International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2022): 7.942

Detection and Mitigation of Rogue Access Points

Hope Makoni

Harare Institute of Technology Zimbabwe

hopemakoni[at]gmail.com

Abstract: ***The discovery and introduction of mobile devices as smartphones has increased the need and appetite for human beings to be connected. The development of social media platforms such as Facebook, Instagram, and WhatsApp, among others, has increased this connection. However the mobile device connectivity has also introduced further vulnerabilities associated with the use wireless technology. Technology advancements have increased the use of wireless devices to access corporate network resources in corporate environments. The wireless technology by mobile phones have been greatly appreciated especially in this COVID pandemic where there is great need to decongest offices according to WHO guidelines without necessarily affecting the productivity of an employee. Network access for mobile and wireless devices including internet is facilitated by an access controller which is usually an access point or wireless router. A beacon frame is used for advertisement by access points. It contains network information needed by a station before it can transmit a frame. Mobile phones can be a big threat if configured to be so as an access point. The technological advancements have also brought a lot of applications on the internet which does packet sniffing. These internet-based applications paired with a smartphone set up as an access point can result in a Smartphone Rogue Access Point. An intruder in an organization can use a smartphone to capture packets from unsuspecting employees at an organization. An intruder can sniff the Service Set Identifier (SSID) of the organization and then deploy her SRAP with same SSID and unsuspecting employees will connect via the SRAC. The report proposes constructing the beacon frame to contain an Authentic Access Point Value in order to identify and minimize RAP in this study (AAPV). The paper should deduce fake access points to safe guard the network.***

Keywords: Rogue access point, wireless security, service set identifier, beacon frame

1.Introduction

A wireless network is a computer network that connects network nodes via wireless data channels. Cell phone networks, wireless local area networks (WLANs), wireless sensor networks, satellite communication networks, and terrestrial microwave networks are all examples of wireless networks. It connects the network's nodes through radio frequency (RF) links. One of the most important standard bodies in the IT sector is the Institute of Electrical and Electronics Engineers. It defines and publishes standards for wired Ethernet, LAN, MAN, Wireless networks. The wireless concept brings increased mobility. It also allow users to access real-time information so they can roam around the organization space without getting disconnected from the network. Significantly the technology has come at the right time with the COVID pandemic that requires a lot on social distancing.

An access point is required to make this technology possible. An access point is a wireless network device that acts as a portal for connecting devices to a local area network. It is a wireless networking radio transceiver that allows appropriately equipped computer or other wireless client device like mobile phone, camera to connect to a network.

While wireless network has brought in some mobility advantage it has equally created serious security challenges that are more difficult to manage compared to the wired network.

Literature Review

1.1 Introduction

The evolution of technology has led to many theories and solutions being undertaken by researchers to find ways to mitigate problems as new hardware and software pose new security threats. It has become known that there are many ways that can be used to detect and eliminate rogue access points in a network with particular interest on wireless networks. These ways encompass a deep understanding of wireless technologies. These technologies include wireless standards, wireless frames, broadcasting access points and many other concepts. Researchers have come with commercial solutions to detect and mitigate RAP. However it argued that hackers have always found a way around them.

1.2 Problem statement

It has been demonstrated that smartphones can be used as access points. Packet sniffing is a recent technique for detecting and observing packet data travelling over a network. Packet sniffing tools are used by network administrators to monitor and validate network traffic, but hackers may use similar tools for malicious purposes. Smartphones as access points and packet sniffing poses a serious threat in the wireless environment. Intruders or hackers may then decide to use smartphones as rogue access points on a network. For example the intruder can set the SSID name which is similar to that of an organization. This will result in users connecting unsuspectingly to the intruder SSID through the smartphone rogue access point. As a result, the user has gained access to the information of the other users. This could mean getting sensitive personal information.

1.3 Proposed Solution

This study presents a method for detecting and preventing rogue smartphone access points in a network. The research should be able to define how a device connecting to an

access point can detect the legitimacy of that access point. Organizations should employ rogue access point detection systems to make sure they are always able to detect unauthorised or illegitimate access points before their personnel or employees connect to them.

Beacon frame manipulation is going to be part of the solution of the smartphone rogue access point.

1.3.1 Objectives

1. To distinguish between legitimate and non-legitimate access points
2. To restructure or manipulate the beacon frame.
3. To prevent stations from associating with unauthorised access points.
4. To identify stations by their Media Access Control (MAC) address.

IEEE 802.11 Standards

One of the most important standard bodies in the IT sector is the Institute of Electrical and Electronics Engineers. It defines and publishes standards for wired Ethernet, LAN, MAN, Wireless networks. Some examples of the most popular IEEE 802.11 standards include:

802.1 – Internetworking
802.3 – Ethernet
802.11 – Wireless networking just to mention but a few.

To make the standards easier to recall and understand, the Wi-Fi Alliance attached generational names to them.
Wireless Security

A wireless computer network's design, implementation, and security are all part of this process. In wireless security passwords do not provide full protection of the network. Anyone with a computer or mobile device within range of the wireless signal can connect to a networking device like a wireless access point or a router without using Wi-Fi security. There are four critical areas of security namely Confidentiality (data hiding), integrity (resistance to alteration), availability (access when needed) and authenticity (verification of sender) according to Clemer 2010. The use of access points (APs) in wireless networks introduces new areas of vulnerability. There are a number of threats to wireless that can turned into attacks subsequently these attacks reflect the vulnerabilities of access points. These vulnerabilities include RAP attacks (AP impersonation).

2.Related Studies

2.1 Round trip analysis

The main difficulty with WI-FI use, especially in public places, is that consumers have no way of knowing whether their devices are directly connected to a real AP. While encryption mechanisms in the data link layer (such as WEP, WPA, and WPA2) have been utilized in many cases, they are vulnerable to MITM attacks. The network administrator can utilize many monitoring tools and techniques, such as timing behaviour observation, to mitigate the effects of an MITM attack. The round trip is most affected by transmission and access delays. This is one technique that uses round trip time (RTT) measurement to detect rogue APs on client-side via mobile networks.

The total latency in a network can be calculated using the round trip time. There have been numerous techniques to measuring round trip time in the literature, some active and some passive; nonetheless, the majority are interested in.

2.2 Commercial defences against RAP

These are conventional software and solutions that are used to detect and mitigate the rogue access points. Firewalls, intrusion detection systems, and Wired Equivalency Protocol are just a few examples (WEP). Examples of technologies include:

i. Wireless Intrusion Prevention System (WIPS)
ii. The radio of a wireless network is monitored by a specific security equipment or an integrated software application. It looks for unauthorised or unexpected activity and frequencies in the radio spectrum within a wireless network's airspace. The technology is capable of detecting and shutting down threatening activities on its own. Modern WIPS categorize known wireless devices using more than just frequency analysis to classifying known wireless devices.
iii. Wireless sniffing tools

Wireless sniffing is the practice of listening in on wireless network communications using special software or hardware. WI-FI sniffers are packet sniffers or network analyzers that capture packet data via wireless networks. These solutions are designed to record and analyze wireless network data in order to provide insights into what is happening in a network at any given time.

2.3 RAP Protection for Commodity Wi-Fi Networks.

This solution combines centralized wired end socket level traffic "fingerprinting" with ubiquitous wireless media surveillance. The former is designed to not only detect various types of rogue applications, but also to keep them from being put in place. However, in order to prevent attackers from turning victim applications into rogue devices, it is also necessary to detect suspicious activities. Socket level traffic fingerprinting is one of the existing ways that helps our system achieve finer granularity in rogue AP detection. Some of the framework's advantages are as follows:

i. It does not involve the usage of specialized hardware or changes to established standards.
ii. The suggested mechanism increases the likelihood of detecting rogue APs, resulting in increased network resilience.
iii. It uses free yet mature software to give a cost-effective solution for improving WI-FI network security.

iv. It can defend the network against attackers who are capable of modifying equipment and circumventing the IEEE 802.11 standard.
v. Its open architecture makes it simple to add new features in the future.

A distributed detection module (DDM) and a centralized detection module are the framework's two main components (CDM). The former can be linked to or installed as small plug-ins on access points, whilst the latter is located at a local network's gateway router. The framework is compatible with WEP and WPA security standards and does not necessitate the use of specialized wireless equipment.

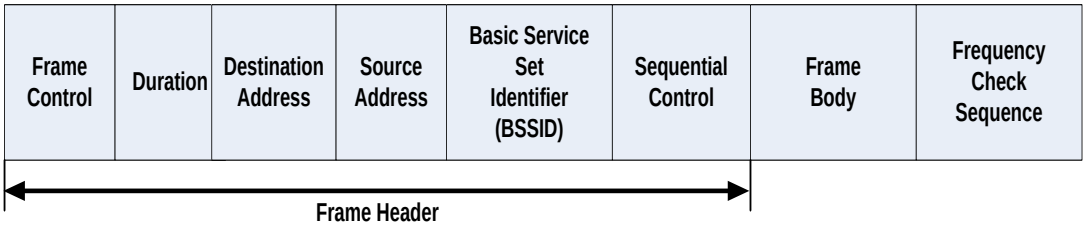
3.Methodology

The corporate world has continued to lament over expensive bandwidth especially here in the third world countries. There has therefore great need to mitigate rogue access points as one of the causes of increased cost of internet in organizations. This section of the research outlines the methodological approach taken in an attempt to solve the above stated problem and describes the methods used to approach the problem.

3.1 Structure of the Beacon Frame

A beacon frame is a management frame in IEEE 802.11-based wireless local area networks. Before a station may transmit a frame, it must first receive network information in the form of beacon frame. They are utilised for both notifying the presence of devices in a WLAN and synchronising devices and services.

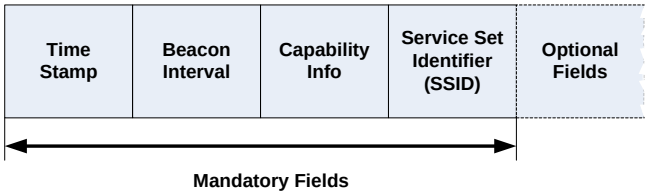
- IEEE 802.11 MAC header
- Body
- Frame check sequence (FCS).



A beacon frame is usually 50 bytes longer. The optional fields of a beacon frame are shown in the diagram above.

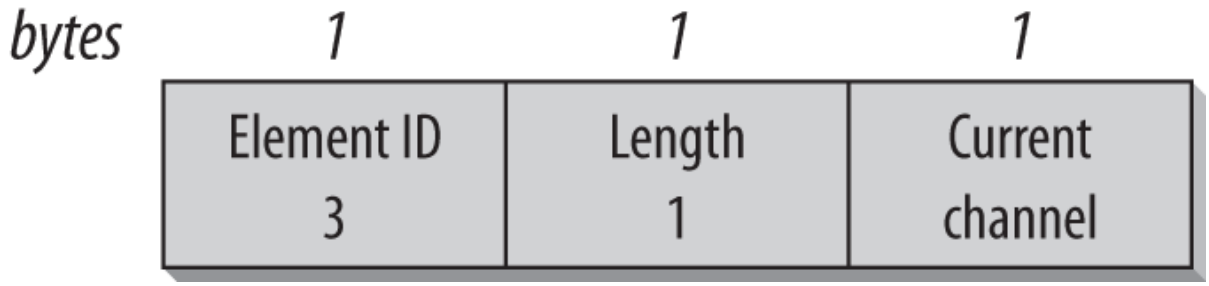
3.1 Information element of the beacon frame

Information element (IE) is made up of three fields namely ID field, Length field and the information field. An information element's general format is shown below.



3.1.2 The DS Parameter Set

The channel number used by the network is the only parameter in direct-sequence 802.11 networks. Because high-rate sequence networks employ the same channels as the low-rate sequence networks, they can use the same parameter set. As demonstrated below, the channel number is represented as a single byte.



3.2 Beacon Frame Manipulation

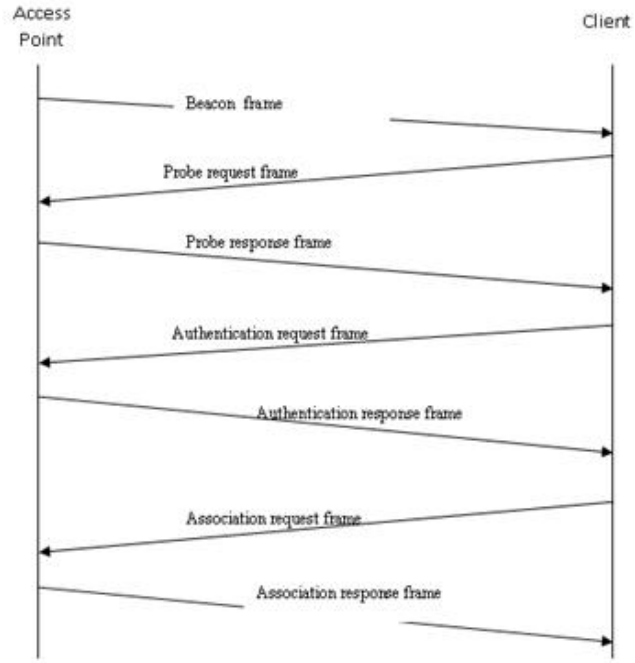
Beacon frame manipulation is a process of editing beacon frames sent by an access point to suit a particular concern. Wireless network security can be improved by using unique beacons. When beacon frames are advertised they do carry values that should be recognised by the clients. If the clients do not have the same values for the beacon as for the sender then there will be no connection. So changing some values can allow only authorised clients to receive the frames.

3.3 How clients connect to an Access Point

The steps or process that should be performed for a network connection between a client and an access point are defined by the 802.11 standard. Below are sequences of steps;

- Client started with active scanning…..
- AP responds with "Probe Response"
- Client sends "Auth Request"
- AP responds with "Auth Response"
- Client sends " Association Response"
- The station sends an "EAPOL- Start" message to the Ap

802.11 wireless clients connect to an access point in managed mode (also called client mode). Once connected, clients can only communicate with the access point; they cannot communicate with other clients. In master mode, wireless access points operate (also known as infrastructure mode)**.**



v

4.Beacon Frame Manipulation Implementation

To preserve the beacon frames, we add an extra Information Element (IE) in each beacon that may be used to validate their authenticity.. The DS parameter set information element of the beacons sent out by hostapd AP is manipulated. Because old clients ignore unknown components, using Information Element provides backward compatibility. It is important to note that this information element is always present in beacon frames and has seven (unused) bits in which we can place our manipulation data hence it has been selected to perform this authentication function. Beacon Frame Manipulation restructures the beacon frame of the access point to include an Authentic Access Point Value (AAPV). The DS Parameter Set has seven (7) unused bits in its length field. The AAPV will be placed on the unused bits of the length field of the DS Parameter Set information element and used to authenticate access points. The access point will then broadcast this special beacon frame and all the clients belonging to the network will seek to connect only to the APs broadcasting these beacons.

4.1 AAPV Polling Implementation on the Client Side

A program that captures beacon packets and searches for the encrypted value (AAPV polling application) is to be designed and coded. This program will be run on the network client machines. When run, the program should check the received beacon frames before connecting. If the captured beacon does not have the AAPV value, it is assumed to be from a rogue access point and connection is dropped while the station continues polling. Otherwise, the client connects to the access point which sent that beacon.

5.Results and Conclusions

The fake access point was created which is called Fake test meant for testing purposes. When the SSID is connected over http it gives the passwords as plain text thereby endangering clients who connect to rogue access points.

By making use of the hostpd DS parameter function the beacon frame is manipulated by adding or inserting an Authentic Access Point Value of "Hovd6" into the length field of the DS parameter set. It starts by checking if the interface mode is set or that the mode configured for hostpd is the mode for the wireless adapter being used in the experiment in this case a tp-link 300 mbps. (This is usually referred to as the "g" mode).

After checking if either is true it returns the element ID of the DS set, which in this experiment is 2. This point to the element ID of the DS parameter set and size of the element which is determined by the length of the eid and max-len. The character array stores the string "HOdv6" which is the value of the AAPV.

5.1 AAPV Client side

This means from the client side there is need to design and code a program that captures beacon packets and check for the encrypted value (AAPV Application). The program is meant to check the received beacon frames before association. If the received beacons do not have the AAPV value it is considered to be from an authorised AP and the association is dropped. Legitimate and illegitimate access points can be distinguished by this polling application. Unauthorised connection is thereby mitigated.

5.3 Conclusion

It is important to note that access points can be used as rogue from both internal and external. It is possible to detect and prevent unauthorised connections by the use of beacon frame manipulation. Clients who do not have the embedded code can never connect to the access point. A beacon frame is the most important wireless frame as it carries all the information about the network.

5.2 Future Work

It is important to also consider other fields that can we can have bit-stuffing like the SSID, BSSID. The SSID is the network name. WLAN must employ the same SSID in order to communicate. The BSSID is always present as a part of the Medium Access Control header in the beacon form is a 6 octet field. The two among others can be considered and see how their weaknesses compare with their strengths

References

[1] N. Agrawal and S. Tapaswi, "Wireless rouge access point detection using shadow honeynet," Science + Business Media New York, Springer, 2015.
[2] V. Roth, W. Polak, E. Rieffel, and T. Turner, "Simple and effective defense against Evil Twin Access Points," WiSec'08, Virginia, USA, 2008.
[3] L. Ma, A. Y. Teymorian, and X. Cheng, "RAP: Protecting commodity Wi-Fi networks from rogue access points," In The fourth international conference on heterogeneous networking for quality, reliability, security and robustness and workshops, ACM, 2007.
[4] http://ettercap.github.io/ettercap/
[5] http://www.wireshark.org/ [8] http://www.snort.org/ [
[6] S. Singh, C. Estan, G. Varghese, and S. Savage, "Automated worm fingerprinting," In Proceedings of the 6th Symposium on Operating Systems Design and Implementation (OSDI), 2004.
[7] J. Levine, R. LaBella, H. Owen, D. Contis, and B. Culve, "The use of honeynet to detect exploited systems across large enterprise networks," In Procee *(1) (PDF) Detection and Mitigation of Rogue Access Point*. Available from: https://www.researchgate.net/publication/320892759_Detection_and_Mitigation_of_Rogue_Access_Point [accessed Dec 20 2021].
[8] Design and Creation SWAL Ozan Satuk and Ismail Kosan 7 Mai 2014
[9] Aboba B., Blunk L., Vollbrecht J., Carlson J. and H. Levkowetz, (2004), **Extensible Authentication Protocol (EAP)**, Copyright (C) The Internet Society (2004). [online] Available from : http://www.ietf.org/rfc/rfc3748.txt, [Accessed: 25 July, 2012]
[10] **Burns J., (2009), Mobile Application Security on Android, 2009, Black Hat, USA**
[11] **CCNA® Wireless Study Guide, (n.d.), Chapter 2: Wireless LAN Standards and Topologies, [online] Available from:** http://www.ciscopress.com/articles/article.aspx?p=1271797, **[**Accessed: 26 July 2012]
[12] Clemmer L, (2012), **Information Security Concepts: Confidentiality, Integrity, Availability, and Authenticity. [**online] Available from: http://www.brighthub.com/computing/smb-security/articles/29153.aspx [Accessed: 18 March 2013]
[13] Cogen D., (2011), **How to root the Samsung Galaxy (all versions)**, December 1, 2011 [online] Available from: http://theunlockr.com/2011/12/01/how-to-root-the-samsung-galaxy--all-versions/, [Accessed: 25 July, 2012]
[14] de Villiers M.R., (2005), **Three approaches as pillars for interpretive Information**
[15] Enck, W. and P. McDaniel, (2008) **Understanding Android's Security Framework,** October 2008, Systems and Internet Infrastructure Securities
[16] Gast, M., (1996), **Wireless Networks. The definitive guide.**
[17] Gast M., (2002), **802.11 Wireless Networks. The definitive Guide,** Chapter 9, pg 223
[18] Geier J., (n.d.), **Beacons Revealed**, [online] Available from: (www.wi-fiplanet.com), [Accessed: 26 July, 2012]
[19] Geier J., (2006), **Identifying Rogue Access Points**, 06 January 2006, [online] Available from: (www.wi-fiplanet.com), [Accessed: 28 July, 2012]
[20] Gopinath K. N, (2009), **WiFi Rogue AP: 5 Ways to (Mis)use It**, 28 July 2009, [online] Available from: http://blog.airtightnetworks.com/wifi-rogue-ap-5-ways-to-%e2%80%9cuse%e2%80%9d-it/ [Accessed: 19 October, 2012]
[21] Gopinath K. N. and H. Chaskar, (2009), **All You Wanted to Know About WiFi Rogue Access Points: A quick reference to Rogue AP security threat, Rogue AP detection and mitigation**, AirTight Networks, www.AirTightNetworks.com
[22] Gupta V. and M. K. Rohil, (2012), **Information Embedding in the IEEE802.11 Beacon Frame**, National Conference on Communication Technologies & its impact on Next Generation Computing CTNGC 2012 Proceedings published by International Journal of Computer Applications® (IJCA)
[23] Hevner A.R., March S.T., Park J. and S. Ram, (2004), **Design science in information systems research,** MIS Quarterly, 28
[24] Hostapd, http://en.hostapd.org/wiki/Hostapd#Jouni_Malinen.27s_hostapd
[25] John A., (2011), **What is rooting on Android, The advantages and disadvantages**
[26] Johnson R., (2012), **Wireless Security Vulnerabilities**, R. J. Computer Consulting, [Online] Available from: http://www.streetdirectory.com/travel_guide/2497/computers_and_the_internet/wireless_security_vulnerabilities.html [Accessed: 16 October, 2012]
[27] Kock N., (n.d.), **Action Research: Its Nature and Relationship to Human Computer Interaction Systems research: development research, action research and grounded theory In: Bishop, J. & Kourie, D. (Eds.)** ***Research for a Changing World***
[28] Kuan C. C.,(2011), **Understanding Wireless Intrusion Prevention Systems**, February 2011,[online] Available from: http://www.networkworld.com/news/tech/2011/021411-wireless-intrusion-prevention.html [Accessed: 22 November, 2012)
[29] Ma .L, Teymonan A. Y. and X. Cheng, (2008), **A Hybrid Rogue Access Point Protection Framework for Commodity Wi-Fi Networks**, IEEE INFOCOM 2008

[30] Mateti P., (2005), **Hacking techniques in wireless networks**, IEEE INFOCOM 2005
[31] Mitchell, Bradley., (nd), **Wireless Standards - 802.11b 802.11a 802.11g and 802.11n The 802.11 family explained,** About.com Guide, [online] Available from: http://compnetworking.about.com/cs/wireless80211/a/aa80211standard.htm, [Accessed: 23 October, 2012]
[32] National Instruments Corporation, (2008), **WLAN - 802.11 a,b,g and n**, Wireless Standards Whitepaper Series, 11 April 2008, [online] Available from: http://www.ni.com/white-paper/7131/en
[33] Nobel R., Lovison F., Riesen F., Vangrunderbeek E. and F Ziliotto., (2012), **Planning and Designing 802.11 Wireless Technologies**, Cisco Press, May 16 2012, [online] Available from: http://www.ciscopress.com/articles/article.asp?p=1873028&seqNum=3, [Accessed: 23 October 2012]
[34] O'Brien R., (2001), **An Overview of the Methodological Approach of Action Research,** [online] Available from: http://www.web.ca/robien/papers/arfinal.html [Accessed 27 February, 2013]
[35] Parthip, S., (2012), **802.11 Sniffer Capture Analysis - Management Frames and Open Auth**, [online] Available from: https://supportforums.cisco.com/docs/DOC-24651, [Accessed: 27 July 2012]
[36] Potter, B., (07/22/2007). **Wireless Intrusion Detection**. Retrieved April 22,2013, from http://www.itsec.gov.cn/webportal/download/88.pdf
[37] Rapoport R.N, (1970), **Three dilemmas in action research**, Human Relations, 23, 499-513.
[38] Ruiz V., (2008), **GNU/Linux Basic Operating System**,
[39] Shetty, Sachin., Song, Min., Ma, Liran., (2007), **Rogue Access Point Detection by Analyzing Network Traffic Characteristics**, IEEE Conference Publications
[40] Singh S. K., (2004), **Computer Aided Process Control**, PHI Learning Pvt Ltd (1 August 2004)
[41] Sommerville, I., (1996), **Software Engineering**, Fifth Edition, Addison Wesley, Reading, MA,
[42] Spamlaws, (nd), **Types of Wireless Network Attacks: RAP**, [online] available from < http://www.spamlaws.com/rap-attacks.html> [Accessed: 2 July, 2012]
[43] Stallings W., (2006), **Cryptography and Network Security,** 5th Edition, Prentice Hall.
[44] The MathWorks Inc, (nd), **IEEE 802.11 WLAN – Beacon Frame**, Available from www.mathworks.com. (Accessed 24 January 2013)
[45] Thomas, O.,and C. van Oosten, (2007), **Information Security Magazine.** October 2007
[46] Timofte J., (2004), **Wireless Intrusion Prevention Systems**. Revista *Informatica Economică* nr.3(47)/2008
[47] Vanderauwera J., Bruinsma L., Carlier S. and T. Hassanmahomed, (2009), **Compromising Wireless Security with Android**, 31 December 2009.
[48] Vaishnavi V. K. and W Kuechler Jr., (2007), **Design Science Research Methods and Patterns: Innovating Information and Communication Technology**, Taylor and Francis(2007)
[49] Walls J., Widmeyer G.R. and O. A. El Sawy, (1992), **Building an Information System Design Theory for Vigilant EIS**, Information Systems Research, 3 (1), 36-59.
[50] Wexler J., (November 15, 2004), **Do we really need RAP protection?**,. (http://www.networkworld.com/newsletters/wireless/index.html)
[51] XGC Software, (2005), **What is GCC?,** http://www.xgc.com/misc/tech_note_0.htm
[52] Zhu, H., Zhang, Y., Hou, Q. and S. Greenwood, (nd), **Application of Hazard Analysis to Quality Modelling**, Proc. Of IEEE COMPSAC 2002, Oxford, UK