Spring 2008

Wireless Handheld Solution for the Gaming Industry

Mo T. Hyder
Regis University

Running head: Wireless Handheld Solution for the Gaming Industry

WIRELESS HANDHELD SOLUTION FOR THE GAMING INDUSTRY

Mo T. Hyder

Regis University

School for Professional Studies

Master of Science in Computer Information Technology

Abstract

One of the essential elements of success in the gaming industry is the requirement of providing exceptional customer service. Technology plays a significant role in bringing state of the art solutions that enhance the overall customer experience. Currently a guest must go through multiple steps and a variety of departments to simply resolve issues with their player accounts (loyalty programs), update customer profiles, book hotel and restaurant reservations, sign up for promotions, etc. In order to effectively take care of these customers in both a timely and efficient manner, a wireless handheld device is needed that employees can carry with them to resolve and address these concerns. This project is aimed at identifying the proper wireless infrastructure for the gaming environment and also the wireless handheld device, such as an Ultra Mobile PC (UMPC) to effectively and efficiently take care of customers.

Acknowledgement

I would like to acknowledge the assistance of Professor Erik Moore and Professor Archer for their guidance in making this project possible. Acknowledgement is also given to William Gustafson for providing his expertise in the gaming industry. Finally, I am very grateful to my wife Marcy for her patience in allowing me to spend countless hours tethered to a computer to complete this project. In addition, a big thank you to all my five boys who remained patient and helped their mom while I was busy working on the project.

Project Paper Revision/Change History Tracking

Revision	Date	Description
1.0	10.5.2007	Initial Draft
2.0	11.25.2007	Revision/APA Formatting
3.0	01.25.2008	Revision/Structural/APA

Table of Contents

List of Tables

List of Figures

Wireless Handheld Solution for the Gaming Industry

The gaming industry needs a state of the art solution to enhance customer experience. This study analyzes the capabilities of both a wireless infrastructure and a mobile handheld device to bring efficiencies to accomplish this goal.

Chapter 1: Introduction

1.1 Thesis Statement

The gaming industry requires a reliable communications infrastructure to remain competitive in the market place. With the proliferation and ubiquity of the Internet and enhancements in technology, the guests have come to expect immediate access to services or problem resolution. Services can range from making room, show or restaurant reservations from anywhere on the property. Problems can include issues with guest accounts, their accumulated points, and dissatisfaction with a service. All these requirements are fueling the need for an infrastructure that will allow employees and guests access to services located on the network anywhere, anytime throughout the entire property. The technology that is currently deployed includes legacy systems consisting of a variety of Operating System platforms, such as RS6000, Windows 2000, AS400, etc. The solution provides access to each of these platforms through the implementation of a wireless infrastructure and handheld devices.

1.2 Statement of the Problem

The gaming industry in the Quad Cities has been in existence since 1991. It started out as riverboat gaming and Iowa was one of the first states to introduce casino style gaming outside of Las Vegas and New Jersey.

The market place consists of three casinos that fiercely compete for market share. Additionally, with new entrants in the surrounding market place, the Quad Cities casinos have seen their share erode. The newer facilities are taking a jump-start by deploying new technologies geared towards enhancing overall customer experience. The existing facilities in the Quad Cities have always been well know for delivering exceptional customer service and being at the forefront of introducing cutting edge technology.

Today’s gaming customers are technically savvy and customer service is critical. To satisfy the immediate gratification need of today’s customer, the gaming industry must design systems that will address specific requirements. Currently, customers must leave their particular experience, such as slot machine, table games, to make a hotel reservation, address issues with their points, and check on their restaurant reservations. To make matters worse, they most often have to stand in long lines at guest service centers to have their needs taken care of. This process is very inefficient and adversely impacts the gaming establishments’ ability to generate revenues effectively. Our internal estimates show that each customer contributes $50 towards their gaming experience during an average trip. The average trip, which is defined as the time spent for the gaming experience lasts about two hours. Maximizing the time spent during the gaming experience directly translates into a greater share of the revenues for the company. Gaming companies as a matter of policy are always looking for opportunities to increase the customer’s gaming experience time to drive more revenues.

According to Hickey (2007), their research indicates that mobile security was one of the biggest concerns by IT professionals today, especially when it was connected to a network. Therefore, it is expected that deploying a new wireless and mobile computing solution will present challenges, such as security and reliability. Regardless, there are several new wireless technologies including mobile devices with a wide array of features that can help the gaming industry gain more efficiency and provide better customer experience.

1.3 Project Goals or Objective

One of the major goals of this project is to identify the various types of wireless technologies and mobile devices that can be deployed by the gaming industry. The industry is highly regulated and both integrity and credibility of the systems installed is not only critical but imperative as well. Gaming regulations are enforced through the legislatively enacted Iowa Code 99F, which defines the guidelines for the code enforcement by the Iowa Racing and Gaming Commission (IRGC). The IRGC has the obligation and ultimate authority to enforce the regulations at each of the gaming establishments. The gaming industry is held to high level of standards, including ethics, public perception, credibility and integrity. Every new system deployment or upgrades go through the highest and stringent level of scrutiny to ensure compliance with the code. Therefore, security issues in a wireless and mobile computing environment will be given significant consideration in addition to the management of these technologies.

1.4 Barriers or Issues

As previously mentioned, the gaming industry is highly regulated (Iowa Code 99F) and the final wireless infrastructure and the mobile device will be subject to rigorous regulatory testing and scrutiny. The industry will have to re-write Standard Operating Procedures (SOPs) to address the new technology and provide any special reports when the mobile devices interface with slot and table games systems.

1.5 Assumptions and Limitations

As later described in section 2.4 of this research, technology plays a critical role in enhancing guest experiences. Similarly, this project will also help the gaming industry attract new customers and give them the ability to maintain current customers and build a loyal customer base. The wireless network with handheld computing will increase employee efficiency and increased customer satisfaction, resulting in greater share of the revenues for the industry. For instance, instead of the guest leaving their gaming experience to redeem their accumulated points, or make restaurant and hotel reservations, increases in gaming revenue will be derived from customers because they will be able to conduct all these transactions while spending more time at the gaming devices without having to leave their gaming experience.

This project will also allow for seamless integration with other existing wireless systems across the property. For instance, a wireless infrastructure currently exists in our high-end steak restaurant. The guests are provided with a small device that allows them to key in their overall experience following their meals. The big advantage of tying in the wireless infrastructure is that it will allow the customer feedback to be immediately incorporated into their account and alert the guest service representatives of any issues. It will also provide a secure access to the existing property management systems that include hotel reservations, guest services, restaurant reservations, slot and table games systems and other back-end administrative systems. Security will be accomplished by applying both risk and vulnerability assessments as detailed in sections 4.2 and 4.3 of this analysis.

The primary objective of this study was to demonstrate how the wireless handheld technology could bring benefits to the gaming industry. Additionally, as previously discussed, the wireless infrastructure is vulnerable to security risks and the study takes into consideration any potential downtime. Therefore, security in the wireless environment is analyzed in great detail in the later sections of this project.

1.6 Scope of Project

The wireless handheld device will be deployed based on the requirements as described by the gaming industry. In addition to compiling best practices, interviews were conducted to seek expert advice from both gaming industry officials and customers. The interviews were conducted by our marketing department while the customers were present at the establishment. Similarly, both phone and in-person interviews were conducted with industry professionals. The results were compiled and utilized to develop specific features that the customers expressed would enhance the gaming experience. The main emphasis of this project will be to develop a wireless infrastructure and identify a mobile computing device. Also, all other existing systems, especially the ones for the hotel and restaurant will require slight modifications by adding the necessary wireless hardware to connect to the wireless infrastructure. It is anticipated that some training will be required to help the employees navigate the handheld device to take care of the customers needs immediately.

1.7 Project Outline or Deliverables

Following is the project outline:

- Introduction to Wireless
- Wireless Technologies
- Wireless Services
- Wireless Security
- Wireless Management
- Mobile Computing Device

1.8 Definition of Terms

Both the Glossary and Acronyms are represented in different tables. The purpose is to give the reader better understanding of certain industry specific words and terminology. In some cases, an expanded definition was provided for the benefit of the reader.

Table 1: Glossary of Terms

Terms	Definition
802.11a	The 802.11a utilizes the same protocols as 802.11g operating at 5GHz with transfer speeds of 54 Mbps. Compared to 802.11b and 802.11g networks, which use DSSS or FHSS schemes, the 802.11a operates in the OFDM, which due to higher frequency results in lower range. This lower range results in increased costs as more access points are required and because of the different RF bands it cannot operate with other 802.11a or 802.11g devices. However, this issue is resolved by using either client adapters or a multi-node 802.11a/b/g access point.
802.11g	The 802.11g utilizes the 2.4GHz ISM band with transfer speeds of 54Mbps using the OFDM and is backward compatible with 802.11b devices. The 802.11g is also known as 54g™.
802.11b	The 802.11b also known as the 802.11 High-Rate (HR) is the most widely used WLAN, using the DSSS scheme; it operates in the 2.4GHz ISM band, with transfer speeds of 11 Mbps. As a Wi-Fi, transfers data at 1 Mbps, 2 Mbps, 5.5 Mbps and 11 Mbps rates.

Access Point (AP)	The Access Point provides both a connection to a wired network and serves as a ‘hub’ to the wireless realm. Within a radio coverage area, an AP establishes the Basic Service Set (BSS) or SSID, which allows it to both associate and authenticate with the particular access point.
Ad-Hoc Mode	It is a mode where wireless devices communicate with each other. They do so by discovering each other in a WLAN and communicate in a peer-to-peer configuration.
AES (Advanced Encryption Standard)	The US Government and organizations use the AES to protect sensitive data during transmission by using a symmetric encryption algorithm. The US National Institute of Standards and Technology (NIST) approved this encryption, which is based on Rijndael algorithm, to be used for the Federal Information Processing Standard (FIPS-197). For 802.11 WLAN securities, AES will be become a part of the 802.11i standard.
Authentication	Before granting access to individuals to networks or systems, authentication is the process that identifies the individuals and ensures that they are who they claim to be.
DSSS (Direct Sequence Spread Spectrum)	The DSSS is a data transmission scheme which is usually used in 802.111b Wireless LAN environments. A radio transmitter is used and data is transmitted between fixed ranges of frequency bands. However, when 802.11a/g is not operating in 802.11b mode then the OFDM scheme is used.
EAP (Extensible Authentication Protocol)	EAP is an authentication protocol and a key element for mutual authentication to a secured wireless network. EAP come in the following forms: MD5, LEAP, TLS, TTLS and Protected EAP (PEAP).
IEEE (Institute of Electrical and Electronics Engineers)	It is a membership-based organization made up of scientists, engineers belonging to electronics or a related field. The IEEE is responsible for creating both the wireless LAN and the 802 series protocols. More information about the organization can be found at http://www.ieee.org.
Infrastructure Mode	The Infrastructure Mode is the alternative to the Ad-Hoc Mode and uses a central access point to transmit data. It allows communication from a wired network by managing the wireless traffic within a coverage area that is set up by the BSS.
LAN (Local Area Network)	A LAN is a communications network that provides computing services to users that are located within a geographical area and with a specified distance. Similarly, a Wireless LAN allows devices to communicate within a medium without the use of cables.
Medium	The MAC operates in Layer 2 of the OSI Model and determines and controls

Access Control (MAC)	the transmission of data over a communications link. IEEE defines the 802.11 standards on how MAC shares the addressing, wireless medium, the formats of the packets, and how errors are both detected and recovered.
Protocol	Also known as a set of communication rules and exists at all 7 layers of the OSI Model. Protocols define the formats of data packets and addressing schemes utilized.
Radio Frequency (RF)	Refers to frequencies that operate between 30KHz and 300 GHz. Many wireless devices such as cordless or cell phones, satellite communications, radio and television broadcasts, etc., operate in the RF spectrum.
Repeater	A device that regenerates signals to amplify or extend the range of a wired or wireless device. A signal is regenerated when it is received, re-timed, re-shaped or re-transmitted.
SNMP (Simple Network Management Protocol)	SNMP is a client-server protocol and operates over both the UDP/IP and the Ethernet. Version 3 is the only one considered secure. In a SNMP configuration, the networked devices are allowed to be managed by the network management station, by retrieving the Management Information Base (MIB) data by the agents.
SSID (Service Set Identity)	The SSID is the name given to the Basic Service Set and is made up of 32 case sensitive character. SSID can distinguish between the wireless networks and an access point can have more than one SSID as well. SSID is not secure and can be sniffed.
WEP (Wired Equivalent Privacy)	In order to be defined, WEP requires between one and four keys and is both a protocol for authentication and encryption in the 802.11 WLAN environments. For data to be exchanged and encrypted, both the client and the access point must have a common WEP key. WEP is vulnerable to security threats ad is not considered secure as it only encrypts data while it is being transmitted over the air.
Wi-Fi (Wireless Fidelity)	Wi-Fi devices are carried under the Wi-Fi logo and are considered compatible and interoperable with 802.11 standards.
Wireless	Any device that can communicate with each other without being connected via cable. Some of the most common transmission protocols include: RF, laser and IrDA.
Wireless Gateway	Enterprise Wireless Gateways (EWG) provides both traffic control and security in wireless networks. It is accomplished through authentication, Role Based Access Control (RBAC), data encryption, bandwidth management, traffic shaping etc.

Workgroup Bridge (WBG)	A WBG is a device, that without using a wireless bridge, through an access point, bridges a wired network to another wirelessly.
WPA (Wi-Fi Protected Access)	The Wi-Fi Alliance introduced the new WPA, which uses TKIP and MIC for authentication and encryption scheme during 2006. For WEP's RC4 based encryption, the TKIP and MIC schemes use both dynamic and unique keys. WPA is considered relatively secure in WLAN deployments where extremely sensitive information is not transmitted.

Note: The terms & definitions were adapted from Certified Wireless Network Professionals. (2006). In WLAN Glossary. Retrieved November 20, 2007 from http://www.lever.co.uk/wlan-glossary.html#Decibel

Chapter 2: Review of Literature and Research

The research for this project was conducted using several methods. The most common method was utilizing the Internet and literature published in gaming publications, such as the Casino Journal, Casino Executive and the Slot Manager. Some of the websites reviewed for research and validate theory included: Wireless LAN Association, Converge! Network Digest, IEEE 802.11™ Wireless Local Area Network, InfoWorld, Network World, Inc., WLAN Forum and other sites mentioned in the 'reference' section of this project. Other methods, as previously mentioned included informal interviews with department heads to identify specific needs for their respective areas.

2.1 Literature Overview and Research

Most of the research for this project was completed in several ways. Interviews were conducted with gaming industry experts to clearly understand the scope and need for the device. Additionally, literature on wireless, mobile computing and security was reviewed by reading variety of books, research papers, and Blogs. The Internet played a key role in delivering good resources for this type of research.

2.2 Initial Areas of Uncertainty

At the beginning of the project it was unclear as to which type of wireless standard would work best to make the handheld wireless device operable. I also had a lot of uncertainty about the mobile computing device that would be used and effectively work in the wireless infrastructure that did not exist before. The scalability of the various components was unknown as well.

2.3 Literature and Research Specific to the Project

After considerable research of industry publications, such as the Casino Journal, Casino Executive and other sources, such as the Internet, I found Cellular Specialties, Inc. as the only vendor that has made claims to successfully designing and implementing the wireless solution in the gaming industry. Unlike our scope of the project that actually seeks to deploy a handheld device to enhance customer experience; CSI's solution is geared, towards the management of slot machines information wirelessly.

2.4 Contribution the Project will make to the Industry

The wireless handheld device will provide significant contributions to the industry while improving guest experience. Employees will be able to provide services to guests that include, making room, show or restaurant reservations from anywhere on the property. Additionally, any guests concerns can be addressed relatively quickly because the employees will have access to guest information. Employees will be able to access any of the restaurant, hotel, and account information using this device anywhere on the property. However, as discussed in later sections, employees will be made aware of the wireless connectivity limitations due to signal reliability, coverage, dropouts and connectivity.

Technological advances have been important for the growth of the gaming industry. Some of the milestones include when the bill acceptors replaced tokens (coin). Eliminating coin made it possible to eliminate heavy coin counting machines in the cashiers vault. Another more recent break through adding to the efficiencies of the customers experience while reducing costs to the company was the ability to download credits directly to the machine. Historically, customers would bring in their direct mail coupon; go the club to have it validated then to the cashiers' windows to collect cash before inserting it into the machine. Now we simply send the customer a letter in the mail or email letting them know that a cash offer is waiting for them at the machine. The customers, at their convenience, come to the property and insert their player's club loyalty cards in their favorite slot machine and the cash is immediately downloaded for them to enjoy the gaming experience. This technology alone has saved the gaming industry millions of dollars allowing us to focus on delivering the customer experience. Similarly, since the guest will not have to leave their gaming experience to address their needs and as previously referenced in section 1.2, it means additional time by the guests to enjoy their experience, which translates into more revenue for the property.

Chapter 3: Deploying the Wireless Infrastructure

This chapter is included as a survey of the current state of the wireless and mobile technologies for individuals in the gaming industry. The various types of wireless networks, security requirements, technologies, services and various other protocols will be described in great detail.

3.1 What is Wireless?

According to Virginia Polytechnic Institute and State University, (2002), wireless is described as a standard that allow connection between products without using wires or electrical conductors. Wireless means that an electromagnetic wave is traveling through the air while transmitting between two locations. Wireless operates using different frequencies and exhibits a variety of properties. For example, microwaves, starting out with GHz have a tendency to deflect off from objects and walls. Conversely, MHz on the other hand is low frequency wave and can travel through objects and waves. When applications are being developed, wireless system designers select the frequencies that are conducive for their project.

According to White (2005), wireless technology continues to emerge and is used for many applications, such as: computer networking; providing security; making data acquisition and remote monitoring possible and providing access control solutions. It is often considered to be a telecommunications solution. Wireless solutions are becoming very popular with hand-held devices, such as Personal Digital Assistants (PDA’s), Radio Frequency Modems (RF), Wireless Local Area Networks (WLANs), Infrared (IR) ports on devices, Radio Frequency Identification Technology (RFID). Also with the proliferation of wireless technologies, most companies are choosing to convert their wire tethered applications wireless.

3.2 Types of Wireless Networks

As noted by the Greyfriars Consulting Group (2004), there are several different types of wireless networks, which add value and play an important part in providing wireless solutions. These various types are described as follows:

A. **WLANS: Wireless Local Area Networks**

   They provide wireless connectivity to networks within a limited coverage area. WLANs are typically used in solutions that require high data transfer rates in a limited coverage area. WLAN spectrum is unregulated and anyone can create a Wireless network solution with complete control over the coverage area. They are popular and allow users to form a network or gain access to the Internet in a local area, such as hospitals, library, office, university, including hotspots. WLANs are also referred to as 802.11 and Wi-Fi standards.

B. **WPANS: Wireless Personal Area Networks**

   They provide wireless connectivity to networks with a limited distance of approximately 10 meters. WPANs allow devices to be connected to each other wirelessly such as to a printer or a cell phone using Infra Red (IR) and Bluetooth (IEEE 802.15) technologies. WPANs work independent of defined or pre-existing networks and connections are made using an ad-hoc connection to devices that are within range. The exception is IR, which technically requires a direct line of sight.

C. WMANS: Wireless Metropolitan Area Networks

Wireless Metropolitan Area Networks are utilized within a metropolitan area by connecting several networks. They connect building without having the expense of installing expensive fiber cabling.

D. WWANS: Wireless Wide Area Networks

Wireless Wide Area Networks can be managed over large areas through antenna sites, satellites and can cover countries or cities. They started out by providing cellular services followed up by data services. WWANS are also referred to as second-generation networks. They are a great solution for providing team members with access to the corporate network remotely. Some typical standard WWAN terms include; GSM/GPRS and 1XRTT, which are completely incompatible with each other.

3.3 Network of Choice: Wireless Local Area Network (WLAN)

For the purpose of this study, I selected the Wireless Local Area Network (WLAN) solution as it provides wireless connectivity to networks within a limited coverage area and high data transfer rates. WLAN will free up our employees from behind the desk and provide them access to real time connectivity and information immediately. WLAN solution will not only provide scalability to existing networks but also provide a general improvement in process efficiency.

3.4 Benefits of Deploying a Wireless LAN

It is expected that deploying WLAN technologies will provide the following benefits:

Improved Mobility: It will allow employees to connect to the enterprise from different locations adding value in terms of productivity and satisfaction. For instance, employees will be able to freely roam the properties and interact with the guest more frequently to address their needs, such as making restaurant or hotel reservations, etc. However, there are risks associated with having employees dispersed all over the property as well. From a technology standpoint the coverage area may be limited in some cases adversely impacting the benefits of improved mobility.

Improved Collaboration: It will allow teams working in different locations to collaborate in real time. For instance, with increased mobility the employees from various departments will be able to come together to resolve customer disputes or requests in a timely manner. Occasionally, guests that are interested in making hotel reservations also expect their room to be complimentary. Therefore, often employees from both the hotel and guest services department must be available to address this need.

Enable Decision Making: Employees will have immediate access to information so they can make informed and immediate decisions. For instance, currently the employees must walk away from the guest to look up account information before addressing any concerns or disputes. As previously mentioned, gaming companies make revenue by finding ways to extend the customers gaming experience.

Scalability: The time to deploy a WLAN will be relatively fast and easy in our environment because of the layout of our current property. The gaming vessel currently has all the necessary wiring, conduits, access points, switches, etc., in place. However, because of the metal decks between the two levels, additional access points may have to be placed to address any signal degradation or attenuation issues. WLANs can also be extended to provide connectivity with other LANs. For instance, the hotel information will no longer be limited or accessible only at the hotel front desk.

Business Continuity: Because WLANs can be both quickly installed quickly and relocated; they can also be repaired faster in the event of a technical problem. Continuity will allow customers to enjoy their experience without any disruption, despite the fact that certain continuity risk elements do exists as it relates to wireless in the form of bandwidth overlap, cross-talk, hostile hammering and building structural issues.

Low Costs of Entry: The physical structure of our facility is not conducive to installing wires. For instance, the penetrations required to feed cable between decks can very expensive. Additionally, any physical changes to the vessel need pre-approval from the Coast Guard and other regulatory authorities adding time and expense to the project. Therefore, a site survey as proposed in Appendix A will be required first to understand the coverage possibilities and concerns. A successful survey will eliminate the need to install expensive cable every time a change is made to the infrastructure or physical layout

3.5 Concerns about Deploying Wireless LAN

While the Wireless LAN provides a number of benefits, it is important to keep in mind several issues before deploying a WLAN infrastructure. Some of the issues include:

Security: In order to prevent the expected range of hacker attacks and deal with ongoing and developing threats, security architecture must be given a thorough and comprehensive review and analysis. Some security technologies include:

DpAC Technologies Corp (2005) described Wired Equivalent Privacy (WEP) as another way to secure networks and is also considered a security protocol for the IEEE 802.11b standard. WEP encrypts data packets using RC4 cipher stream to protect the security of the information as it transmits from one location to another. However, WEP dates back to 1999 as one of the original standards. According to Home-WLAN (n.d.), WPA actually provides several advantages over WEP, which include: a) better key management and message integrity checking; b) no direct use of master keys, c) better protection and encryption key methods.

WiFi Protected access (WPA), addresses the known security issues of a WEP protocol and Assureconsulting (n.d.), described it as an integrity check of the messages, re-keying mechanism, packet key mixing and extended initialization vector. WPA utilizes pre-shared keys and works effectively when over-laid on 802.11 architecture. WPA works with 802.11 based devices and expected to be compatible with future 802.11i devices as well. Additionally, WPA2, ratified by the IEEE 802.11, provides a high level of comfort that their networks will not be compromised by unauthorized users.

Light Extensible Authentication Protocol (EAP) was described by Ou (2007) as a flexible standard for both wired and wireless networks and is the basis for many other existing and newly developed EAP methods. It was created by CISCO to address the WEP security weaknesses, known as Lightweight EAP. According to TECH-FAQ (n.d.), a Rogue Access point is set up by a hacker to sniff out legitimate network traffic and continues to be a serious threat from outside the organization. Since our regulatory compliance criteria are stringent as described in the Iowa code 99F, it is imperative to take all the necessary precautions to detect and mitigate rogue access points. In conjunction with the study, a complete security analysis will be provided later in future chapters.

Bandwidth: Whatis.com. (2006) defined Bandwidth as being synonymous with data-transfer rate, which is the rate at which data is transmitted between two points in a certain period of time. It is expressed in bits per second (bps) or bytes per second (Bps). In general, a high bandwidth transmission delivers better quality data or images. This feature despite occasional concerns of bottlenecks, provides the applications to be accessed in a timely manner

Interference: WLAN transmission rates can vary due to natural interference or radio transmissions. These sources can also be from unlicensed radio devices, such as garage door openers, cordless phones, etc., that cause WLAN performance issues. Interference can also occur when we place wireless devices of the same frequency too close to each other in a gaming room as well. Transmission may also be impacted by building structures, other RF sources and natural topology. The Access Points (APs) have limited range and must be positioned with both range and bandwidth requirements in mind. Mitchell, B, (n.d.), described the Access Point (AP) as a node that has been configured to both transmit and receive radio signals. Access Points support the communications standards for Wi-Fi wireless.

Roaming: Often time's design issues can lead to other concerns. For example, users connections may get are dropped and need to be reestablished as they move from one location within an access point coverage area to another. Handoffs must be seamless in order for mobility to be effective

In short, based on the above discussions, for a Wireless LAN to be successful, it must be designed appropriately with both the benefits and concerns in mind to be managed effectively.

3.6 IEEE 802.11: Overview

In a WLAN environment, data is transferred between devices within the coverage area using the spread-spectrum technology which is based on radio waves. As addressed in Nortel Networks (2005), the Institute of Electrical and Electronics Engineers (IEEE) developed the 802.11 standard for the Wireless LAN network communications developed the 802.11 standard in 1997. It addressed how WLANs should operate down to the microscopic level of details, including the Medium Access Control (MAC) and the physical layer protocols as illustrated in Figure 1.

The MAC as discussed previously is part of the data link layer and provides addressing, which is assigning unique serial numbers to each network adapter and channel access. It also allows the nodes on a network to communicate on a LAN and allows data packets to be delivered to a destination within the sub-network. The sub-layers of the MAC address interface with both the Logical link Control sub-layer and the physical layer.

The Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA), which is the MAC mechanism for the 802.11 standard, is capable of both detecting and avoiding collisions with transmissions from other devices. It also makes an attempt to transmit especially when the wireless medium is idle.

The robustness of the MAC protocol is significantly improved through the Request-To-Send/Clear-To-Send (RTS/CTS) mechanism, which reduces collision impacts during long transmissions. The RTS/CTS also detects hidden wireless devices and usually capable of causing high rate of collision. The RTS/CTS is therefore practical in WLAN environments with high traffic and large data packet sizes.

This section on 802.11 is based on Cisco (2006), where the Open Systems Interconnect (OSI) Network Model, MAC (definitions) represents the lower portion of the Data Link layer. The OSI network model is the primary architecture that describes how communication occurs between computers. It defines the process through which information from a software application in one computer is transmitted to another software application located in another computer. OSI is made up of seven layers and each layer provides a specific function. Each task is broken into groups and assigned to each layer which allows them to perform independently. For instance, one layer can be updated without impacting the other layers. The seven layers of the OSI network model, starting from the top include: Layer 7 – Application, Layer 6 – Presentation, Layer 5 – Session, Layer 4 – Transport, Layer 3 – Network, Layer 2 – Data Link and Layer 1 – Physical.

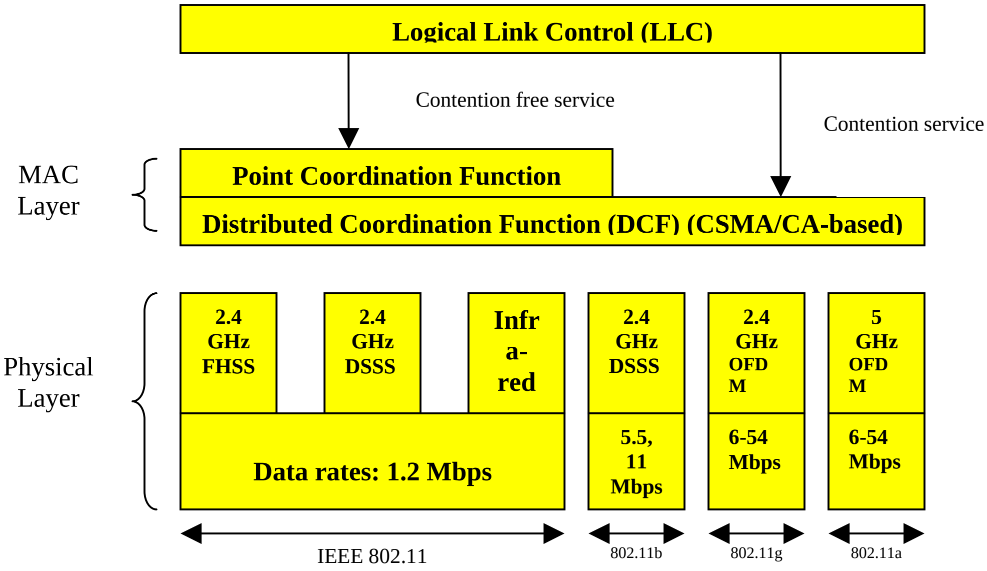

Figure 1: IEEE 802.11 Standards

Note: adapted from Nortel networks. (2005). In Engineering a WLAN Network. Retrieved December 9, 2007 from http://i.i.com.com/cnwk.1d/html/itp/NTN2018Engineer_Final.pdf

There are several 802.11 standards that apply to this project as options and they are family assigned a single-letter suffix to identify the family as follows. The 802.11a was the first wireless networking standard, which was followed by 802.11b and also considered the most popular and widely which was the most widely accepted. It was then followed by the 802.11g standard and 802.11n (late 2007).

The original **802.11a** standard operates at 5GHz with a throughput of 54Mbps. The frequency range is between 50 and 60 feet. The standard utilizes 12 channels using orthogonal frequency Division Multiplexing (OFDM). The WAVE Report (2007) defined OFDM as the mechanism that uses the cable or wireless systems to transmit a number of signals at the same time using a single transmission path. OFDM has high spectral efficiency, low distortion and not susceptible to Radio Frequency (RF) interference. Each single signal has its own frequency range and is modulated by data, which includes voice, text, data and video. The OFDM uses a spread spectrum technique to distribute data to carriers that have specific frequencies and spread apart. OFDM technology is used in the point-to-point and point-to-multipoint configurations of the Wireless Local Area Networks.

The 802.11a standard provides good throughput and performance for applications that require high bandwidth. However, due to range restrictions, additional access points are required to cover the same area that is usually required by 802.11b standard. Although the 802.11a proposition is expensive, administrators choose it because of quality and security.

The **802.11b** operates at 2.4 GHz with a throughput of 11Mbps. The frequency range is between 200 and 300 feet. This standard is fairly inexpensive and is the most widely deployed; however, it does face interference issues as the 2.4GHz frequency is very crowded and used by many devices. This standard utilizes 11 channels for communications using the Direct Sequence Spread Spectrum (DSSS) modulation. According to Wi-Fi Planet (2002) a DSSS modulation is defined as when both the chipping code (data rate bit sequence) and the transmissions are combined and then divided based on a spreading ratio. Chipping code essentially provides redundancy to the transmitted bit pattern and signal interference is reduced. Because of the redundancy, the original data is recoverable if any packets are damaged during transmission.

The **802.11g** operates at 2.4 GHz with a throughput of 54Mbps. The frequency range is between 100 and 200 feet. Although 802.11g is expensive, most organizations are deploying them because of higher throughput. It is backward compatible with 802.11b and most access points support 802.11a and 802.11g standards. GNS Wireless (2007) pointed out that 802.11g provide good speed and range without any significant interference.

The table below reflects the physical layer requirements of the 802.11 standard and the physical rates that are supported by the respective frequency bands.

Table 2: 802.11 Physical Layer Characteristics

	802.11b	802.11g	802.11a
Adopted by IEEE	1999	2003	1999
Technology	DSSS	OFDM & DSSS	OFDM
Frequency Band	2.4 GHz	2.4 GHz	5 GHz
Channels (US)	3 non-overlapping	3 non-overlapping	13 increasing to 24
Physical Rates	11, 5.5, 2 & 1 Mbps	All 11a & 11b rates	54, 48, 36, 24, 18, 12, 9 & 6 Mbps

Note: adapted from Nortel networks. (2005). In Engineering a WLAN Network. Retrieved December 9, 2007 from http://i.i.com.com/cnwk.1d/html/itp/NTN2018Engineer_Final.pdf

3.7 Factors Affecting Capacity & Performance

The WLAN environment is dynamic and therefore, during the planning phase of WLAN architecture, several of the following interacting factors must be taken into consideration as described below:

3.7.1 Radio Link Performance

The wireless medium is extremely dynamic and both interference and, transmission errors are not only common but also unavoidable. As previously discussed, wireless signals have a tendency to loose their strength when information is transmitted in environments that include buildings, walls and other obstacles. These conditions can cause signal reflection, refraction or absorption. According to Nutter (2005) it is important to consider the characteristics of the building where the WLAN will be deployed. Too much metal or obstacles blocking a clear line of sight between the access point and the device can impact signal strength. There is no one thing that can cause signal strength issue. Therefore, a site survey as detailed out in appendix A will be completed to understand any signal performance issues.

Rate versus Distance

The reliability of a signal is determined by the distance that exists between any wireless device and the access point. In other words, the farther the device is from the access point, the weaker is the physical rate or signal resulting in frame error. High frame rate errors adversely impact speed and high data rate transmissions. 802.11 devices determine the best throughput by constantly monitoring the quality of signal from other devices. [Motion Computing. (2007)].

The distance from the access point determines the data rate, therefore, in a business environment such as ours where there are walls, slot machines, bulkheads, metal decks, etc., are prevalent the absorptions or reflections of the signal may cause shadowing, which in turn then also determines the actual data rate that may be achievable. For instance, on the first deck of the vessel, we may have an issue with the bulkheads that exists on the ceiling. The access points will need to be positioned in a strategic way to get maximum signal gain.

In short, it is necessary to factor the effects of shadowing when determining a location to deploy WLAN in order to achieve a base rate with certain level of assurance. In our physical environment, in order to sustain a 95 percent of probability that a 42 Mbps is achieved consistently, the Access Points may have to be placed in multiple locations due to a variety of bulkhead designs. [Motion Computing. (2007)].

802.11a vs. 802.11b vs. 802.11g

Historically, the 802.11a devices have been marred with poor performance. Confusion still exists as it relates to the 2.4 versus the 5 GHz bands. Different types of obstacles provide different absorption and reflection characteristics. Wireless links can cause poor performance and the user's connectivity and the network topology are dynamic and continue to change over time. This requires the need for these channels to be both adaptive and robust at all layers from the link to the application layers according to Goldsmith (n.d.). Therefore, it is possible for propagation between these bands to be minimal resulting in acceptable performance.

As for the 802.11b devices, they cannot decode OFDM (definitions) signals nor detect 802.11g devices. This is the reason why 802.11g devices should take precaution when operating in an 802.11b devices simultaneously due to OFDM signal interference. The fact is that capacity is reduced when both 802.11g and 802.11b operate at the same time in the same environment. However, maximum capacity is achieved when 802.11g operates in a sole environment that does not contain any other standards. [GNS Wireless. (2007)].

Packet Size versus Efficiency

According to Nortel Networks (2005), a fixed overhead is involved when a packet is transmitted utilizing a wireless medium. Overhead consists of preamble, an inter frame gap and acknowledgements. The 802.11 MAC and physical layer efficiency is determined by the packet size and exchange type. For example, using a simple message of 1,000 bytes, the maximum effective throughput of the packet size in an 802.11a with the lowest rate of 6 Mbps will outperform an 802.11b with the highest rate of 11Mbps. Similarly, on an 802.11a device with a physical rate of 54 Mbps, the approximate theoretical output is 30 Mbps.

Based on the results of the site survey and in order to minimize signal interference in a simultaneous 802.11a and 802.11g environment, couple of protection protocols can be deployed. They are:

1) Lower-overhead CTS: By omitting the Request-to-send (RTS), the device transmits a Clear-to-send (CTS) message that is self-addressed, and

2) RTS/CTS: In this case the CTS messages are aware that the transmission was successful and hence is considered a more robust solution. In a RTS/CTS mechanism, a node sends out a request-to-send (RTS) when it is transmitting to another node. The receiving node responds with a cleared-to-send (CTS) and subsequently the transmitting node sends the packet. The RTS/CTS packets are encoded with a duration field ensuring that the information is transmitted within a certain period of time. In the event the transmitting fails to receive the CTS, then the node turns into an exponential back-off mode. [The RTS/CTS Mechanism. (n.d.)].

Although backward compatibility is possible with 802.11b devices, costs can be pretty significant. For practical purposes, it is recommended to transmit shorter frames using DSSS modulation, as opposed to self-addressed CTS that utilize DSSS modulation (definitions) and subsequently use OFDM modulation (definitions).

3.7.2 Single Access Point Capacity

A mediums capacity is reduced due to interference from contention, collisions when multiple devices are active simultaneously. Compared to an environment that has no interference, often degradation can often be as high as 60 to 70 percent. For instance, for a packet size of 1500 bytes utilizing a single access point for an 802.11a system is 30 Mbps. However, in an environment where there is interference, collision and contention, capacity may be reduced by as much as 60 to 70 percent.

Effect of Data Rates on Cell Capacity

Achievable throughput is determined by the rate of transmission that exists between a wireless device and the Access Point. Every device in the wireless medium by design is shared and the 802.11 MAC Layer provides equal access to each of them.

Devices that transmit short packages during times of heavy usage are at a disadvantage. Additionally, if the connectivity is slow it affects throughput, especially when a large frame is either transmitted or received at very slow rate causing error rates.

Nortel networks (2005) asserts that when two wireless devices are connected, especially one at a high rate and the other at a slow rate and transmitting the same packet size, the 802.11 MAC causes an averaging affect or 'edge user effect' for the two different rates. The capacity of the medium value is closer to the lower rate from the averaging action than it is for the higher rate. The averaging effect confirms the theory that merely increasing cell coverage will not increase throughput for devices close to the access point.

Capacity, Coverage and Inter-Access Point Spacing

Capacity and coverage are considered WLAN performance metrics, which are impacted by the density of a system or the inter-access point spacing**.** There is both interplay and interaction between capacity, coverage and inter-access point spacing, the need to reutilize frequencies is not necessary, especially when adequate channels are available.

The capacity metric describes the amount of throughput that is available to the users. Coverage is where the wireless signals exists and defines the probability of a user connecting reliably to an Access Point located inside the WLAN. Both capacity and coverage metrics are impacted by the inter-access point spacing and related directly to the area where connectivity is provided.

According to Nortel Networks (2005), as the inter-access point spacing is decreased, the area of service for the access point also decreases. It does so in conjunction with the decrease in the average distance that exists between the closest user and the access point. Assuming there is no other parameters are affected within the WLAN, two important things occur:

1. Allowing the same access point to connect at a higher data rate increases the capacity per access point.
2. Achieving minimum connection speed despite the risk of shadowing increases the coverage reliability. Additionally, coverage reliability is also enhanced because signals converging from different access points improve the opportunity for a good signal despite obstacles and interferences.

Let's assume that in a WLAN deployment there are 6 cells averaging 12 Mbps, with a total system capacity of 72 Mbps (6 * 12). As the density of the access points double, the services are reduced in half, which allows the users to connect at 24 Mbps, which is a much higher rate. This results in total capacity of 288 Mbps (12 * 24).

In summary, the capacity of the system is increased by more than the increase in the Access Point density, as a result of simply reducing the areas that are serviced by the Access Points. Adequate non-overlapping frequencies are required to achieve this level of capacity and to provide adequate coverage in dense areas that contain obstacles, especially without reutilizing a certain frequency. Conversely, signal degradation can also result from the interference of overlapping frequencies, which eliminate the benefits accrued by a smaller service area. With three non-overlapping frequencies for 802.11b and 802.11g systems, this can be a limiting factor for deploying a medium and larger WLAN.

Finally, Kolodziej & Hjelm (2006) argue that mobile wireless devices, while roaming, are most effective and gain maximum capacity efficient when they have the ability to connect to the best

Access Point (best data rate). On the contrary, they may connect to different Access Points resulting in different rates. The averaging or the edge-user effect occurs when the user moves from one Access Point service area to another, but still remains associated with the previous AP service area (p. 134).

Contentions and Collisions

A collision avoidance system is utilized in an 802.11 Wireless LAN system to control and direct multiple devices attempting to share the wireless medium simultaneously. The mediums efficiency is improved with a little contention, where the device with the shortest back-off interval is allowed to transmit while the other devices have to wait for the opportunity. The short latencies result in improved utilization of the medium.

However, Motion Computing (2007) pointed out that excess contention results in inefficiency, especially when multiple devices are attempting to access the medium and they collide. This forces the devices to wait longer for transmission as the entire duration of the transmission is lost.

In short, the bandwidth of a wireless LAN cannot be assigned to each individual device in the medium and for the wireless medium to be efficient; the chances of collisions must be kept minimal.

3.7.3 Multiple APs, Co-Channel Interference and Capacity

The capacity of all single access points make up the capacity of a WLAN. Steps must be taken to reduce interference between cells utilizing similar frequencies, especially when the number of deployed access points outnumbers the available frequencies.

Co-channel interference is a result of remote cell devices transmitting signals in similar frequencies, which are usually, too faint to detected and disrupt signals. Typically, radio signals are weak when they are the farthest from their source. In order to minimize interference, frequencies must be re-used across the two or three-dimensional space for cells with same frequencies. [Extricom. (2007)].

A point to keep in mind is that simply adding access points to increase capacity will cause signal degradation. Compared to a single access point deployment, capacity is impacted by as much as 85% due to Co-channel interference.

Frequency Planning (Re-Use Planning)

Access Points are assigned frequencies in such a way as to maximize the distance between cells with same frequency, also known as reuse distance. Typically when larger numbers of frequencies are used, it is indicative of high re-use distance. Re-use is basically defined as how often a frequency can be reutilized within the same network.

According to Shah (2003), the maximum reuse distance in a two dimensional deployment for any given cell for the number of available frequencies is its’ square root. For instance, the distance achieved by 12 frequencies is twice that of achieved by three, resulting in much lower interference.

Prior to deployment, frequency planning requires evaluating interfering sources, such as walls, floors, etc., that are present in the environment.

Co-Channel Interference and Noise Rise

A 2.4 GHz band WLAN consists of channels that are non-overlapping and the 5GHz band consists of 24 channels. WLAN deployments require frequency reuse, which also leads to background noise in any given cell. Miceli (2001) pointed out that a key re-use factor and co-channel interference is determined by the distance ratio that exists between the radius and the interfering cells. Reduction in co-channel interference is not rectified by increasing the cell size, it can only occur if the interferes are far away from the access point, while allowing for a proportionate reduction of signal strength.

Therefore, WLAN must be designed with adequate overlap between cells to avoid coverage gaps. As background noise rises, the overall performance is impacted. It is critical to understand the effect of the background noise. It will manifest itself during heavily loaded wireless system avoiding detection during an initial site survey.

Interference in Three Dimensions

WLANs are typically deployed in buildings with multiple levels and have the potential of interference from other frequencies or WLANs operating in any of those levels. For instance, let's assume a frequency plan for a multi-level building that uses eight separate frequencies. The odd or even numbered frequencies follow the odd or even numbered floor numbers, consisting of the frequency plans for both the vertical structures and the floors. According to Nortel Networks (2005) the interference issue is significant in a three-dimension situation and potentially due to:

1. The reuse factor is greater and possibly the reuse distance is the same. For instance, in a two-dimension deployment, the distance of reuse grows by the square-root (four frequencies) and in a three dimension; it grows by the cube root (eight frequencies).
2. The numbers of interfering sources are double in a three dimension, which is equal to hexagonal cell packing, six versus 12 in three dimensions.
3. The interferer in a two dimension furthest away grows linearly (42 interferers) versus square of the distance (12 interferers) in a three dimension.

Propagate Networks (2003) argued that the interferences can be mitigated because concrete floors are able to attenuate signals by several decibels in the 2.4 to 5GHz frequencies causing the effective distance to increase. Additionally, azimuth controls on antennas allow the confinement of signals to particular floors because antennas are omni directional and lack predetermined spatial orientation. This technique is not effective for a mobile computing device.

3.8 Application Requirements

The application mix, which is the combination of voice and data and traffic demands, must be considered when deploying a WLAN environment. These requirements eventually determine the parameters for the WLAN environment by defining coverage areas and minimum performance rates.

3.8.1 Quality of Experience

The end users in a WLAN environment determine the Quality of Experience and the performance metrics determine whether the system is delivering and meeting end users expectations.

Data Applications

In general and according to Nortel Networks (2005), the performance metric for a data application is determined by the time it takes the end user to initiate a command and the time it takes for it to be displayed on the mobile device. The response times vary based on the application deployed.

When small amounts of data are transmitted, there is only a limited effect on the wireless link. In a wireless environment, both delay and the quality of the experience are based on small transactions. End users are more tolerable when they are transmitting large amounts of data, for example, e-mail, web-based applications, making the connectivity reliability critical. Additionally, the quality of the link is critical because the transport protocol (TCP) interprets loss of data packets as a reason to reduce its transmission rate.

Pentikousis (2000) described the Transport Control Protocol (TCP) as both a full-duplex and transport layer network protocol. It provides a reliable connection and the connection is supported by streams of data that are flowing in the opposite direction. One of the features of the TCP is to avoid overflowing the capacity of the buffer through flow control mechanism. Another feature of the TCP is that it prevents excess network traffic through the congestion control mechanism. Finally, TCP converts host data packets delivery mechanism into the process communications channel and is therefore also known as the end-to-end protocol.

Voice

Voice applications are adversely impacted by both delays and distortions. For good conversational experience, the delay should be less than 150 milliseconds and anything above it will produce excessive delays. [Nortel Networks. (2005)]. Delays can be caused by packetization, propagation and play-out delay. Other items causing delays include, processing and queuing delays in routers and switches. For this project and at this juncture there are no plans to deploy Voice applications. This discussion was provided to assist the reader to be aware of the voice application possibilities.

Mixed Data and Voice Applications

The information for the following two sections was extracted from Nortel Networks (2005) to discuss the varying characteristics of both voice and data, because it is challenging to meet the requirements on a single network. Data packets on the same LAN generate bursts of packets of varying sizes and can co-exist without impacting on the same LAN without degradation in performance. However in a Wireless LAN, without adequate measures, a stream of data bursts can overwhelm the medium temporarily causing voice quality delays and losses.

On the other hand, voice packets are made up of small packets and are evenly distributed. Several voice streams can coexist in a WLAN medium without degradation in performance as long as the capacity is not exhausted.

For the voice users an 802.11 environment will not yield a satisfactory experience. Without QoS mechanisms, the best way is to separate the data by utilizing 802.11a for data users and voice bands by utilizing 802.11b/g for voice and 802.11a for data users. This configuration can be implemented by deploying multi-mode access points that contain multiple- channels in both the 2.4 and 5GHz bands. Larger deployments have significant co-interference problems, because the frequencies that are available in the planning of data and voice are much smaller.

Microsoft TechNet (2003) described Quality of Service (QoS) as the industry standard or mechanism that ensures an exception level of performance for applications. Network administrators rely on QoS mechanisms to ensure an efficient use of resources and a consistent delivery of service level without having to make adjustments or modifications to their networks. QoS essentially gives priority to users and applications that are preferred or critical than others by giving them preferential treatment as opposed to equal treatment. QoS allows network administrators to manage the networks from a business standpoint as opposed to technical. Additionally QoS reduces costs through efficient utilization of resources and significantly improves the users’ experiences.

Employing QoS mechanisms is the most effective methodology to ensure higher priority access to voice traffic than the data traffic. The quality experience, when transmission occurs on the same channel is much better, especially when both the voice and data are shared.

3.9 WLAN Planning

A tremendous amount of site specific information is required to plan a WLAN deployment. For good coverage and capacity, the number of access points required must be determined by evaluating information such as floor plans, coverage areas, mass distribution of the personnel, location of connectivity devices, such as hubs, switches, etc., must be determined. [Nortel Networks (2005)]. A site survey is critical, particularly in our operating environment, where we still operate a portion of our business on first generation riverboat, we have to deal with steel bulkheads, and other nuances in the form of obstacles consistent with a vessel.

Site Survey

The site survey begins with floor plans and they are used to define the physical environment, which depicts the shape of the coverage area and any obstacles. The radio conditions also known as both signal strength and interference are also graphically depicted on the layout.

Coverage Area

For all intent and purposes, the size of an area does not necessarily reflect its shape. In our physical environment, we have long, wide and narrow areas and additional access points may be required than indicated by the coverage area. This occurs because the coverage area in some or most instances will fall outside the circular area. Additionally, in irregular areas directional antennae's are may be used as well. On the other hand, when coverage is required between multiple floors, depending on construction materials, radio signals may penetrate floors and only use minimal number of access points.

Obstruction

The characteristics of the type of building material used for floors, walls also dictate where the access points may be located. Column or large objects affect signal propagation so special care must be taken to consider them during site survey. Signal reflection can also be caused by fire doors, metal filing cabinets, air ducts, etc., causing disruption. Water absorbs radio signals and fish tanks or waterfalls are impermeable barriers. The following three different types of antennae: Omni-directional, Semi-directional and Highly-directional may be used to mitigate signal degradation. [AT&T (2007)].

The following table shows the degree of attenuation for the most common obstacles.

Table 3 : Obstruction and Degree of Attenuation

Obstruction	Degree of Attenuation	Example
Open Space	None	Cafeteria, courtyard
Wood	Low	Inner wall, office partition, door, floor
Plaster	Low	Inner wall (old plaster lower than new plaster)
Synthetic materials	Low	Office partition
Cinder blocks	Low	Inner wall, outer wall
Asbestos	Low	Ceiling
Glass	Low	Non-tinted window
Metal tinted glass	Low	Tinted window
Wire mesh in glass	Medium	Door, partition
Human body	Medium	Large group of people
Water	Medium	Damp wood, aquarium, organic inventory
Bricks	Medium	Inner wall, outer wall, floor
Marble	Medium	Inner wall, outer wall, floor
Ceramic (metal content or backing)	High	Ceramic tile, ceiling, floor
Paper	High	Roll or stack of paper stock
Concrete	High	Floor, outer wall, support pillar
Bulletproof glass	High	Security booth
Silvering	Very High	Mirror
Metal	Very High	Desk, office partition, reinforced concrete, elevator shaft, filing cabinet, sprinkler system, ventilator

Note: adapted from AT&T. (2007). In Implementing a WLAN: Good Planning is the Key to Success. Retrieved December 23, 2007 from http://www.business.att.com/nx_resource.jsp?repoid=Topic&rtype=Whitepaper&rvalue=implementing_a_wireless_lan&repoitem=mobility&segment=ent_biz

Interferences

At a minimum, it is critical to identify the devices that may be operating in close proximity to the WLAN. These devices may include Bluetooth that utilize 2.4 GHz frequency; cordless phones; 802.11b standard devices operating on channel 9 frequency, such as microwave oven and devices using Radio frequency (RF), etc. Most of the interference surrounds around the 2.4GHz band and most devices use the 5 GHz band simultaneously to avoid over-lapping of frequencies. The other most important fact to consider during the WLAN site survey is to detect other WLANs that are operating in proximity.

Coverage versus Capacity

Site surveys by definition provide coverage assurance and do not guarantee performance or capacity. Also, the inherent conditions of the shared medium and the requirement for effective and efficient throughput can cause the WLAN traffic patterns to vary and assure satisfactory performance. [Nortel Networks (2005)].

In a large scale deployment such as ours, channels will get reused causing performance degradation from co-channel interference. A site survey may determine this form of interference, however may not be able to detect data rate degradation due to noise rise. For these reasons, a complete analysis must be under taken to guarantee both coverage and capacity.

3.10 Equipment

After proper planning, the implementation is largely a plug-and-play initiative. The WLANs are designed with a few types of components and the infrastructure is composed of the following:

- **Hardware**: the two main components are the Access Points (AP) and a wireless adapter to connect to the network. The wireless adapter is then installed into the handheld or mobile computing device.
    - **Access Point (AP):** it is a radio based device that both transmits and receives signals. The access point is connected to the wired LAN through Ethernet cables and has a small box like appearance that consists of one or several antennas.
    - **Antennas and Bridges:** antennas extend the range of 802.11 systems by amplifying the radio frequency. A Bridge typically connects two LANs wirelessly and is also known as the point-to-point wireless connection.
    - **Wireless Adapter:** it allows the computing device access to the network wirelessly by connecting through the access point. It is also similar to the network interface cards (NIC) that are inserted into computing devices to establish connection.
- **Clients:** these include mobile computing devices, laptops, workstations, phones, printers and other Wireless network Interface Cards (WNIC) enabled devices.

Devices located on a WLAN are known as Wireless network Interface Cards (WNICs). A service set is described as a collection of stations, which is usually connected to a Distribution System such as a wired LAN.

Security and policies should include an authentication server to validate both the user and the access point. A WLAN management system is also used to monitor the performance and maintenance of the wireless network. A gateway server is also recommended to ensure Quality of Service (QoS) for certain application and groups of users.

AT&T (2007) noted that because 802.11a and 802.11b operate on different frequencies, it is important to ensure that the clients are on the same frequency, else the devices will not communicate with each other. The exceptions are 802.11b and 802.11g standards as they both operate on the same frequencies, however, differences do exists due to modulation. Therefore in some or most cases the devices are designed with dual mode capability (802.11 b/g) to be able to work effectively. Finally, it is important to ensure interoperability between the network infrastructure and the client devices as well.

3.11 Roll Out

Because our physical operating environment is so complex, we will use a Build-and-Test approach. This allows us to bring up one segment up of the WLAN at a time. Ensure it is functioning as intended before moving to the next segment. From a planning standpoint, when new APs are added, the entire infrastructure will be retested before moving forward, especially if errors were made in RF frequency placement.

3.12 Emerging Technology

The existing 802.11a/b/g WLAN provides adequate convenience of both connection and performance for today’s applications. However, in the future, applications will require greater data throughput. The IEEE Standards Association created the 802.11Task Group N (802.11TGn) and charged them with the task of developing the standard that would deliver a minimum of 100 Mbps by modifying both the Physical and the Medium Access Control Layer. Wilson (2004) asserted that this task represents a four times leap compared to today’s standards. The higher throughput will improve efficiencies, user experience, while leading the way for new applications. The task force (TGn) has claimed that the new standard will provide backward compatibility with existing standards, including a smooth transition. The following table reflects the WLAN throughput based in the IEEE standard. Additionally, Intel is supporting the 802.11n standard initiatives to ensure that WLAN technology supports mobile computing, handheld devices and consumer electronics.

Table 4: 802.11 Transfer Rate Comparisons (Source Intel Labs)

IEEE WLAN Standard	Over-the-Air (OTA) Estimates	Media Access Control layer, Service Access Point (MAC SAP) Estimates
802.11b	11 Mbps	5 Mbps
802.11g	54 Mbps	25 Mbps (when .11b is not present)
802.11a	54 Mbps	25 Mbps
802.11n	200+ Mbps	100 Mbps

Note: adapted from Wilson, J. (2004). In Quadrupling Wi-Fi speeds with 802.11n. Retrieved December 23, 2007 from http://deviceforge.com/articles/AT5096801417.html

The 802.11n standard depends on new technology and uses existing technologies to make Wi-Fi faster with better range. The new technology Multiple In, Multiple Out MIMO utilizes several antennas to transmit data streams from one location to another. Instead of sending one single data stream, MIMO transmits three streams and receives two allowing more data to be transmitted. This technique also increases both range and distance.

The 802.11n also incorporates bonding which allows the use of two non overlapping channels simultaneously to transmit data, also allowing for more data to be transmitted. Payload optimization or packet aggregation technology in 802.11n allows more data to be stuffed in each data packet. 802.11n technology will result in greater speed and range.

Most business are not deploying 802.11n standards until vendors ratify them and then will we see an increase in the corporate setting. It is not to say that products are not available under

802.11n standards. As a matter of fact, products based on Draft 2.0 are available now with great reviews of both speed and range.

802.11n devices will be backward compatible with the 802.11 legacy standards and will operate in both the 2.4GHz and 5GHz frequencies. These devices will also be compatible with 802.11g standard and can operate on the same channel by reducing speed to match that of 802.11g affecting the entire network.

Jacobs (2007) asserted that since 802.11n will provide high data rates and new applications, they will have an impact on the existing network. Switches will need to be replaced and may eventually be replaced in favor of a new technology. Wired components will need upgrading. While a 100 Mbit Ethernet link was adequate to connect switch to an 802.11g Access Point, a Gbit Ethernet may be required for an 802.11n standard.

According to WiFi Alliance Senior Director Karen Hanley, the Wi-Fi technology is pervasive and currently utilized by 350 million people around their homes, businesses and hotspots. The 802.11n 2.0 draft products certified by Wi-Fi are at the cutting edge because they provide both increased range and throughput. Additionally, the 802.11n 2.0 draft products have passed some of the most rigorous interoperability testing. Karen expects that the adoption of the next generation standard will become prevalent as companies continue to adopt them in new products and multimedia applications. [WiFi Alliance. (2007)].

Additionally, ABI Research is also forecasting that 90 percent of the Wi-Fi chipset sales by 2012 will support the 802.11n standard. According to Phil Solis, principal analyst at ABI Research, the 802.11n will allow for deployment of larger applications that include video, opening up possibilities for a whole set of new consumers that had previously not tried the Wi-Fi technology. [WiFi Alliance. (2007)].

In summary, a WLAN deployment in our business will increase productivity, resolve guest issues and improve collaboration between team members resulting in efficient, quick and effective decision making. The key elements to consider in architecting the 802.11n WLAN are costs and robust performance. A complete analysis and redesign may be required. As 802.11n will offer opportunities to leverage the new technology and applications it brings forward.

Chapter 4: Securing and Scaling the Wireless LAN

Security is a big concern and an issue in a WLAN environment. I have dedicated to this topic with its own chapter to convey the importance of adopting a strong security protocol. Without it our business would be exposed to wireless threats, abuse, misuse causing significant financial harm. The damage can be significant and result in costs associated with investigation, down time, decline in competitiveness and market value. As previously discussed, gaming establishments have to comply with Iowa Code 99F that provides specific guidance and requirements for holding a gaming license and non-compliance can mean loss of our gaming license. This chapter will address the various security technologies, such as WEP, EAP, WAP, etc., discussed in previous sections and their application to our environment.

There are considerable options available to safeguard wireless LANs against 802.11 attacks. An in-depth security approach is required for an effective defense, which requires identification and elimination of vulnerabilities. This section will identify a process, which will define risk analysis, vulnerability identification and threat remediation.

4.1 What are WLAN Vulnerabilities?

In a wireless environment, the medium for transmission and receiving is air. As discussed in previous chapters, obstacles such as walls and floors can cause signal degradation, however, they do not discourage attacks from nearby locations. Intruders may use one of the following vectors to exploit WLAN vulnerabilities:

Inability to Control Access

Intruders use high gain antennas and shareware Stumblers to discover and exploit WLANs. Often, unsuspecting employees will install “rouge” access points inside the firewall allowing intruders to exploit their vulnerability as these devices are willing to connect and interact with others. Upon connecting, the intruders can launch traditional attacks to cause harm by probing servers, locating open ports and services. InformIT (2005) described a rouge access point as an access point that was installed without the knowledge of the network administrator. It may also be one that was installed by the intruder so they can access the network resources remotely.

Friday (2007) contends that a WLAN is essentially a Radio Frequency (RF) transmitter and the use of unlicensed 802.11 bands can not be controlled and the placement of Access Points to avoid RF leaks is critical. Therefore, to avoid attacks, it is imperative to assume that neighboring devices are present and deploy strict security protocols to reduce both intrusion and interference.

Lack of Confidentiality

Once intruders have access to the system, they can use capture tools that can record and extract TCP/IP headers, passwords, etc., sent over the air. To prevent eavesdropping, data can be encrypted using:

Wired Equivalent Privacy (WEP) protocol: The encryption algorithm built into the 802.11 standard is known as WEP. Most or all vendors design the 802.11 devices so that WEP keys which are in ASCII passphrase or the hexadecimal format can be used to secure transmission. However, WEP is not inherently secure and contains security concerns, such as: 1) The administrative overhead is high, so many networks disable their WEP, 2) The vector that contains the WEP algorithm is transmitted clearly and lastly, because of linearity, the WEP checksum can be predictable. [The TECH-FAQ. (n.d.)]

Temporal Key Integrity Protocol (TKIP): TKIP was created to correct the weaknesses of the WEP and provide additional features. Using the RC4 encryption algorithm it corrects the problem associated with the generation of a weak key by generating a new key every so often. The TKIP also uses the Message Integrity Check, which is a much secure and stronger method of confirming data integrity. This particular step prevents the intruder from uncovering the key to determine the both the plain text and encrypted value, by injecting data into the packets. [InformIT. (2004)].

Advanced Encryption Standard (AES): The National Institute of Standards and Technology (NIST) developed the AES standard, which uses the larger key sizes of 128, 192 and 256 bits to protect data through encryption. It replaced the Data Encryption Standard (DES) that used 56 bit size key. AES data encryption is faster than a Triple-DES, which is a by-product of DES encrypting data at three times its normal rate. [Networkworld. (n.d.)]. According to NIST's AES overview [Federal Information Processing Standards Publication 197. (2001)]: "The AES algorithm is a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) information."

Counter Mode CBC Protocol (CCMP): The AES Counter Mode CBC Protocol is the encryption algorithm that limits the length of the key to 128bits and uses the AES cipher block. To provide a secure protocol between the Access Point and the mobile device, the AES-CCMP uses a sophisticated technique that combines the counter mode and the CBC-MAC making it difficult for intruders to detect patterns or eavesdrop. Additionally, the CBC-MAC provides the mechanism that ensures the integrity of the message was not compromised. [TechWeb Network. (n.d.)].

However, all of these protocols are susceptible to static key cracking because intruders can guess short WEP key or simple TKIP/AES and Pre-Shared keys (PSKs). Therefore, long keys for TKIP and AES with complex PSKs is recommended. Regardless, 802.11 management header control frames can not be encrypted and therefore it is important to evaluate what information may be seen.

Phifer (n.d.) claimed that by utilizing the Extended Service Set Identifier (ESSID), 802.11 systems roam automatically to the best available access points and users get lured by and end up connecting through the “Evil Twin” Access Point. Once the association has occurred, intruders can launch Man-in-the-Middle attacks. This type of attack allows intruders to introduce viruses through the web or email, intercept data sent through secure SSL or SSH servers and hijack customer data and information.

Unauthorized Network Use

A WEP key, which is a hexadecimal value, is used for controlling access to WLAN. A PSK, an alphanumeric password is used in a TKIP or AES network. Users gain access by using any of these keys and it is important to keep them secured for any unauthorized access.

WLAN access is granted to users based in authentication. In the TKIP or AES networks, it is granted through the 802.1x Port Access Control (PAC), which carries the Extended Authentication Protocol (EAP) used to validate identity. It does so by delivering access to dynamic session keys and rejecting others. However, EAP (definitions) have vulnerabilities, for instance, to obtain passwords, a dictionary attacked known as Lightweight EAP (LEAP) may occur.

Other options include using a higher level authentication at application servers or Virtual Private Network (VPN) gateways. Mitchell (n.d.) described a VPN as a Wide Area network (WAN) that allows sharing of network services over long distances. They are both cheap and efficient to implement. VPNs use a method known as tunneling and work with both private and public networks.

Regardless, WLAN hotspots provide plenty opportunities to attackers to capture PPTP password hashes, which is Point-to-Point-Tunneling-Protocol (PPTP) that was created by Microsoft to deploy VPNs. The tunneling method transfers the point-to-point frames over networks that are not secure, such as the WLAN. [Wright (2004)]. The intruder can also attack a weak IPsec (Internet Protocol Security), which is a protocol that uses cryptography to protect data that is transmitted over the Internet protocol (IP). [Microsoft TechNet (n.d.)]. Therefore, it is important that authentication vulnerabilities are mitigated to avoid unauthorized access.

Forged Messages

Cyclic Redundancy Check (CRC) prevents transmission errors; however it can not eliminate forged frames with valid CRCs. RAD (n.d.) described a CRC as a relatively easy and powerful mechanism that protects frames or blocks of data for obtaining data reliability. It is the most common mechanism used in data communications to detect errors. Both TKIP and AES use cryptographic message authentication to reject infected data packets. There is no standard protocol to detect spoofed packet in the 802.11 management control and intruders use packet injection tools to launch attacks, particularly the Denial of Service (DoS) attack.

Denial of Service (DoS)

In this scenario, the attackers generate a high volume of packets to adversely impact legitimate WLAN use. The hacker transmits continuously so it prevents others from transmitting or staying connected and they flood the air with fake access point beacons, EAP logoff frames to a point that it disassociates and cripple the wireless devices. [McDowell. (2007)]. While it is not impossible for attackers to replicate our WLAN spectrum, as network administrators, we can put processes in place to spot, detect and react in a timely manner before the malicious attack impacts business.

Vulnerable Stations

Attackers also focus on 802.11 devices, because by default they will associate with other devices such as other access points and Ad-Hoc peers. This type of characteristics can expose the stations to multiple risks, including file sharing and creating a bridge between private and public WLANs.

Additionally, code flaws in 802.11 devices and drivers can cause buffer overflows, execute malicious code causing stations to crash. This why it is important to stay up on upgrades and patches and 802.11 station software can help mitigate these vulnerabilities.

The following table summarizes the common 802.11 attacks and tools typically used by intruders and these same tools can be utilized by us to find our own security vulnerabilities.

Table 5: WLAN Attacks and Tools

Category	Attack	Examples
Authentication Attacks Steal credentials to penetrate wired network and services	PSK Cracking	coWPAtty, Rainbow Tables
	LEAP Cracking	Anwrap, Asleap, LEAPcracker
	Password Capture	Dsniff, WinSniffer
	VPN Login Cracking	Ike_crack, pptp_bruter
Access Control Attacks Circumvent filters and firewalls to obtain unauthorized access	War Driving	NetStumbler, WiFoFoFum
	MAC Spoofing	SMAC, MacChanger
	Rogue Access Points	WKnock, Draft 802.11n APs
	Unauthorized Ad Hocs	“Free Public WiFi” ESSID
Confidentiality Attacks Intercept sensitive or private data sent over	Eavesdropping	Wireshark, Wellenreiter
	WEP Key Cracking	Aircrak-ptw, chopchop
	Evil twin	RGlueAP, 4-in-1 USB APs

wireless associations	AP Phishing	Airsnarf, Hotspotter, KARMA
Integrity Attacks Modify packets sent over wireless to mislead attacker	802.11 / EAP Replay	Airpwn, wnet reinject
	802.11 / EAP Injection	Void11, LORCON
	Response Poisoning	Dsniff, MonkeyJack, Airpwn
Denial-of-Service-Attacks Inhibit or prevent legitimate use of WLAN services	RF Jamming	Alchemy, HyperWRT
	Management/Control DoS	CTS-Jack
	Beacon Flood	FakeAP
	Deauth Flood	FATA-Jack, MDK2
	EAP-of-Death	Libradiate
Station Attacks Crash or compromise laptop, phone, or other Wi-Fi endpoint	Wireless Driver Exploits	Metasploit, LORCON
	Wireless Station Probes	WZCOOK, nmap

Note: adapted from Phifer, L. (2006). In WiFi Vulnerability assessment checklist. Retrieved December 27, 2007 from http://searchsecurity.techtarget.com/general/0,295582,sid14_gci1167666,00.html?track=wsland

4.2 Risk Analysis

Risk analysis is a good process to implement security policy and definition. After implementation, it is critical to ensure that the WLAN is performing as intended and meeting the desired objectives through ongoing monitoring and periodic testing. This allows any new vulnerabilities or holes in the existing systems to be identified in a timely manner and refined fixes applied. An iterative process ensures a strong and measurable foundation for WLAN threat management.

It is important to understand that attacks will occur and no one can possibly be prepared against every single type of attack. Also some attacks are or can be more damaging than others. The right approach is to define an acceptable level and put processes in place to reduce the associated risk. Phifer (2006) stressed that risks must be put into perspective and understand that attackers will exploit vulnerabilities and business may be compromised. For instance:

- Both Stumblers and WEP/PSK crackers allow attackers to gain access to wireless networks. Unauthorized users try to gain access to free Internet or users sometime unintentionally associate with the wrong access point. Regardless, the probability of the WLAN being accessed or compromised is high. Therefore, every attempt must be made that WLAN is security is set high to reduce adverse business impact. Care must be taken to ensure that rogues do not connect to the wired network or employee devices.

- Studies show that 9 out of 10 users connect to unknown WLANs and an Evil Twin attack is more persistent than a cleartext data capture. Companies must take care to protect its assets from the evil twin attacks, because they are medium difficulty and probability.

- DoS attacks may appear trivial when point-and-click raw packet injection tools are used and the impact on business can be significant. For example, taking down an Access Point in the conference room has less dire consequences than an access point located on the gaming floor, which can have extreme dire consequences.

Business needs must be first defined before starting a risk analysis initiative. Security is not only focused on keeping intruders out, but a significant effort is also made to let authorized users access services.

Risk analysis includes identifying who needs access to what and when, which users or groups require different types of access and also which databases and applications must be made available over the wireless. Business risk assessment also requires identifying assets that will be subject to compromise and also determine the nature of data that is being put to risk. We will also need to quantify costs due to business loss from downtime, recovery, breach notification costs, fines, and criminal penalties as a result of failed compliance audit.

Based on the discovery of the above mentioned items, a security policy should be written to defend the most important assets from wireless borne attacks. Then purchase and install countermeasures that help mitigate attacks and implement security policies. Finally, the WLAN implementation must be tested on an ongoing basis to ensure compliance with security policies.

4.3 Vulnerability Assessment

A vulnerability assessment utilizes observation and penetration testing to identify security weaknesses. The results are evaluated for severity and steps taken to mitigate risks, examples include, applying patches, upgrades, access point update, reconfiguring client, adding a firewall, etc.

For effectiveness, assessments must be routinely repeated. For instance, repeat the assessment particularly after updates and upgrades or simple policy changes to prevent vulnerabilities from injecting themselves into the WLAN. According to Phifer (2006) WLAN weaknesses and vulnerabilities can be discovered using the assessment process before intruders compromise the network resources.

For my company, we will in addition to in-house assessments, utilize a third party consultant to conduct periodic audits to ensure compliance with Sarbanes Oxley (SOX) and PCI DSS, which is a security standard that defines the security policies, management requirements, processes, software and network design and other protective mechanisms. It was developed to assist companies to get aggressive about protecting customers' information. [PCI (n.d.)].

WLAN vulnerability assessments begin with defining the objectives, methodology and expected outcomes. Depending on the tools available, tests may vary including the topology of the network. Documentation is critical to ensure and verify fixes and continuous evaluation of the network. Sometimes it is not a bad idea to conduct prototype assessment on a few WLAN resources. It allows you to refine your methods, expected outcomes before deploying them on a large scale avoiding unnecessary testing and wasting time.

The following sections identify the tools and techniques that are useful when conducting a WLAN vulnerability assessment. They include security event monitoring, discovery and penetration and spectrum analysis. A sample work sheet has been included as Appendix A in the appendix section.

Tools for WLAN Discovery

The first step is to identify all wireless devices that are going to be on site and tested. The site specific devices will undergo assessments, while the rest will be scrutinized for threats, ownership and evaluated for their impact on the WLAN. This stage of discovery is for security purposes only and not that of a site survey for initial implementation.

JiWire (2005) asserted that Stumblers are relatively easy to use and are available for most operating systems, including mobile computing devices. However, Stumblers have limitations, while they can locate Access Points, they can not find non-802.11 interference or stations. Despite pin point accuracy of the GPS, they fail to determine indoor locations. For vulnerability assessment to be effective, a WLAN Analyzer is required that can scan all RF channels, plot locations, export information about devices and make new devices discoverable.

The floor plan is the best place to start and scanning should occur at regular intervals for all channels in RF bands for the entire site. A list should be generated for all 802.11 devices. Record the ESSID, MAC address, IP address, Channel and settings for the Access Points. A list should also be generated for stations associated with Ad Hoc mode and for non-802.11 devices spectrum analysis should be used.

The next step is to use the site's WLAN inventory to identify any previously unknown devices, but ignore weak Signal to Noise Ratio (SNR), which is a measure of the signal strength compared to the background noise and transient unassociated stations for efficiency. For the remainder of the devices use a Wireless Intrusion Prevention Systems (WIPS) with rogue mapping or a 'find' tool to identify the owner of the device.

After collecting all the data, download the results into a WLAN planning system to see a graphical view of all the locations, overlapping coverage and Radio Frequency leaks. These are the basic elements for penetration testing, inventory update and Access Control Lists. When the WLAN Analyzer is configured properly, it can help identify known authorized devices, known neighbors and new rogues.

Using Penetration Tests

Intruders utilize a variety of tools, such as wireless, TCP/IP and server attack to compromise the WLAN. The same tools are suggested to try and attempt penetration of our own infrastructure and system devices to understand immediate consequences.

Darknet (2006) described Nmap (Network Mapper), as a security auditing and network exploitation tool designed to scan networks. It is an open source program that runs on most computers and comes free. Similarly, Superscan tool is an alternative to Nmap and considered a very powerful port scanner and a pinger. Both are used by attackers to scan devices and ports for attacks.

Winfingerprint is a program that exposes details, such as users list, services, sessions, etc., about a Windows based Operating System. An Xprobe is an alternate to most common tools that monitor TCP protocol usage and it operates by fingerprinting the active operating system. [Wiretapped. (n.d)]. Both of these are used on active devices to map the identity of their operating systems, applications, and accounts.

A Common Vulnerabilities and Exposure (CVE) database is consulted for issues and the tools that can exploit the WLAN. It is recommended that these tools are used at the wireless gateways, Access Points, DHCP and DNS servers, hosts to detect vulnerabilities. Open ports and Access Points are exploited by intruders using the default logins for probing Management ports, such as, Telnet, SSH, SNMP and TFTP.

It is also important to assess the WLANs Denial-of-Service (DoS) defenses as intruders use DoS tools at the WLAN infrastructure. Tests should be conducted on wireless gateways, switches and firewalls. Since DoS attacks are disruptive, extreme caution should be used when the test is being conducted.

Finally, run Evil Twin, which gathers information without the user's consent by disguising itself as legitimate hot spot (wireless Access Point). It exploits access points and wireless driver to assess the effectiveness of the deployed countermeasures. You can use KARMA and WIPS tools, which essentially assess WLAN security to ensure that Evil Twin is effectively contained, particularly without network connectivity.

Wireless Intrusion Prevention System (WIPS)

WIPS is a good tool for full time monitoring of the entire LAN and its devices. WIPS uses traffic analysis for trends and looks for attack signatures, protocol errors, policy violations, providing alerts and initiating defensive actions. WIPS servers enforce security policies and can thwart off wireless attacks, for instance a rogue device is dis-authenticated automatically.

WIPS are great for vulnerability assessment and useful during WLAN discovery. Using a combination of several remote and spectrum sensors, WIPS is able to triangulate the devices location. Utilizing policy based alerts WIPS can identify mis-configured devices, recent attacks, problematic location. WIPS uses both past and recent observations and makes suggestions on how to combat the threats.

The following results from the survey conducted by the ITtoolbox regarding intrusion prevention and detection, confirms the importance of deploying an intrusion prevention system. The results showed that only 45.7% of IT professionals claimed that they had adequate security. However, they felt that they could improve their intrusion prevention systems. Interestingly enough 90% of the respondents stated that they were using an intrusion prevention system when their systems were compromised. [ITtoolbox. (2007)]

Wireless Analyzers

Henderson (2003) claimed that WLAN and spectrum analyzers play a key role during vulnerability assessment. Mobile computing devices are great tools for discovering devices, capturing traffic, and monitoring wireless activity and address potential vulnerabilities. For example, a handheld analyzer can capture and decode live packets and identifies a weak RF interference. After drilling down with a handheld spectrum analyzer the non-802.11 rogue may be identified and location determined.

Analyzers are an efficient tool for on-site investigation and let you dig into 802.11. Conversely, remote analyzers are cost effective for off site investigation and spectrum analyzers peer into non-802.11 transmissions. For Voice over IP applications, VoFi analyzers can be used to assess call impact. A combination of all these analyzers provides the best vulnerability assessment solution.

4.4 Conclusion

Wireless technology has brought incredible gains in productivity and it is important to develop and deploy security solutions to remain competitive. As discussed above, the most effective security measures deployed are within the context of risk analysis and management. Risk assessment begins by understanding the threats that face our business and the potential adverse impact.

First, all devices must be examined to ensure that they are not exposed for misuse or intentional attacks. Secondly, consider the costs associated with the attacks in terms of downtime, regulatory fines, compliance, and loss of business. It is not possible to think of every attack scenario and mitigate all of them either. The best defense is completing a vulnerability assessment and business risk analysis as they help you focus on items with greatest impact. Finally, security is accomplished through policy definition and enforcement with readily available tools ensuring safety and integrity of the corporate network.

Chapter 5: Handheld Device for Mobile Computing

The Wireless LAN provides real-time connectivity to network resources from any location that is within range of an Access Point. In our industry, mobile computing devices can help with guest service resolutions, restaurant and hotel reservations and verify marketing promotions eligibility by connecting to real-time applications. Mobile devices will allow the employees to address all these issues right on the spot without having the customer to leave their gaming, dining experience or relaxation activity to take care of their needs. Real-time access via WLAN will optimize guest service, resulting in improved customer satisfaction and better financial results.

Research conducted by ZDNet UK shows that the numbers of mobile workers have increased over the years. There are different types of mobile devices that provide functionality and the technology to keep the workforce mobile. It addresses every single aspect from battery life, to portability, security and durability of the mobile devices. [ZDNet. (2007)]. The following discussion reflects some of the key points that are relative to this research topic.

The research shows that with nearly two-thirds of the respondents the penetration of the mobile workforce is maintaining an upward trend. The following types of mobile devices were most prevalent (in order) and with some indication about the future applications:

- Mobile phones were the most widely used device.
- Approximately four-fifths of the company’s laptops have mobile connectivity.
- More than 44 percent use Personal Digital Assistant (PDA) devices such as Blackberry, Palm-Treo (smart phones) that have email capabilities.

The respondents favored laptops with mobile connectivity and the most prevalent users included senior management, sales personnel and service engineers. Applications that were used the most also included voice communication, email and data communications, internet access, and personal organizer for calendar, journaling and diary. However, there were often concerns about the cost of airtime, available bandwidth and battery life. Additionally, many respondents were concerned that the functionality of the mobile devices often did not match up to that of a laptop.

As for the future deployments and consideration, the most desired applications included: mobile videoconferencing, access to company network resources, database applications, Global Positioning System (GPS) capabilities, whiteboarding and ability to collaborate with workgroups in real time.

On the technical side, the most desired applications to further enhance productivity and deliver exceptional customer experience in the future included: WiFi connectivity (approximately two-thirds), high-speed access to both the Internet and data communications, Bluetooth connectivity capabilities, devices that are interoperable on multiple networks, integration of both fixed and mobile devices.

A mobile device is generally meant to include products that offer communications and data handling capabilities utilizing a small form factor and portable. Technology is continuing to evolve and the functionality and portability of the mobile devices is improving each and every day. Although laptops are an excellent solution as a mobile device, a smaller device will be more compatible and effective in daily mobile computing for our operations. There are a lot of handheld devices on the market, such as PDAs, Ultra Mobile PC, Notebooks, and MID (mobile Internet Device), I narrowed my research down to Ultra Mobile PC (UMPC) and the MID after reading the material posted on the Internet and the research provided by Ricker (2008). (p1).

Ultra Mobile PCs (UMPCs) have all the characteristics of a PC, but can fit into your backpack or purse. They bridge the gap between PDAs and laptops. PDAs lack powers to effectively use applications and laptops, though powerful are bulky for mobility. [Sony. (n.d.)]. Following are some of the key features of a UMPC:

- Uses Microsoft® Windows® XP or Vista.
- Screen size measures between 4 and 7 inches and is the image is amazingly clear and crisp with excellent colors and contrasts.
- The UMPC screen is touch sensitive and works with fingertip and stylus. An on-screen keyboard can also be used for typing.
- The UMPC comes with an integrated 802.11a/b/g wireless LAN cards for connectivity.
- Other features include Bluetooth® technology for connectivity with PDAs, GPS receivers.

Samsung, Asus, Founder, Sony, Tabletkiosk are all manufacturers of UMPCs and provide a variety of features and benefits. After researching several of these vendor products, I narrowed my search to the UMPCs by Sony and Samsung based on the specific features such as built in Wi-Fi, storage, processing speed, portability, screen size and resolution, USB ports, etc., that were available. The following sections will discuss the features for each of these UMPCs.

5.1 Samsung Q1 Ultra (Q1U-V) UMPC

Both Dan Ackerman and Matthew Elliott, editors for CNET, reviewed the Q1 and provided the following observations: The Samsung Q1 Ultra (Q1U-V) is the second generation UMPC from Samsung. It includes a small keyboard, which is split between two screens for text input. It is perfect for brief scripts, inputs and short email replies. Other input methods include touch screen and a ThinkPad-style mouse pointer. All these various methods of input make the UMPC useful. [Ackerman & Elliott (2007)].

The 7 inch monitor is larger than most handheld devices on the market. The black plastic chassis features native resolution of 1,024x600. It is also perfect for doing on-the-go type of web research, displaying perfect web pages and plenty of room for the Windows desktop.

The Samsung Q1 is a little larger and heavier at 1.5 pounds than most UMPCs on the market. The look and feel of the Ultra model makes the UMPC look lighter than Sony’s VAIO UX390. It is relatively easy to carry around, either in a case or wrist strap.

The Ultra includes a few touch-sensitive buttons next to the Web cam that include volume controls, custom onscreen menu, brightness control, Wi-Fi connection and other options.
The Q1Ultra features the latest network communication technologies: it includes the 802.11b/g Wireless LAN, a 10/100 Ethernet LAN port, USB 2.0 ports, Bluetooth 2.0 with the EDR (Enhanced Data Rate) and a VGA out, however, does not include a FireWire device. It allows you to access the Internet, connect to mobile devices, and share information quickly and easily. It also includes a 2 in 1 memory card reader to store files and pertinent information.

While the Ultra has lot of good features, it lacks performance by utilizing 800MHz Intel A110 CPU versus competitors like Sony that use 1.3 GHz Intel Core Solo CPU. Perhaps it is the reason why the system crawls when running the Windows Vista OS menus. The Wi-Fi connection provides good range and coverage. Future models are expected to include cellular broadband capability and helpful where WLAN access is not available.

Table 6: Samsung Q1 Ultra

Description	Specifications
Processor	800 MHz Intel A110
Memory	1GB, 400 MHz DDR2
Hard drive	60GB, 4,200rpm
Chipset	Intel 945
Graphics	Mobile Intel Express 945GM (integrated)
Operating System	Windows Vista Premium
Dimensions (WDH)	9.0x4.9x0.9 inches
Screen Size (diagonal)	7.0 inches
System Weight/ Weight with AC Adapter [Pounds]	1.5/2.4 pounds
Category	UMPC

Note: adapted from Ackerman, D & Elliott, M. (2007). In Samsung Q1 Ultra (Vista Home Premium). Retrieved December 28, 2007 from http://reviews.cnet.com/laptops/samsung-q1-ultra-vista/4505-3121_7-32459191.html

The battery life is pretty good and lasted up-to 2 hours and 16 minutes on the DVD grueling battery test. It lasted up to 3 hours during the hands-on testing. The Ultra also includes a built-in 1.3 megapixel camera and a 0.3 megapixel webcam, the dual camera allows the users to take picture or short clips and post them to the preferred locations. All these features are useful for our environment: a good battery life means less trips back to the office to charge the units; a good WLAN standard means reliable connectivity and coverage along with speed; a camera allows the customers pictures to be captured immediately and post them to their account so other guest service representatives can quickly recognize and personalize the experience.

5.2 Sony VAIO UX390 UMPC

Similarly, Dan Ackerman, the editor for CNET also conducted research on the VAIO and provided the following comments. The Sony VAIO UMPC is based on Windows Vista Business platform. It includes a solid state hard drive that extends the battery life and stability than other hard drives. The UMPC has a two-hand design and a slide out keyboard. It measures 5.9 inches wide and 3.7 inches deep by 1.5inches thick. The UMPC is only 1.1 pounds and is lighter than the smallest ultra portable laptop on the market. [Ackerman. (2007)].

The screen has a 4.5 inch display screen with native resolution of 1,024x600 and is both bright and clear. It includes two zoom keys, but sometimes the zoomed in image is slow and choppy making it hard to see. Setting it a lower resolution addresses this issue.

The UMPC has multiple input options including a backlit keyboard. Also included is a pencil-eraser-style nub on the right side of the chassis and is used for moving the mouse pointer. Both right and left mouse buttons are included on the left of the screen. The UMPC is also a tablet PC with touch sensitive input using both stylus and finger.

The UX390 includes USB 2.0 port, a memory card reader and a webcam. Networking options include 802.11a/b/g wireless, Bluetooth and EV-DO, using a small antenna located on the back. It also comes with a docking station that includes: Ethernet port, USB 2.0 ports (3), FireWire port (1) and an A/V (audio/visual) out port for connecting to an external monitor.

SmartWi™ technology is an original Sony technology that seamlessly manages the 802.11a/b/g Wireless LAN, Bluetooth and the Wide-Area-Network (WAN) technologies, allowing users' to toggle between the various wireless connectivity options.

The UMPC has two built in digital cameras and they allow you to capture, share and participate in live chats. The image is viewable both in portrait and landscape formats.

The Sony performance is pretty good and includes a 1.3GHz Intel Core Solo U1500 CPU, 1 GB of DDR2 RAM and Intel 945GM graphics. It includes a 32GB solid state hard drive, which lends to faster data access, less heat, better battery life. Flash memory is also a good source for storage. The integration of flash memory reduces the time it takes to access programs, power up, and write data allowing the use of multiple applications efficiently and simultaneously. The battery life under normal conditions is 3 hours and 32 minutes, which is pretty good for a UMPC.
For Sony security is of utmost importance and the UX390 includes an integrated Biometric Fingerprint sensor ensuring device security. [Ackerman. (2007)].

Table 7: Sony VAIO UX390 Specifications

Description	Specifications
Processor	Intel® Core™ Solo Processor U1500
Memory	L2 cache 2MB/1GB RAM/DDR II SDRAM – 400 MHz
Hard drive	32GB/Removable
Chipset	Intel® 945GMS
Graphics	1024x600 (WSVGA)
Operating System	Windows Vista™ Business
Dimensions (WDH)	5.91x3.74x1.27-1.5
Screen size (diagonal)	4.5”
System weight	1.2
Category	UMPC

Sony. (n.d.). In VAIO UX Premium Micro PC. Retrieved December 28, 2007 from http://www.sonystyle.com/webapp/wcs/stores/servlet/ProductDisplay?catalogId=10551&storeId=10151&langId=-1&productId=8198552921665246465

5.3 Mobile Computing Security

One of the biggest concerns by security experts is mobile computing, especially when they are connected to the network. Searchmobilecomputing conducted a survey of 540 professionals, which included IT managers, business executives, consultants, mobile support staff, and network architects. Thirty-four (34%) percent of the respondents indicated that security was their biggest issue as more devices were attaching to the network. The second most prevalent concern at 28% was about the data stored on mobile devices. Respondents were also asked about the mobile security issues facing their organization. Seventy (70%) cited loss or theft of mobile device was their biggest concern and 49% were concerned about unauthorized network access. [Hickey. (2007)].

Craig Mathias the principal for the Fairpoint Group noted that security will continue to remain and mobile security was even more so excruciatingly painful. He goes on to say that their goal is to keep sensitive information secure by keeping the intruders off the networks. [Hickey. (2007). p.3].

In the gaming industry and like most other businesses, data loss or theft from deploying mobile devices can adversely impact the company's competitive position, reputation and result in regulatory fines and penalties. The key is to find a balance between usability and security.

How to Mitigate Security Threats

In the previous chapter on security, I have already addressed the risks associated with security breaches and they apply here as well. However, as it relates to mobile security threats, the following defensive techniques are suggested to prevent loss of data, network compromise and compliance and regulatory threats:

- A comprehensive and strategic plan should include security policies and strict enforcement of accountability. This information will be incorporated into the facilities business plan model.

- Mobile devices must be treated and protected like a desktop from a security standpoint. The same security software such as anti-virus, antispyware should be applied. Our current security policies will be modified to include these mobile devices and given security priority.
- The IT department should select the mobile devices and not employees. The company should own them and maintain control. This allows the IT department to upgrade software, firmware, apply patches and end-to-end encryption. This information will be covered under the IT policy and procedures manual.
- Only authorized applications should be installed on the device and steps should be put to prevent any unauthorized application to be added. This information will be covered under the IT policy and procedures manual.
- Develop proper usage policies and train the employees. Current standard operating procedures will be modified to accommodate the mobile devices and the change in processes.
- Both audit and monitor the mobile device activity to ensure employee compliance with security policies. The compliance department will play a significant role in ensuring compliance with the established policies and procedures.

In order to manage security risks for mobile devices, the first step is to define which mobile devices are applicable and under what circumstances. Limits should be applied to both network and application access, including data storage and transfer. Both security practices and measures should be implemented to monitor and enforce compliance. The following are some recommended security measures to secure mobile devices:

Power-On Authentication: To prevent the use of both lost and stolen devices.

File and/or Folder Encryption: To prevent unauthorized review of data.

Backup and Restore: To prevent against data loss and corruption.

Secure Communication: To prevent backdoor access and prevent eavesdropping.

Mobile Firewalls: To prevent wireless borne attacks

Mobile Antivirus & IDS: To prevent device compromise.

Application & Interface Authorization: To provide control for installing programs, network usage, synchronization and transfer of data between removable storage.

It is important to understand that the mobile computing environment is dynamic and an integrated management and security plan is necessary. In the end, regardless of the manufacturer of the devices, it is important to work closely with everyone in your infrastructure to find the most applicable security solution.

5.4 Emerging Technology: Mobile Internet Devices (MIDs)

Mobile Internet Devices (MIDs), compared to an Ultra-Mobile PC (UMPC) are smaller. A MIDs device screens are 4x6 inches, boot simplified Linux-based UIs with “instant on” performance. MIDs are also considered devices between mobile phones and computers.

According to Intel Senior Engineering Manager Danny Zhang and PengCheng Zou, Senior Manager of Red Flag Linux’s R&D department, Intel has developed a Tolapai chip, which integrates the Pentium core processor and the Integrated Graphics processor (IGP i915) to create what is essentially the Pentium M based system on chip. Additionally, the MIDs will have

256MB to 512MB of RAM, and Linux file-systems of 500MB. The screen resolution is expected to be 800x480 or 1024x600. Intel is also working on the “master user interface”, which will replace the ‘desktop’ as we know it and into something that can be carried around. [LinuxDevices. (2007)].

MIDs will run appliance-like Linux software stacks with four key objectives: 1) Stay in touch: instant messaging, videoconferencing, browsing, etc. 2) Be entertained: games, video, music, browsing, etc. 3) Access Info and Locate: shopping, points of interest, directions, etc. 4) Be Productive: remote access, internet, communication, collaboration, etc.

In short, the Mobile Internet devices provide a new category of small, mobile computing device while enabling a PC like internet experience. Intel is also working on the “master user interface”, which will replace the ‘desktop’ as we know it and into something that can be carried around. It also has the capabilities of communicating and accessing information from the WLAN to improve accessibility and efficiency of applications to service the customer. Intel expects that by 2010, the chip sales will reach 180 million annually for the MIDS (Mobile Internet Devices). Both Ultra Mobile PC (UMPC) and the Mobile Internet Devices (MIDs) provide the flexibility to access resources, communicate, access digital resources in a mobile environment and connect to the Internet. Both technologies will provide not only significant usage model, but also some new exciting growth opportunities redefining how they can best meet the business requirements while providing extreme mobility.

Chapter 6: Conclusions

6.1 Lessons Learned from the Project Experience

The project was conceptualized to assist the gaming industry develop a wireless handheld device. In the course of the project, I gained experience in setting up and deploying the wireless infrastructure to support the mobile handheld device. It included developing a site plan, understanding the various standards, and steps necessary to deploy the wireless infrastructure.

I also learned the importance of security and the catastrophic impact on businesses that are not adequately prepared to combat threats. I have a deeper understanding of the various types of security risks and steps to take in order to mitigate those risks.

Experience was also gained by learning about the Ultra Mobile PC (UMPC) and the Mobile Internet Devices (MIDs). They both appear to be a great solution as the mobile handheld device for this project. I had the opportunity to research several different manufacturers and narrowed the choice down to two popular vendors that met the project goals.

Finally, the goal of this project was to develop relevant expertise in identifying and deploying a wireless handheld device. This project provided that experience to learn wireless technology, security, and mobile computing devices to make this project work.

6.2 What might have been done differently?

Given the proper resources and time, I would have actually worked on designing a wireless handheld device. It would have included all the necessary functionalities and interfaces with the various applications to be workable.

In addition to the above thoughts, the experience would have been significantly enhanced if a real-working project had been deployed. Even though the requirements of this project were based on real life situations, I believe that objective was accomplished. The enclosed solution can or could have been deployed in real life.

6.3 What is the next stage of evolution for the project?

Incorporating the 802.11n when it becomes available will significantly enhance the productivity and satisfaction levels. The 802.11n standard depends on new technology and uses existing technologies to make Wi-Fi faster with better range. The new technology Multiple In, Multiple Out MIMO utilizes several antennas to transmit data streams from one location to another. Instead of sending one single data stream, MIMO transmits three streams and receives two allowing more data to be transmitted. This technique also increases both range and distance.

According to Dave Molta of InformationWeek, the 802.11n will be the popular WLAN standard by 2009. He recommends that transitioning from the 802.11 a/b/g standards in 2007 or 2008 is the difference between selecting an old or legacy technology versus one that is more powerful and strategic. Additionally, embracing new technology too soon, especially for a wide scale deployment can be inherently risky. [Molta. (2007)].

Also, as discussed in the previous section, I believe the UMPCs will be replaced by the MIDs. As the next generation MIDs get to market, they will be faster, easy to handle, and an effective way for mobile computing.

6.4 Summary

As previously stated, the project was a great learning experience and particularly one that can be deployed in real life. It began as a project to validate all the learning from the master's program and get a hands on experience. With each research and analysis, the project started to take a life of its own and I am extremely excited that the prospects of deploying this project for the gaming industry are extremely possible and relevant.

References

Ackerman, D. (2007). In Sony VAIO UX390. Retrieved December 28, 2007 from http://reviews.cnet.com/laptops/sony-vaio-ux390/4505-3121_7-32306444.html

Ackerman, D & Elliott, M. (2007). In Samsung Q1 Ultra (Vista Home Premium). Retrieved December 28, 2007 from http://reviews.cnet.com/laptops/samsung-q1-ultra-vista/4505-3121_7-32459191.html

Assureconsulting. (n.d.). In Wireless local area network. Retrieved December 2, 2007 from http://www.assureconsulting.com/articles/wlan.php

AT&T. (2007). In Implementing a WLAN: Good Planning is the Key to Success. Retrieved December 23, 2007 from http://www.business.att.com/nx_resource.jsp?repoid=Topic&rtype=Whitepaper&rvalue=implementing_a_wireless_lan&repoitem=mobility&segment=ent_biz

Certified Wireless Network Professionals. (2006). In WLAN Glossary. Retrieved November 20, 2007 from http://www.lever.co.uk/wlan-glossary.html#Decibel

Cisco. 2006. In Internetworking Basics. Retrieved December 9, 2007 from http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/introint.htm

Darknet. (2006). In Top 15 Security/Hacking Tools and Utilities. Retrieved December 27, 2007 from http://www.darknet.org.uk/2006/04/top-15-securityhacking-tools-utilities/

DpAC Technologies Corp. (2005). In Wireless Networking Basics. Retrieved December 2, 2007 from http://www.dpactech.com/docs/evaluation_support/DPAC_Networking_Basics.pdf

Extricom. (2007). In Coverage, Capacity and Bandwidth. Retrieved December 22, 2007 from http://www.extricom.com/content/products/faq/coverage-capacity-and-bandwidth

Federal Information Processing Standards Publication 197. (2001). In Announcing the ADVANCED ENCRYPTION STANDARD (AES). Retrieved December 26, 2007 from http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

Friday, S. (2007). In Wireless security: Keeping the Network Under Wraps. Retrieved December 26, 2007 from http://www.facilitiesnet.com/bom/article.asp?id=3743&keywords=wireless%20security,%20wireless%20networks,%20802.11

GNS Wireless. (2007). In 802.11a vs. 802.11b vs. 802.11g. Retrieved December 16, 2007 from http://www.gnswireless.com/AvsBvsG.htm

Greyfriars Consulting Group. (2004). In Different Types of Wireless Networks. Retrieved

December 2, 2007 from http://www.greyfriars.net/gcg/greyweb.nsf/miam/article01

Henderson, T. (2003). In WLAN Analyzers. Retrieved December 27, 2007 from http://www.networkworld.com/reviews/2003/0414rev.html

Hickey, A. (2007). In Mobile Security tops concerns, but policy isn't enforced. Retrieved December 28, 2007 from http://searchmobilecomputing.techtarget.com/originalContent/0,289142,sid40_gci1277383,00.html

InformIT. (2004). In Temporal Key Integrity Protocol (TKIP). Retrieved December 26, 2007 from http://www.informit.com/guides/content.aspx?g=security&seqNum=75

InformIT. (2005). In Wireless Intrusion Detection Tools, Part 2. Retrieved December 26, 2007 from http://www.informit.com/guides/content.aspx?g=security&seqNum=145&rl=1

ITtoolbox Research. (2007). In 2007 ITtoolbox Survey: Intrusion detection & Prevention. Retrieved December 27, 2007 from http://research.ittoolbox.com/surveys/survey.asp?survey=nokia_intrusion_survey&grid=4720&ref=http%3A%2F%2Fresearch%2Eittoolbox%2Ecom%2Fsurveys%2Fvendor%2Easp%3Fgrid%3D4720%26ref%3Dhttp%253A%252F%252Fresearch%252Eittoolbox%252Ecom%252Fwhite%252Dpapers%252Fnetworking%252Fsecurity%252Fan%252Dinteg

rated%252Dapproach%252Dto%252Dwireless%252Dintrusion%252Dprevention%252D3830%26kb%3Dsecurity%26sp%3DCM&kb=security

JiWire. (2005). In Understanding the Basics of Wi-Fi Security. Retrieved December 27, 2007 from http://download.jiwire.com/spotlock/userguide/whitepaper-security.pdf

Jacobs, D. (2007). In 802.11n creates systems integration opportunities. Retrieved December 24, 2007 from http://searchnetworkingchannel.techtarget.com/tip/0,289483,sid100_gci1255715,00.html

Kolodziej, K & Hjelm, J. (2006). Local Positioning Systems. Page 134. Retrieved December 16, 2007 from http://books.google.com/books?id=8Kn6nN8PMyIC&pg=PA134&lpg=PA134&dq=capacity+coverage+and+%22inter+access%22+point+spacing&source=web&ots=hvl1JpjiAb&sig=Y9xmQRXWemDvUXJPCi2Wr5Xwprc#PPA134,M1

LinuxDevices. (2007). In Intel debuts Linux-based "Mobile Internet Device". Retrieved December 28, 2007 from http://www.linuxdevices.com/news/NS8166710404.html

McDowell, M. (2007). In Understanding Denial-of-Service Attacks. Retrieved December 26, 2007 from http://www.us-cert.gov/cas/tips/ST04-015.html

Miceli, A. (2001). In Fear of Interference. Retrieved December 22, 2007 from http://telephonyonline.com/wireless/mag/wireless_fear_interference/

Microsoft TechNet. (2003). In What is QoS? Retrieved December 23, 2007 from http://technet2.microsoft.com/windowsserver/en/library/1c1f53a6-da9e-496f-be84-b91e2763dbeb1033.mspx?mfr=true

Microsoft TechNet. (n.d.). In IPsec. Retrieved December 26, 2007 from http://technet.microsoft.com/en-us/network/bb531150.aspx

Mitchell, B. (n.d.). In "Access Point Wireless." Retrieved December 9, 2007 from http://compnetworking.about.com/cs/wireless/g/bldef_ap.htm

Mitchell, B. (n.d.). In What is a VPN? Retrieved December 26, 2007 from http://compnetworking.about.com/od/vpn/a/what_is_a_vpn.htm

Molta, D. (2007). 802.11n Wireless: Is Now the Time to Deploy? InformationWeek. http://www.informationweek.com/story/showArticle.jhtml?articleID=202602009

Motion Computing. (2007). In Designing WLAN (802.11) to Support Tablet PC Mobility. Retrieved December 16, 2007 from http://www.motioncomputing.com/resources/wireless/Config_wireless_for_Tablets.pdf

Networkworld. (n.d.). In AES (Advanced Encryption Standard). Retrieved December 26, 2007 from http://www.networkworld.com/community/node/16348

Nortel Networks. (2005). In Engineering a WLAN Network. Retrieved December 9, 2007 from http://i.i.com.com/cnwk.1d/html/itp/NTN2018Engineer_Final.pdf

Nutter, R. (2005). In Fixing 802.11b Link Performance Problems. Retrieved December 11, 2007 from http://www.networkworld.com/columnists/2005/021405nutter.html

Ou, George. (2007). Ultimate Wireless Security Guide: An introduction to LEAP authentication. Retrieved December 3, 2007 from http://articles.techrepublic.com.com/5100-1035-6148551.html

PCI. (n.d.). In About PCI Data Security Standard (PCI DSS). Retrieved December 27, 2007 from https://www.pcisecuritystandards.org/tech/index.htm

Pentikousis, K. (2000). In Can TCP be the transport Protocol for the 21st Century? Retrieved December 23, 2007 from http://www.acm.org/crossroads/xrds7-2/tcp21.html

Phifer, L. (2006). In WiFi Vulnerability assessment checklist. Retrieved December 27, 2007 From http://searchsecurity.techtarget.com/general/0,295582,sid14_gci1167666,00.html?track=wsland

Phifer, L. (n.d.). In Managing WLAN Risks with Vulnerabilities and Assessment. Retrieved

December 26, 2007 from www.airmagnet.com/assets/whitepaper/WLAN_Vulnerabilities_White_Paper.pdf -

Propagate Networks. (2003). In AutoCell – The Self-Organizing WLAN. Retrieved December 22, 2007 from http://www.propagatenet.com/news/docs/wpaper_autocell_soWLAN.pdf

RAD. (n.d.). In Cyclic Redundancy Check (CRC). Retrieved December 26, 2007 from http://www2.rad.com/networks/1994/err_con/crc.htm

Shah, A. (2003). In Saving spectrum: ad-hoc frequency planning a must as wireless operators move to 3G – Wireless. Retrieved December 22, 2007 from http://findarticles.com/p/articles/mi_m0NUH/is_2_37/ai_97757993

Sony. (n.d.). In What is an Ultra Mobile PC? Retrieved December 28, 2007 from http://my101.learningcenter.sony.us/briefs/viewBrief.jsp?courseId=13708&webPageId=1000005

Sony. (n.d.). In VAIO UX Premium Micro PC. Retrieved December 28, 2007 from http://www.sonystyle.com/webapp/wcs/stores/servlet/ProductDisplay?catalogId=10551&storeId=10151&langId=-1&productId=8198552921665246465

TechWeb Network. (n.d.). In AES-CCMP. Retrieved December 26, 2007 from http://www.techweb.com/encyclopedia/defineterm.jhtml?term=AES-CCMP

The RTS/CTS Mechanism. (n.d.). Retrieved December 16, 2007 from http://nislab.bu.edu/sc546/sc546Fall2002/blocknode/understandingrts.html

The TECH-FAQ. (n.d.). In What is a Rogue Wireless Access Point? Retrieved December 2, 2007 from http://www.tech-faq.com/rogue-access-point.shtml

The TECH-FAQ. (n.d.). In What is WEP (Wired Equivalent Privacy)? Retrieved December 26, 2007 from http://www.tech-faq.com/wep-wired-equivalent-privacy.shtml

Virginia Polytechnic Institute and State University. (2002). In Center for Wireless Telecommunications. Retrieved December 2, 2007 from http://www.cwt.edu/faq/default.htm

WAVE Report. (2007). In OFDM Tutorial. Retrieved December 11, 2007 from http://www.wave-report.com/tutorials/OFDM.htm

Whatis.com. (2006). In Bandwidth. Retrieved December 9, 2007 from http://searchnetworking.techtarget.com/sDefinition/0,,sid7_gci211634,00.html

Wi-Fi Planet. (2002). In DSSS. Retrieved December 11, 2007 from http://wi-fiplanet.webopedia.com/TERM/D/DSSS.html

WiFi Alliance. (2007). In Next-Generation Wi-Fi a Reality with More Than 95 Products Wi-Fi CERTIFIED™ for 802.11n Draft 2.0. Retrieved December 24, 2007 from http://www.wi-fi.org/pressroom_overview.php?newsid=618

Wilson, J. (2004). In Quadrupling Wi-Fi speeds with 802.11n. Retrieved December 23, 2007 from http://deviceforge.com/articles/AT5096801417.html

Wiretapped. (n.d.). In Network Mapping. Retrieved December 27, 2007 from http://www.wiretapped.net/indexes/network-mapping.html

Wright, J. (2004). In asleap recovers weak LEAP passwords. Retrieved December 26, 2007 from http://asleap.sourceforge.net/README

ZDNet. (2007). In Research: Mobile working on the increase. Page 7. Retrieved December 27, 2007 from http://www.zdnet.co.uk/misc/print/0,1000000169,39289565-9001117c,00.htm

Appendix

Appendix A: Vulnerability Assessment Documents

Note: adapted from Phifer, L. (n.d.). In Managing WLAN Risks with Vulnerabilities and Assessment. Retrieved December 26, 2007 from www.airmagnet.com/assets/whitepaper/**WLAN**_Vulnerabilities_White_Paper.pdf -

The following documents should be used to compile results during a vulnerability assessment. There is no standard form and the utilization will depend on your own specific architecture and the documents should be used to setup a baseline for monitoring and testing vulnerabilities.

Test Date						
Tester MAC(s)						
AP	Number	Station	Number	Other	Number	Assigned ESSIDs
802.11b		802.11b		Micro Waves		Employee Intranet =
802.11g		802.11g		Cordless Phones		Guest Intranet =
802.11a		802.11a		Bluetooth Devices		Other =
802.11n		802.11n		Video Cameras		
WLAN Bridges		Ad Hoc Stations		Other RF Sources		

Intended / Deployed WLAN Characteristics

Site Survey Floor Plan and Test Locations

AP Inventory

AP MAC	ESSID	Ch#	IP Address	SNR	Owner	Location	Classification
: : : : :							
: : : : :							
: : : : :							

AP MAC	Protocol Types	SSID Beacon	802.11 Encrypt	PSK	802.1X	EAP Types	Other
: : : : :							
: : : : :							
: : : : :							

Station Inventory

STA MAC	Last ESSID	Last Ch#	SNR	Owner	Location	Adapter	Classification
: : : : :							
: : : : :							
: : : : :							

1.	**Insert floor plan here**
2.	Mark testing locations on floor plan
3.	Describe testing locations at left
4.	(or generate from Survey/Planner)
5.	

STA MAC	Protocol Types	Assoc ESSIDs	802.11 Encrypt	PSK	802.1X	EAP Types	EAP User ID
: : : : :							
: : : : :							
: : : : :							

Network Scan Results: Discovered Devices (Complete for each VLAN/Subnet)

Role	MAC Address	IP Address	Owner	Notes
WLAN Controller	: : : : :			
DHCP Server	: : : : :			
DNS Server	: : : : :			
RADIUS Server	: : : : :			
Access Points	: : : : :			
Stations	: : : : :			
Other	: : : : :			

AP Test Results (complete for each tested AP)

AP MAC	: : : : :	AP IP Address	
Virtual AP?		VLAN ID	
OS/Version			
Open TCP/UDP Ports		Service Banners Returned	
SNMP Admin Used?		SNMP Community Strings	
Telnet Admin Used?		Telnet Login / Password	
Web Admin Used?		Web Login / Password	
Blocks Broadcasts?		Blocks station-to-station?	

Blocks WLAN SNMP?		Blocks WLAN Routing?	
Accepts Spoofed ARP?		Physically secured?	
Encryption off?		Observed Encryption Types	
WEP Weak ICs?		Cracked WEP Keys	
MAC ACL Used?		Valid Station MACs	
PSK Guessable?		Cracked PSK	
802.1x Required?		Observed EAP Types	
AP DoS Test Results		RF Interference Sources	

Station Test Results (Complete for each tested station)

Station MAC	: : : : :	Static IP Address?	
OS/Version		VLAN ID?	
Open TCP/UDP Ports		Service Banners Returned	
NETBIOS Name		NETBIOS Shares	
NETBIOS Service List		NETBIOS User/Group List	
Assoc with ANY AP?		Assoc with Ad Hoc Peer?	
Encryption off?		Observed Encryption Types	
WEP Weak IVs?		PSK Guessable?	
802.1x Used?		Observed EAP Types	
802.1x IDs Exposed?		Observed 802.1x User ID	
LEAP Used?		Cracked User Password	
Applications Protocols		Observed Servers & Logins	

WLAN Infrastructure Test Results
(Complete for each tested controller / switch / server)

Device MAC	: : : : :	Device IP Address	
OS/Version		VLAN ID	

Open TCP/UDP Ports		Service Banners Returned	
SNMP Admin Used?		SNMP Community Strings	
Telnet Admin Used?		Telnet login / Password	
Web Admin Used?		Web Login / Password	
Accepts spoofed ARP?		Physically secured?	
Uses RADIUS Server?		RADIUS Test Results	
Acts as DNS Server?		DNS Test Results	
Acts as DHCP Server?		DHCP Test Results	
Acts as VPN Gateway?		VPN Test Results	
Acts as Web Portal?		Web Server Test Results	

The following table summarizes WLAN analyzer and Wireless IPS security alerts. They correspond to both anomalies and attacks that were noted during the vulnerability assessment period. Any security policy and rogue device variances should be noted in the Station or Access Point List.

Detected Attacks & Anomalies

Types of Event	Source Address	Dest Address	Time	Location	Observations & Details
Network DoS Attacks - CTS Flood - Queensland DoS - PS Poll Flood - Virtual Carrier Attack - RF Jamming - RF Spectrum Interference					

AP DoS Attacks - 802.11 Association Flood - 802.11 Authenticate Flood - 802.11 MIC DoS Attack - 802.1x EAP Start Flood - 802.1x EAP of Death - Fuzzing Attacks (illegal 802.11 packets)					
Station DoS Attacks - 802.11 Deauth Flood - 802.11 Deauth Broadcast - 802.11 Disassociate Flood - 802.11 Disassociate Broadcast - 802.1x EAP Failure - 802.1x EAP Logoff Flood - Wireless driver Exploits - PSPF Violation					
Reconnaissance Activities - NetStumbler - Wellenreiter - FATA – Jack - AirSnarf - MAC Address Spoofing					
Evil Twin / MitM Activities - Fake AP Detected - Fake DHCP Server - Hotspotter Detected - SoftAP or HostAP - AP in Bridged Mode - Suspicious ESSIDs					

Spoofing / Cracking - MAC Spoofing - Fast WEP Crack Attack - ASLEAP Attack - EAP Dictionary Attack - EAP Type Attack					