Open Journal of Business and Management, 2014, 2, 292-297
Published Online October 2014 in SciRes. http://www.scirp.org/journal/ojbm
http://dx.doi.org/10.4236/ojbm.2014.24034

Wireless Network Security Threats and Mitigation—A Survey

Mohammad Bajwa

Healthcare Systems Management, Metropolitan College of New York, New York, USA
Email: mibajwa@hotmail.com

Received 28 June 2014; revised 29 July 2014; accepted 18 August 2014

Abstract

Mobile technology and wireless networking are the latest technologies finding their way in the US healthcare system. One major concern about the use of wireless technology in healthcare is that the signals traveling through the atmosphere are apt to be eavesdropped and intercepted. On the other hand HIPAA and HITECH Acts hold the healthcare organizations and their associates responsible for the health information security and privacy of the patients and the public. A survey was conducted to learn about the views of the health information technology (HIT) managers and users to gauge their gravity of concern about this issue. Majority of the interviewees expressed their reservations about the use of mobile technology till it becomes perfect and foolproof security can be enforced.

Keywords

Mobile Technology, Wireless Networking, HIPAA, HITECH, HIT

1. Introduction

Being a significant part of our lives, wireless communication is one of the most commonly discussed topics. It has changed the way we live, work and communicate. Wireless technology implies sending and receiving messages by electromagnetic (EM) signals, principally radio waves, through the atmosphere (wirelessly) instead of the guided or wired media using copper or fiber optic cables [1]. Having emerged only in 1980s, it is the latest, yet the least understood, communication technology [2]. Its use in businesses, education and healthcare is gaining rapid momentum and includes e-Banking, e-Financing, e-Commerce, distance learning, and mobile health (mHealth) [3].

Wireless communication technology has several advantages of being mobile and easy to install and maintain. However, being still in infancy, it is far from perfect; both protocols and services are still in the process of de-

How to cite this paper: Bajwa, M. (2014) Wireless Network Security Threats and Mitigation—A Survey. *Open Journal of Business and Management*, **2**, 292-297. http://dx.doi.org/10.4236/ojbm.2014.24034

velopment. Like unique potentials, it has unique flaws, most significant being interception, and hence data and identity theft [4] [5]. Standard organizations and forums have not yet plugged the existing security holes. Because of these vulnerabilities, wireless technology has not gained the anticipated momentum and remained restricted to voice communication and non-sensitive data transmission till recently when considerable attention has been diverted to it because of its use in business and healthcare fields.

This report provides an overview of the wireless technologies and then reviews results of a survey conducted to gain firsthand information on the use status of wireless devices, technologies in place, and security threats and their mitigation measures.

2. Wireless Technologies

The most common two technologies deployed for wireless networks are Infrared and Radio Frequency [6].

2.1. Infrared Transmission

In Infrared (IR), data are transmitted as flashes or ON/OF light in binary code to represent 1 s and 0 s. IR devices could send direct and diffused transmission referred to as *line-of-sight* and *reflected* transmission. Since IR is not subject to interference by other transmission signals and cannot penetrate objects like walls, it is considered safe against eavesdropping. However, this advantage quickly translates into disadvantage as the IR devices have narrow coverage in terms of distance. Significant less speed of IR transmission than the wired networks is yet another disadvantage. Because of these limitations IR transmissions are normally restricted to special applications like data transfers between mobile devices and computers and printers.

2.2. Radio Transmission

Being highly effective, it is the most common means of communication in today's wireless networks. Here the data are transmitted as electromagnetic energy that travels as radio waves called Radio Frequency (RF). The technology is based on passing a current through a wire creating magnetic waves which radiate away from the source as radio waves in all directions. They not only can travel long distances, but can also penetrate non-metallic objects, like walls. This advantage of RF becomes disadvantage as the signals can be accessed by the hackers.

Data through radio waves can be transmitted in several ways [1].

Frequency Modulation (FM): by varying frequency of wave or number of times that a wave completes cycles in one second.

Amplitude Modulation (AM): by varying height of each wave through application of differential voltage.

Phase modulation (PM): by varying starting points of wave cycles.

Digital Modulation (DM): by varying binary signals; the binary signals vary between positive and negative voltages but unlike continuous analog wave have start and stop points.

Amplitude Shift Keying (ASK): a binary technique similar to AM except that height of the wave can be changed to represent 1 and 0; 1 is represented by positive voltage and 0 by none.

Frequency Shift Keying (FSK): similar to FM but a binary technique that changes frequency of the carrier signal into start and stop.

Phase Shift Keying (PSK): identical to PM except that signals start and stop.

Spread Spectrum: transmits signals across several frequencies (broad band) rendering data both availability faster and secure.

3. Research Methodology

Since the author is not associated with any organization where original research would have been possible, it was decided to conduct telephonic interviews of some experts in the wireless network security to find information on:

- Current wireless network implementation status.
- Types of wireless networks under implementation.
- Wireless network security threats.
- Wireless network security mitigation measures.

To gain responses to these queries, two security experts, one network administrator and one wireless network user were interviewed. They represented an ISP, healthcare facility, an academic institution and a telecommuter.

Following were the interviewees:

- Mr. Mathoor Iqbal, CCIE, Senior Engineer, Verizon Corporation, Virginia (ISP).
- Mr. Michael Serrano, MS MCSE, Director of Information Technology, East Harlem Council for Human Services, Inc. New York (Healthcare).
- Mr. John Smith, MCSE, Interboro College, New York (Academic/Education).
- Ms. Salma Shafique, Deputy Director, Services and General Administration, US Government, Washington DC. (User).

Their general and specific views are summarized below.

4. Wireless Network Implementation Status

Implementation of wireless networks for data communication in medium to large organizations is still not common, according to the interviewees, for several reasons including but not limited to the following:

4.1. Wireless Technology Is Still in Infancy

Wireless network technology is yet far from being perfect and still evolving though rapidly during the last five years, both in terms of standards and devices. Such circumstances warrant updating hardware and software continuously that progressively adds to network's fixed and operational costs. Such organizations thus would wait till the wireless technology matures and investments last longer.

4.2. Wireless Networks Are Still Very Insecure

Large to medium organizations are very uncertain about security of their information being transmitted wirelessly which is prone to interception. Hence, wireless communication is restricted to insensitive data and mostly intended for Internet usage (e-mail, instant messaging, text messaging), web browsing and downloading software.

Almost all educational institutions are replacing the wired networks with the wireless networks on their campuses and class rooms for academic purposes to provide easy access, and save on the initial cost and maintenance. These networks provide hotspots for internet access where security is not an issue. However, their sensitive networks, containing students' academic, financial and administrative information, are still wired.

New York City has implemented wireless networks for city-dwellers to facilitate web browsing and e-mailing from anywhere within the city as well as access company's networks by authorized users.

4.3. Wireless Networks Are Slow Compared to Wired Networks

Notebook computers still cost twice that of desktop computers and are much slower, especially when the activities involve graphics and large corporate files. There is also now a tendency to move the smart phones, iPads and other mobile devices to local wireless networks whenever in the vicinity to save on the data package costs.

4.4. Wireless Devices Are Still Expensive

As mentioned above mobile devices that can perform the functions of desktop computers (good quality laptops) still cost twice or thrice the price of desktop computers. Additionally they are apt to misplacement and stealing thus losing the sensitive data.

5. Types of Wireless Networks under Implementation

Wireless networks are being implemented both as WLANs (Wireless Local Area Networks) and CANs (Campus Area Networks) and even WANs (Wide Area Networks). The most common implementations are:

5.1. WLANS and CANs/WANs Using Desk Top Computers with Wireless Network Interface Cards

This implementation reduces expense both on wires and their installations. Such implementation is more common in the changing environments and temporary business/academic sites, such as training workshops, seminars, conferences, temporary offices and computer labs.

5.2. Wireless Network Use through Mobile Devices

This implementation is almost negligible in business organizations but is a common practice in the academic environments. Many organizations now allow their employees to work from home and provide them with laptops preinstalled with VPN (Virtual Private Network) for secure connection to their organizational networks over the Internet. Many government organizations in Washing DC have adopted this technique to save travel cost and avoid traffic congestions. The employees work 2 - 3 days from home and attend offices for 2 days or only the special meetings (Salma Shafique). Online education such as MOOCs (massive open online courses) makes tremendous use of this technology (John Smith). However, business organizations still do not allow connection to their internal networks through any other mobile device, such as smart phones or iPads.

5.3. Internet and Web Connections with Smart Phones and Other Web-Enabled Devices

This implementation is becoming rapidly popular, especially during travel and out of office hours, but is still restricted to exchange servers for e-mails and extranets for some routine information, with no access to internal networks. Mobile devices are still not being used for business purposes and remain confined to cyber navigation, weather updates, stock trading, and other general information (Mathoor Iqbal).

6. Wireless Network Applications

Most common wireless network applications remain restricted to internet use, web browsing, and instant/text messaging. Educational use being the most common allows access to college/university resources for viewing grades and schedules, downloading educational materials, such as eBooks, and downloading and uploading assignments (John Smith). The author has extensively used the notebook computer for attending both asynchronous and synchronous classes with Strayer University and for the other aforementioned purposes. Recently the use of mobile devices (smart phone, iPads, and laptops) for videoconferencing and virtual meetings has become a norm.

Commercial use of mobile devices except for laptops, such as eCommerce, and eFinance, is still rare primarily due to security reasons.

7. Wireless Networks Security Threats

All the interviewees commented that:

1. By and large the common security threat remains vulnerability of wireless transmission to interception and impersonation aimed at stealing identity information and its subsequent exploitation to gain advantage on behalf of the genuine user. The most feared identity elements are social security number, credit card information, and mobile device identification and user location.
2. Physical theft of mobile devices, being small and expensive, is yet another restraint on their use. Mobile devices like notebooks can contain sensitive and valuable information and when lost can fall in wrong hands.
3. Unsolicited products or service advertisement when used in conjunction with the Internet. Other Internet security threats common to wired network remain inherent to wireless networks, like spam, worms, viruses, Phishing, Pharming, etc. also.
4. Loss of wireless connection to the AP results in data loss, and its repeated transmission not only reduces network capacity but also increases its vulnerability to interception.

All interviewees remarked that wireless networks are 3 - 4 times more risky. Their enterprise-wide security expense is also of the same order compared to wired networks being 3% - 5% of the overall IT budget. According to one security consultant (Mathoor Iqbal), 90% of the wireless network users express their security concern as compared to 10% for the wired networks and this fear is on the rise with increased use of wireless networks and devices.

Recent instances of wired network security breaches and infections (spyware, adware, viruses, worms, Trojan horses, etc.), he (MathoorIqbal) quotes has further increased the wireless network security concerns for business use.

8. Wireless Network Security Measures

In the absence of any strong standard, some companies are cobbling together some technologies, living with gaps, and hoping for the best. Wired Equivalent Privacy (WEP) and encryption are supposed to make wireless networks resistant to hackers like the wired networks. WEP, however, relies on unchanged encryption key (MathoorIqbal) and hence is prone to be cracked. He emphasizes stronger authentication along with WEP. In the meantime Microsoft and Cisco have come up with their own security protocols for use in their devices. Healthcare organizations (Michael Serrano) which implemented wireless networks up to 93% of their requirements have become disappointed with the discovery of security holes in WEP. Despite these security challenges a growing number of organizations are adopting Wi-Fi technology, especially the educational and healthcare institutions. Almost 30% - 40% of medium and large healthcare organizations are currently testing this technology and about 10% - 15% is expected to adopt once their pilot project completes successfully (Michael Serrano).

Another approach to wireless network security is the use of VPN (MathoorIqbal) that can provide strong encryption via the Internet Protocol Security (IPSec) that uses public keys. This implementation, however, needs installation of VPN software and hardware and most handheld devices do not support VPN.

Internet Engineering Task Force (IETF) is now in the process of developing an Internet-Access Point Protocol (IAPP) that would enable seamless authentication and fast handshake between wireless devices. Wi-Fi Alliance is also certifying a draft of the wireless security certification, known as Wi-Fi Protected Access (WPA). Extensions of EAP (Extensible Authentication Protocol) to wireless network security are also under consideration by the IETF.

In summary, according to the interviewees, the wireless network security measures are as follows:

- Place wireless devices behind routed infrastructure.
- Pick up a random SSID that provides no information about the network.
- Set APs to “closed network”.
- Set strong authentication method.
- Have broadcast key rotated frequently.
- Set session to timeout every 10 minute.
- Always define and implement a security policy.
- Centrally enforce and monitor security.
- Enforce power-on password.
- Encrypt sensitive data.
- Use personal firewalls.
- Use Anti-Virus
- Backup data regularly.

The interviewees further concluded that:

- Mobile wireless applications present tremendous opportunity, but security remains the critical issue.
- Best time for addressing mobile security is from the start of the wireless network infrastructure as it can be less expensive than adding it later.
- Preventing wireless security breaches is less expensive than the cost of recovery and downtime.
- Understand threats and vulnerabilities and assess their business impact and appropriately apply security measures.

9. Conclusions

Having emerged only in 1980s, wireless technology is still in infancy. Both the wireless products and the standards are still evolving. However, during a short span of time the wireless technology has shown a great potential as being simple, cheap, easy to install, maintain and troubleshoot. Despite these advantages some gaps yet need to be bridged, and most significant of these is the wireless transmission security. The most common wireless technologies are radio frequency (RF) and infrared (IR). Since these wireless signals travel through the atmospheric medium, they have open and diffuse boundaries prone to interception. Views of the interviewed security experts confirm these apprehensions that wireless technology is still far from perfect, insecure, slower, and even expansive.

Current wireless security threats include eavesdropping, communication jamming, DoS, interception, data injection and modification, man-in-the-middle, rouge client and APs. Security measures against these threats constitute stronger authentication, privacy and integrity technologies, such as WEP, TKIP, EAP-TLS, Cisco EAP-LEAP, and VPN.

Formulation of security policies, their implementation and monitoring is the first defense against security threats, followed by the education of the users to develop security awareness and thus a security culture in the organization.

References

[1] Dean, T. (2012) Network + Guide to Networks. Course Technology.

[2] Bajwa, M.I. (2004) Wireless Network Security. Directed Study Project, Strayer University, Herndon.

[3] Krohn, R. and Metcalf, D. (2012) mHealth. Health Information and Management Systems Society—HIMSS.

[4] Hideki, I. (2006) Wireless Communication Security. Artechhouse, Boston/London.

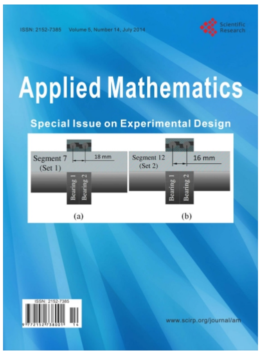
[5] Caludia, T. (2012) Management and Security of Health Information on Mobile Devices. American Health Information Management Association (AHIMA).

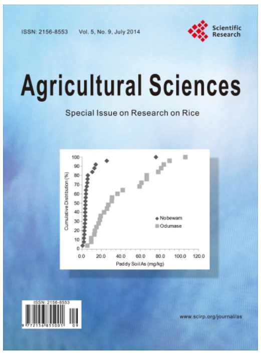
[6] Labiod, H., Afifi, H. and De Santis, C. (2007) Wi-Fi, Bluetooth, Zigbee, and Wimax. Springer, Berlin. http://dx.doi.org/10.1007/978-1-4020-5397-9

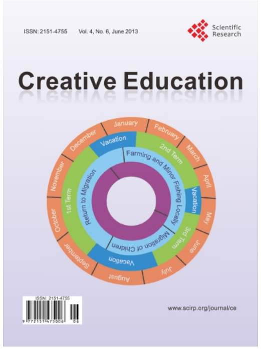
Advances in Bioscience and Biotechnology

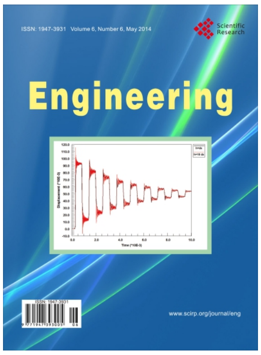
American Journal of Analytical Chemistry

American Journal of Plant Sciences
Special Issue on Photosynthesis

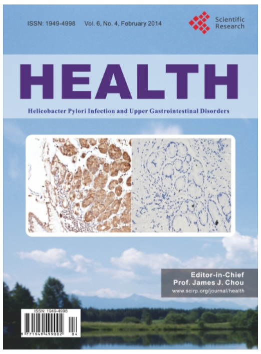

Applied Mathematics
Special Issue on Experimental Design


Agricultural Sciences
Special Issue on Research on Rice


Creative Education

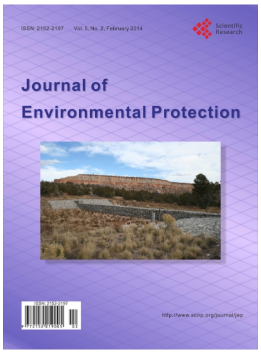

Engineering

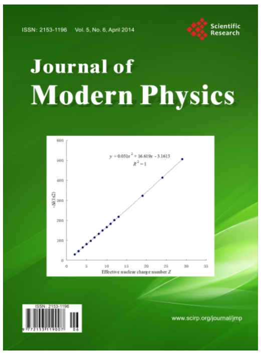
Food and Nutrition Sciences


HEALTH
Helicobacter Pylori Infection and Upper Gastrointestinal Disorders
Editor-in-Chief
Prof. James J. Chou

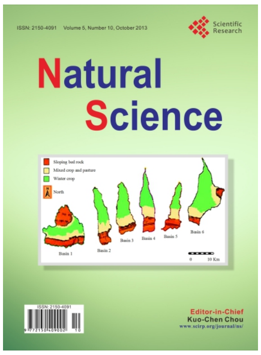
Journal of Computer and Communications

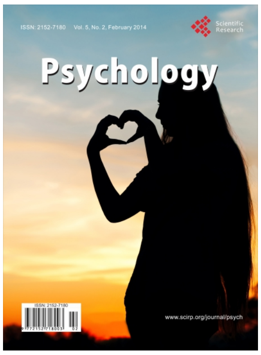
Journal of Cancer Therapy
Special Issue on Bone Tumor Research


Journal of Environmental Protection


Journal of Modern Physics

Modern Economy


Natural Science
Editor-in-Chief
Kuo-Chen Chou


Psychology