is awash with mobile apps particularly Android applications that are capable of performing packet sniffing. A combination of these applications installed on a smartphone and the capability of the smartphone to be configured as an access point can present a Smartphone Rogue Access Point (SRAP). An intended intruder can visit an organisation sit at the reception pretending to be waiting for someone and looking like they are playing with their Android mobile phone all the time capturing packets from unsuspecting employees at work. An intruder can sniff the Service Set Identifier (SSID) of the organisation and then deploy her SRAP with the same SSID and unsuspecting employees will connect via her Smartphone Rogue Access Point. Access Points advertise their availability using what is called a beacon frame. The structure of the beacon frame contains some optional fields called parameter sets. In this research paper we propose a solution which restructures this beacon frame to include an Authentic Access Point Value (AAPV). Manipulation of this variable can be used to defend against Rogue Access Points.