# Wireless Networks Security in Jordan: A Field Study

Ahmad S. Mashhour[1]&Zakaria Saleh[2]

[1]IS Dept, University of Bahrain
Mashhour_ahmad@yahoo.com
[2]MIS Dept, Yarmouk University, Jordan
Drzaatreh@aim.com

***ABSTRACT***

*The potential of wireless communications, has resulted in a wide expand of wireless networks. However, the vulnerabilities and threats that wireless networks are subjectedto resulted in higher risk for unauthorized users to access the computer networks.This research evaluates the deployed Wireless Network in Jordan as well as the use of the security setting of the systems and equipment used. Caution will be taken to avoid network access as only existence of the network is sought. Wardriving involve the use of freeware tools such as NetStumbler, or Kismet, which was originally developed to be used for helping network administrators make their systems more secure. Thestudy is carried out through field evaluation of the Wireless Local Area Network (WLAN)in light of the use of Wardriving, and proposessome measures that can be taken to improve securityof the wireless network by the users.*

***KEY WORDS***

*Security, Wardriving, Wireless Local Area Network (WLAN), Wired Equivalent Privacy (WEP).*

## 1. INTRODUCTION

Wireless networks have evolved rapidly in the last few years due to the developments of new wireless standards and cost-effective wireless hardware. This has led to widespread adoption of the technology in home and small businesses. With the growth of wireless networking, security is the main weakness of the whole wireless system, which resulted in improper uses of network resources. The deployment of wireless networks can potentially make private networks subject to public use. As wireless access increases, security becomes an even more important issue.
Wardriving is a common practice at which an individual equipped with electronic devices capable for wireless access, wanders in the streets with the aim to locate wireless networks for access to the Internet, either house-based or corporate-based wireless networks, map their existence, and hack them. It is using a laptop equipped with awireless LAN adapter or smart mobile phone, and randomly driving around looking for unsecured wireless LANs. This paper provides evidence through a study of how users configure and protect their wireless Internet access points (APs). Wireless networks require a Service Set Identifier (SSID),which represents the name of the wireless network, whichdistinguishes between the wireless networks and offers the ability for the users to identify and use them. If configured to auto-connect, is practical for a client adapter toconnect to an AP, orsimply click on the SSID of a selected AP (SSIDs can be found in the client's list of available wireless networks under "Network and Sharing Center"). This research will evaluate the wireless networks in Jordan, and see if the networks are protected from such actions.

## 2. BACKGROUND

Wireless networking is one of growing technologies being deployed today, from home networks to corporate level wireless networks. Businesses as well as general users are trying to take advantage of the benefits which wireless networking providessuch ascost effectiveness, flexibility and easy to use.Howeverthere has been an increasing demand for greater security in businesses.Most network threats come from the ignorance of users, the inactive attitudes of corporations, and the improper implementation of security features by wireless devices manufacturers[1]. The lack ofsufficient learning materials and or support for users' wireless connections at home, as well as public places wireless access poses a critical threat to the systems as well as the information these systems host. Some researchers suggest that with the increased demand for wireless connections, comes a growing concern about the security and protectionthe wireless networks [2-5, 20].For more details about wireless network problems and solution see[6-10, 25,26].

As communication technology advances, there is a good amount of Wi-Fi networks in populated areas in Jordan. Finding many of these networks does not take much efforts when using some of the tools that can be obtained from the Internet.To automate the searching for wireless access points, many software tools have been developed that allows for detecting Wireless Local Area Networks (WLANs). The Software is available for free on the Internet [11], (e.g. NetStumbler for Windows, SWScanner for Linux and KisMac for Macintosh). This softwarewasmainlydesigned and used to insure that a wireless network is set up properly and as it is intended for,or be used to locatepoor coverage within a WLAN, detect any networks interference, and discover any unapproved "rogue" access points in the company's network. Regrettably, wireless networks are susceptible to attacks if not protected properly[11, 24].Therefore, this toolcan be used by hackers to obtain access to open or inadequately secured networks, in the commonly known"Wardriving" access.We believe that Wardriving is an activity that many can participate in with low cost and minimal technical expertise [22].

## 3. SIGNIFICANCE OF THE STUDY AND RESEARCH OBJECTIVES

Achieving a perfectly acceptable wireless network security performance has not been very easy. The significant of this research is that no other similar testing was conducted in Jordanto provide an evaluation of the wireless networks security in any Jordanian city. Conducting this research is essential because it tries to identifythe wireless network security issues that thesewidely deployed networks maybe facing. The findings of this research should be considered by network owners and the Wireless Internet Service Providers (WISP) to review the recommendations regarding the threats facing their networks, and then, decide the suitable security measures needed to be taken to reduce and/or possibly eliminate these threats.

Because there are so many vulnerabilities associated with wireless networks, there are a lot of tools available to penetration testers for exploiting them. It is important for security professionals (including security auditors) to be familiar with the tools used to spoof MAC addresses, deauthenticateclients from the network, capture traffic, re-inject traffic, and crack Wired Equivalent Privacy (WEP) or the WLAN Protected Access (WPA). The proper use of these skills will help a security auditor perform an effective WLAN penetration test. It is essential for the system security teams running the wires networks in Jordan to have a complete understanding of the existing wireless network threats andhow these threats can be exploited, to determine the

appropriate defense techniques to prevent attacks or unauthorized access to their wireless networks.

### 3.1 Research Questions:

The research answers questions about the security status of wireless networks in Jordan, and how to achieve acceptable wireless security performance. These questions are:

i) Wireless networks are inherently insecure. Can this be actually true about Wireless networks in Jordan?
ii) What are the current approaches used for protecting wireless network and preventing unauthorized users to access the network?
iii) What is the level of threats facing the wireless networks in Jordan?

## 4. WARDRIVING OVERVIEW

Wardriving is not a complex hack. A hacker can workthrough the wireless security issues, and wouldeasily understand most of them. Exploiting the wireless networks requires simply a moving vehicle, a portable device equipped with an 802.11 wireless LAN adapter (see figure 1). NetStumbler is the most favored utility among the entire available ones. In light of that, this research will mainly concentrate on the use of NetStumbler. In addition, nearly allWiFi enabled Windows devices can blindly scan for hotspots by running NetStumbler[23].

It is not always that someone has to do anything deliberately to connect to someone else's network. Some client adapters will hook up with any WAP (Wireless access points) that is non-WEP (Wired Equivalent Privacy), within range, given enough time to perform a DHCP (*Dynamic Host Configuration Protocol)*transaction. NetStumbler is Windows application that scans for wireless networks and generates the information about the network such as SSID, encryption status. In addition, NetStumblercan provide GPS coordinates[12, 23].However, in legitimate operation, NetStumbleris mainly assigned Rogue AP detection[13]. It only monitors theparts of data that the AP makes public. It has no means for reverse-engineering passwords, sniffing packets, or connecting to a network (protected or otherwise). Client adapters can be configured auto-connect to an AP once detected.TheStumbler program does not log any stations with SSIDs other than onessensed by the omnidirectional antenna.

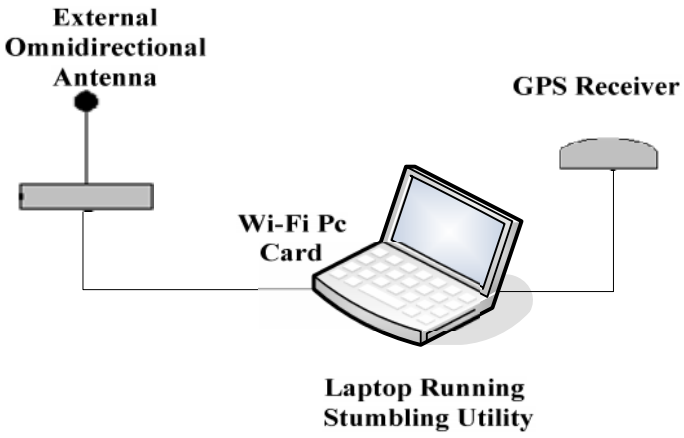


Figure 1: Wardriving Diagram

## 4.1 Wireless Local Area Networks Security Issues

The first launches implementations of wireless technology were very slow, offering only about 1 to 2 Mbps (Megabits per second) speeds for transmission and suffered from lack of reliability and week security, so it did not succeed well in the market[3,8,14].Information security professionals as well as researchers have declared WEP security algorithm to be inappropriate for securing wireless communication [4,12,15-16].WLAN depends on cryptographic methods to enable security. In this research, WEPand WLAN security mechanisms assumed to be providing the security as defined by IEEE 802.11 Standards [17]. WEP was the leading protocol developed for Wi-Fi to provide encryption mechanism that should enable privacy through the means of user's authentication. However, it is a publically known fact that WEP was not able to secure the wireless networks. WPA was suggested by the Wi-Fi Alliance to replace WEP as a new cryptographic protocol. In addition, WLAN suffered from a number of security vulnerabilities, where the seriousness of them was acknowledgedvery late[18].

Using NetStumbler, the tool sends out Probe Requests with pseudo random data included in its request and listens for the response from the access point. The war-driving program then captures the response and then displays the details of the packet for the user's information. The 802.11 header includes information about the network encryption status as well as the SSID. Therefore, this information can be collected by a war-driving program like NetStumbler(see figure 2). In certain ways, information systems breachshares similar concepts with fingerprints [19].Thus, for security and privacy reasons, all actual monitoring data was deleted from figure 2, and only the user interface is being displayed.

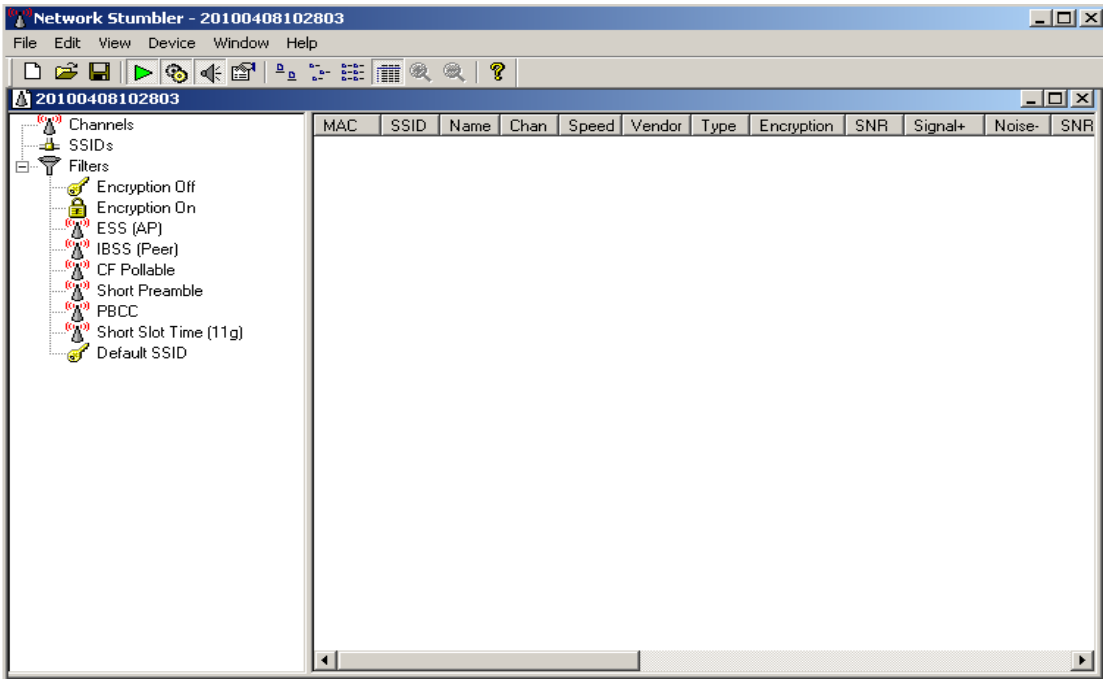


Figure 2: *NetStumbler*user interface

## 5. TEST SETUP AND FINDINGS

To answer the research question, a test was conducted to collect data about existing wireless networks in different Jordanian areas. The tests were simply conducted using a moving vehicle, a laptop equipped with an 802.11 wireless LAN adapter, using NetStumbler as a tool to its request and listens for the response from the access point. The driving was done in two major cities in Jordan; Amman and Irbid. During the test: 1) Thecontents the tested network was not examined or accessed.2) No attemptswere made to effectthe integrity of any system by altering, adding, modifying, or deleting anything on any network, and 3) No actual use the network's was made to connect to the Internet or surf the Web or anything similar activities. The process used to test the networks does not constitute "access" of the company's network (what we did constitutes to the State v. Allen case that took place in an Americancourt of law, which is frequently referred towhen there is a questionregarding an illegal networkaccess [18].

Table 1: Network vulnerability

| Type of Networks | Number of Tested Networks | Type Average |
|---|---|---|
| Vulnerable Network | 132 | 79.52% |
| Protected Network | 34 | 20.48% |
| Total | 166 | 100.00% |

The outcomes of this test reveal that there exist insecure wireless networks in people's homes and in small, medium and large corporationsas well. Because of these insecure deployments, penetration test was conducted to determine the security status on some organizations' wireless

network, as well as home users' systems, to determine if companies and users have deployed their wireless network in a secure fashion. As for the first research question, the majority of the tested wireless networks (79.52%) are unsecured and the security of the networks needs to be further enhanced to protect those networks. The results of the evaluations are displayed in table 1 and figure 3.

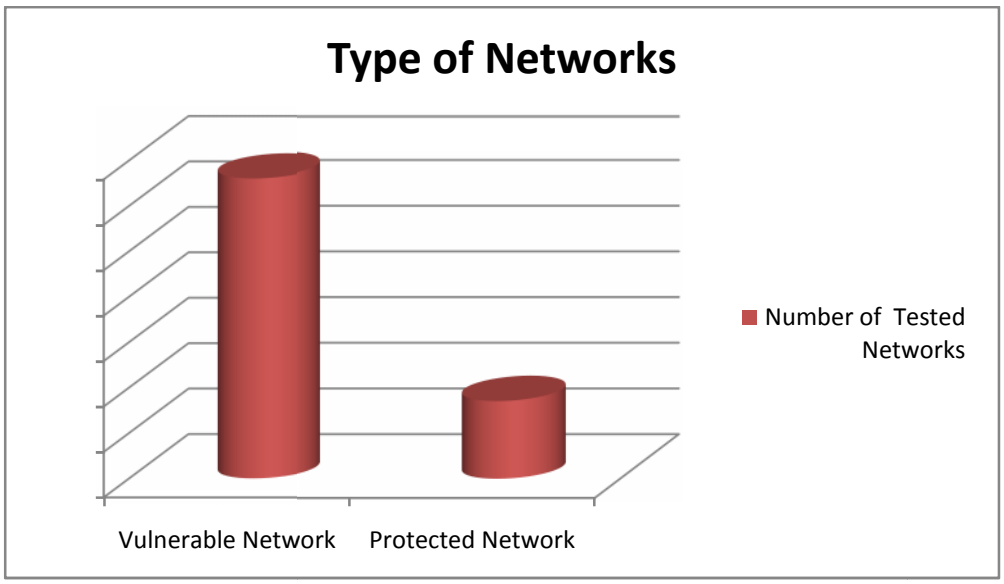


Figure 3: Network vulnerability

As for the current approaches used for protecting wireless network and preventing unauthorized users to access the network, 68.67% of the networks are found to be using low level protection, and 11.45% are not applying any encryption (see table 2 and figure 4).

Table 2: Level Of protection

| Type of Encryption | Number of Tested Networks | Type Average |
|---|---|---|
| Low Level Protection | 114 | 68.67% |
| High Level Protection | 33 | 19.88% |
| No Encryption | 19 | 11.45% |
| Total | 166 | 100.00% |

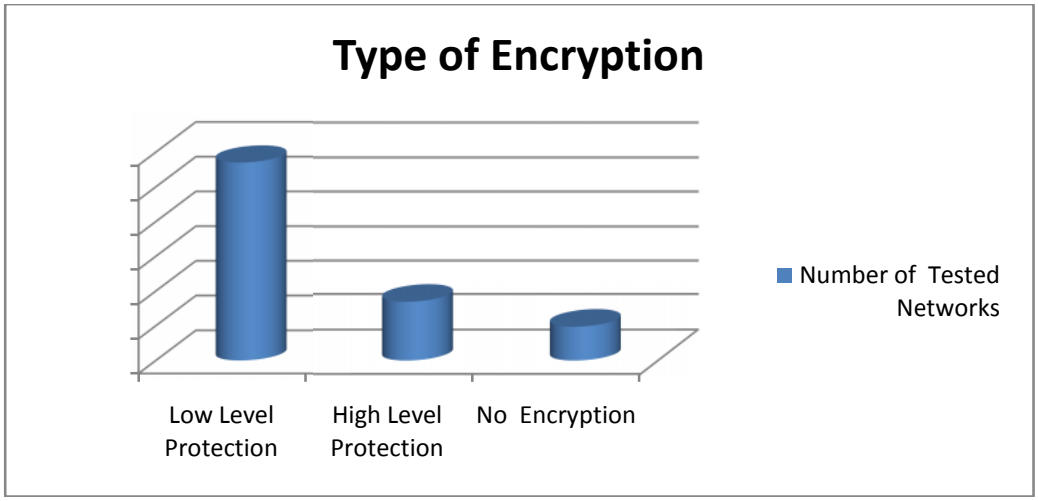


Figure 4: Level Of protection

To improve the security of the wireless network, the SSID needs to be changed to a different name than the default. We have discovered that 92.17% of the networks are using default SSID (see table 3 and figure 5). As for the level of threats facing the wireless networks in Jordan, by default all client devices receive SSID broadcasts from all WAPs that are within range. Being able to receive the SSID, the SSID was broadcasted from all WAPs were tested, when attackers have developed sophisticated and effective techniques to exploit wireless systems.

Table 3: SSID Configuration

| SSID | Number of Tested Networks | Type Average |
|---|---|---|
| Default SSID | 153 | 92.17% |
| Changed SSID | 13 | 7.83% |
| Total | 166 | 100.00% |

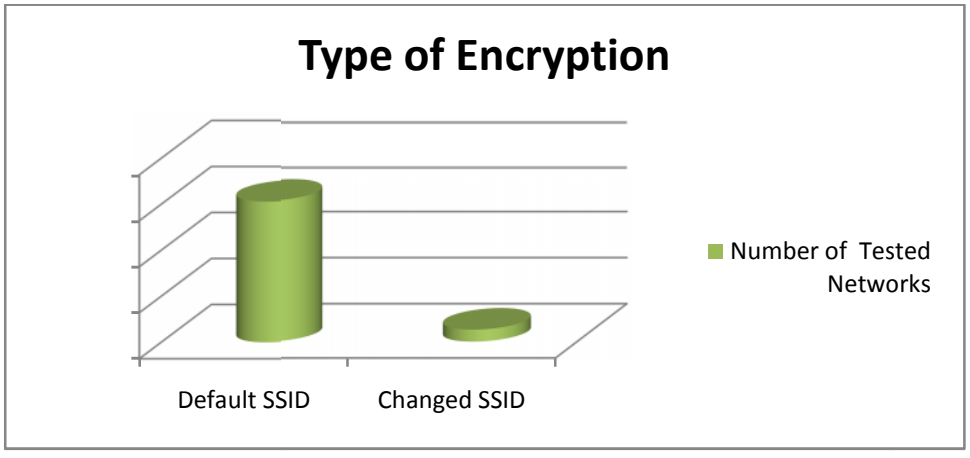


Figure 5: SSID Configuration

# 6. RECOMMENDATIONSFOR SECURING WIRLESS SYSTEMS

With the growth of wireless communication and wireless networks, more advanced and effective techniques were implemented to exploit the wireless communication systems of all types. Using these tools allows an attacker to access the internal networks and client systems, and often it can be used to bypass the deployed security defenses system like intrusion detection systems.In light of that, there will be a need to have a periodic audit of the wireless networks, and to try and assess the wireless networks, evaluate the systems' vulnerabilities, and analyze the security risks associated with it. In addition, there will be a need to continue monitoring the network to identify rogue WAPs and signal leakage. In addition, frequent inspection and adjustment of WAPs is recommended to minimize the damage that WAP physical security issues may cause. This will provide good information on the security of the wireless network. Using suitable assessment tools and techniques to identify and expose threats that wireless network may be faced with, and then use the proper defensive responses to protect wireless network resources.

To protect wireless network from Wardriving and hackers in general, protecting measures must be well planned and thoroughly maintained and updated. In order to prevent the security issues reported in this study, when implementing the wireless network, a security evaluation and risk analysis must be conducted thoroughly. Once the network is fully implemented and operational, there will be a need to have a security policies specific to the use of the wireless network. In addition, a security audit will be essential to help identify and prevent the system's vulnerabilities.

By default all client devices receive SSID broadcasts from all WAPs that are within range. One of the recommend ways to ensuring that a system will not be exposed to wardrivers is to disable SSID broadcasting by the WAPs.Although tools such as Kismet can still discover a non- SSID broadcasting wireless network many would be intruders will however be disappointed by a lack of SSID broadcasts. Therefore, once the wireless devices are installed and set to go, there will be a need to change all the manufacturer default settings. These settings include administrator name and password, network ID and name, methods of authentication, broadcastingsetting, the default encryption methods and pre-shared keys, and the method used to connection to the network [21].
MAC Address filtering can also be applied to enhance security. MAC Address filtering can be implemented to improve authentication of the wireless enabled device. When using MAC Address filtering, a table is developed and a list of all permitted MAC Addresses can be entered into the table, where the default setting would be to deny access to all unlistedwireless systems.
Access to the wireless network must be controlledusing access point authentication, and all traffic transmitted through the wireless networks should be first encrypted using one of the strong and advanced methods of encryption like WPA2. If a default encryption is Wired Equivalent Protection (WEP) then the default 40-bit key is used. WEP is broadly publicized for a number of weaknesses, one of which is the key size. Therefore there will be a need to use 128-bit encryption key to further strengthen the encryption. As a result,it will take significantly longer time for intruders to crack.

To help reduce exposure, depending on the size of the network, the network can be subdivided into several and smaller subnets. This will not only enhance the security of the system, but will alsohelp delivergreater overall network performance as well as higher efficiency.We recommend for those organizations that exemplified system weakness to conduct a network readiness assessments to check for signal leakage from the internal wireless network to the publically

accessible areas, an also look for leakage from the publically accessible ad hoc wireless networks into their network.

It seems that a good number of users are either not aware of the severe outcome of thepotential security breaches, they may believe that their wireless connections are protected. Corporations also underestimate the potential dangers. Therefore urgent action is needed in light of the recent high-profile security breaches.Most threats come from the ignorance of users, the inactive attitudes of corporations, and the improper implementation of security features by wireless devices manufacturers.

# 7. CONCLUSION

The potential of wireless communications combined with high risk for unauthorized users to access the computer networks, dictated the need for higher measures to be taken for protectingsensitive information and insure the privacy of the user and protect theassets of the company. However, it seems that a good number of users are either not aware of the severe outcome of the potential security breaches, they may believe that their wireless connections are protected. This was a clear indication by leaving factory default settings in some network devices. Leavingthese network devices with the default setting will definitely permit other unauthorized users to gains access to the systems.

In this research we evaluate the Wireless Network environment in Jordan in view of the use of the WLAN equipment and found that a high percent of WLAN are not secured, the research also provides some recommendations and best practices regarding the security of WLAN networks.

# REFERENCES


[1] Loo, A. W. (2010), "Illusion of Wireless Security*", Advances in Computers*, Volume 79, 2010, Pages 119-167.

[2] Bulbul, H. I., Batmaz, I., and Ozel, M. (2008). "Wireless network security: comparison of WEP (Wired Equivalent Privacy) mechanism, WPA (Wi-Fi Protected Access) and RSN (Robust Security Network) security protocols". First international conference on Forensic applications and techniques in telecommunications, information, and multimedia and workshop(e-Forensics '08), ICST, Brussels, Belgium, Belgium, Article 9, 6 pages.

[3] Miller, B., and Hamilton, B. (2002). "Issues in Wireless Security (WEP, WPA & 802.11i)". The 18th Annual Computer Security Applications Conference, 11 December 2002.

[4] Welch, D. J., and Sayles, A. (2010). "A Survey of 802.11a Wireless Security Threats and Security Mechanisms",A Technical Report to the Army G6, Internet Technology and Secured Transactions (ICITST).

[5] Zadig, Sean M., and Tejay, G. (2010). "Securing IS assets through hacker deterrence: A case study", In the proceedings of conference on Anti-Phishing Working Groups 2nd Annual eCrime Researchers Summit-eCrime, pp. 1-7, 2010.

[6] Amouzegar, H., Jafar, M. T, and Hidaji, A. N. (2009). "A New SOA Security Model to Protect Against Web Competitive Intelligence Attacks by Software Agents*". International Journal of Information Security and Privacy*, pp. 18-28.

[7] Balfanz, D., Durfee, G., Grinter, R. E., Smetters, D. K. and Stewart, P. (2004). "Network-in-a-Box: How to set up a secure wireless network in under a minute". In *Proceedings of the 13th conference on USENIX Security Symposium* - Volume 13 (SSYM'04), USENIX Association, Berkeley, CA, USA, pp. 15-15.

[8] Ho, J. T., Dearman, D., Truong, K. N. (2010). "Improving Users' Security Choices on Home Wireless Networks"*ACM*, Article 12, 12 pages. DOI=10.1145/1837110.1837126. [online]. Available: http://doi.acm.org/10.1145/1837110.1837126

[9] Hurley, C., Rogers, R., Thornton, F., and Connelly, D. (2007). *WarDriving and Wireless Penetration Testing*, Syngress Publishing.

[10] Grinter, R. E., Edwards, W. K., Newman, Mark W., and Ducheneaut, N. (2005)."The work to make a home network work".Ninth conference on European Conference on Computer Supported Cooperative Work, p.469-488, September 18-22, 2005, Paris, France.
[11] Vladimirov, A., Gavrilenko, K. V., Mikhailovsky, A. (2004). Wifoo: The Secrets of Wireless Hacking. – Addison Wesley.
[12] Borisov, N., Goldberg, I., and Wagner, D. (2008). "Security of the WEP Algorithm, UC Berkeley". [online]. Available: http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html.
[13] Fluhrer, S., Mantin, I., and Shamir, A. (2001). "Weaknesses in the key scheduling algorithm of RC4". Lecture Notes in Computer Science, vol. 2259, pp. 1-24. [online]. Available: http://www.crypto.com/papers/others/rc4 ksaproc.pdf.
[14] Berghel, H. (2004). "Wireless Infidelity I: Wardriving", *Communications of the ACM* – CACM, Vol. 47, no. 9, pp.2.
[15] Burell, J. (2002)." Wireless Local Area Networking: Security Assessment and Countermeasures: IEEE 802.11 Wireless Networks".[Online].[online]. Available:telecom.gmu.edu/publications/Jim-Burrell-December-2002.pdf.
[16] Burell, J. (2002). "Wireless Local Area Networking: Security Assessment and Countermeasures: IEEE 802.11 Wireless Networks". [online]. Available: telecom.gmu.edu/publications/Jim-Burrell-December-2002.pdf.
[17] IEEE Standards Association. Std 802.11, 1999, Edition (R2003), 2003. [online]. Available: http://standards.ieee.org/getieee802/download/802.11-1999.pdf.
[18] Thomas, M. (2004). "Network Security First-Step".*Cisco Press*, Indiana, USA. ISBN: 1-58720-099-6. p315.
[19] Cisco Networking Academy Program (2004). *Fundamentals of Wireless LANs*. Indianapolis, Indiana: Cisco Press.
[20] Ryan, P. (2004). "War, Peace, or Stalemate: Wargames, Wardialing, Wardriving, and the Emerging Market for Hacker Ethics". *Virginia Journal of Law & Technology* vol. 9. No.(7).
[21] TechDoc (2008). Securing Business against War Driving. [online]. Available:http://webupon.com/security/securing-business-against-war-driving.
[22] Etter, A. (2002). "A Guide to Wardriving and Detecting Wardrivers". SANS Institute, document number GSEC Version: 1.4b.
[23] Martin, J. (2005).The Art of casual WiFi hacking. [online]. Available:www.infosecwriter.com/pdf/WiFi%20hacking%20article.pdf.
[24] Verizon (2010). Data Breach Investigations Report. "A study conducted by the Verizon Business RISK team in cooperation with the United States Secret Service".
[25] Taylor, A. S. and Swan, L., (2005). "Artful systems in the home". In *Proceedings of the SIGCHI conference on Human factors in computing systems* (CHI '05). ACM, New York, NY, USA, 641-650. DOI=10.1145/1054972.1055060 http://doi.acm.org/10.1145/1054972.1055060.
[26] Office of the Privacy Commissioner of Canada, (2007, September 24). "Report of an Investigation into the Security, Collection and Retention of Personal Information, TJX Companies Inc./Winners Merchant International L.P". [Online]. Available: http://www.oipc.ab.ca/ims/client/upload/Investigation%20Report%20P2007_IR_0061. Pdf.

**AUTHORS BIO**

**Dr. Ahmad Mashhour**earned his PhD in Information Systems from University of London (LSE), UK, 1989. He is currently an associate professor at the University of Bahrain, Information System Dept. He also joined other universities in the middle East for some time including University of Qatar, and YarmoukUniversity of Jordan. His research interest includes Simulation modeling and Analysis, e-business and e-learning.
Email Address: mashhour_ahmad@yahoo.com

**Dr. ZakariaSaleh** is an AssociateProfessor at the MIS department, Yarnouk University. Before joining the Yarmouk University faculty team, Dr. Saleh was an engineer in the automotive industry, where he worked on the design and development of electronic control systems for Constructions and Agricultural Equipment, and he led the design and development of web based Fleet Management System, which was successfully launched by Case Corporation of the US in the year 2001.