Deployment Issues And Security Concerns With Wireless Local Area Networks: The Deployment Experience At A University

Paramjit S. Kahai, (E-mail: pkahai@uakron.edu), University of Akron
Simran K. Kahai, (E-mail: skahai@jcu.edu), John Carroll University

Abstract

This paper presents and discusses various issues pertaining to the deployment of Wireless Local Area Networks (WLANs). The popularity of WLANs has steadily increased in the last two years and has led to their deployment in a variety of organizations. Yet, making a business case for WLANs is an important step in their deployment. In addition to highlighting the need for a business case for WLAN deployment, the paper outlines the reasons for, benefits of, and security problems associated with, their deployment. The latter part of this paper presents a case study about the deployment of a WLAN at the University of Akron. Therein, it discusses the context for the deployment, the process that was used to justify the deployment, and the efforts made to protect users' information from security deficiencies of wireless networks.

Introduction

The popularity of wireless local area networks (Wireless LANs or WLANs, for short) has steadily increased in the last two years and has led to their deployment in a variety of organizations. Wireless connectivity is now available at airports, hotels, and Starbucks outlets that, among others, have created wireless *hotspots* to allow people to connect to the Internet, for a fee, at speeds of up to 11 Mbps. Many university campuses have also invested in WLAN infrastructure to move faculty, staff, and students into the world of *wireless mobility* (Gaspar, 2002; Green, 2003). The result is that in the third quarter of 2003, shipments of WLAN equipment totaled 12 million units, a 22 percent quarterly growth rate from the 9.9 million units shipped in the second quarter of 2003 (In-Stat/MDR, 2003). Sales of WLAN client devices are expected to hit 8.7 million units in the second quarter of 2004 (Botelho, 2003).

The University of Akron recently deployed a WLAN on its campus. The deployment was a part of the strategic vision outlined by the university president in 1999. There were at least two important aspects of this deployment. One, it was acknowledged that Information Technology (IT) played a vital role in student success. Two, a planned approach was followed to not only justify the deployment but also to subsequently translate the vision into deliverables. Going the wireless route was a very cost-effective strategy for Akron. Since a wired infrastructure was already in place, one option to satisfy the need for additional network connectivity was to supplement the existing infrastructure with additional wired equipment. However, as we discuss later, the wireless infrastructure was relatively less expensive and faster to implement.

Consequently, the purpose of this paper is twofold. First, we provide an overview of general deployment issues and security concerns related to WLANs. Second, we present a case study about the deployment at the University of Akron. The former overview provides a context for the case study which, subsequently, outlines how these issues were dealt with at the university. In addition, the paper discusses the need for adequately justifying the implementation of WLANs and the benefits that ensue as a consequence. This paper, therefore, fills a gap in the

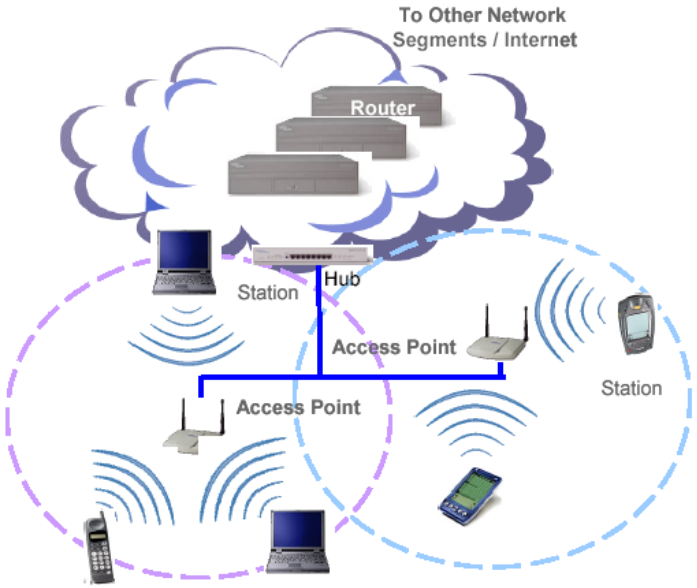
literature by coherently presenting a discussion of these topics, some of which are found in a wide variety of disparate sources.

The paper is organized as follows. First, background material related to WLAN technology is presented. Next, the reasons and business justification for WLAN deployment are outlined. This is followed by a discussion of security problems with WLANs and the solutions that have been proposed for these problems. Then, a case study about the deployment of a WLAN on the campus of the University of Akron is presented. Finally, implications and conclusions are outlined.

Background

Implementing a wireless LAN involves setting up an infrastructure consisting of multiple access points (AP) as shown in figure 1. Usually, APs are connected to an existing wired LAN infrastructure that provides connectivity to the network and to the Internet. Computers that are equipped with wireless Network Interface Cards (NICs) then communicate with the nearest AP which provides simultaneous network connectivity to multiple computers.

Figure 1. Wireless LAN Architecture



Source: Karygiannis & Owens (2002).

Needless to say, there is a distance limitation with WLANs. Although distances of 1,500 feet from an AP are possible, realistically, 150 feet are more practical inside buildings. Thus, conducting a site survey is an important step before any infrastructure is put in place (Geier, 2003). The survey's purpose is to determine where APs have to be located to provide uninterrupted wireless connectivity to users. Since signals can be disrupted and deflected by intervening objects, it is critical that the site survey be done in a very systematic manner so as to locate APs appropriately.

Currently available WLAN equipment is based on one of three Institute of Electrical and Electronics Engineers (IEEE) standards – collectively referred to as 802.11 standards – that have been ratified to date. These standards include 802.11a, 802.11b, and 802.11g. There are some differences among these standards (see Varshney, 2003, for a detailed discussion about the technical differences among these standards); these are presented in table 1. Although 802.11b (also known as Wi-Fi for Wireless Fidelity) WLANs have been the most implemented until now,

WLANs based on the 802.11g equipment are steadily gaining ground (Lingblom, 2003). Equipment based on the 802.11g standard is backward compatible with 802.11b equipment because both operate in the 2.4 GHz frequency range. Thus, companies that have invested in 802.11b WLANs will have an easier migration path to 802.11g.

Table 1 IEEE 802.11 Standards

Standards Characteristics	**802.11a**	**802.11b**	**802.11g**
Data Rate (Communication with AP)	Up to 54 Mbps	Up to 11 Mbps	Up to 54 Mbps
Frequency of Operation	5 GHz	2.4 GHz	2.4 GHz
Compatible with 802.11b	No		Yes

Reasons And Justification For WLAN Deployment

According to the Wi-Fi Alliance (2001), one of the major reasons for deploying WLANs is mobility. Users who are on the go or need to be mobile within an office complex generally would prefer to have access to their e-mail or resources on an Intranet for meetings or providing needed information to clients or customers. Such users equipped with a laptop that has a wireless NIC are able to get access to network resources and the Internet (assuming, of course, that wireless infrastructure is in place). Thus, wireless connectivity is always most beneficial for, and is most used by, mobile users (Wi-Fi Alliance, 2001).

A second reason is the high expenses of wiring buildings, both for access to the network and possibly for electrical outlets. It usually turns out to be less expensive to install wireless APs than it is to wire for network jacks. Network wiring involves laying cable either through available ducts in the floor or through ceilings and walls. Such cabling can involve a lot of effort and expense, both of which can be avoided if wireless infrastructure is used.

A third reason for WLAN deployment is the ability to provide network connectivity in places where providing wired connectivity is difficult. On university campuses that have older buildings which were not pre-wired for network connectivity, providing wall jacks becomes a difficult task. Also, in situations where network connectivity needs to be set up on a temporary basis, wireless connectivity can be provided relatively easily and less expensively.

The Business Case for WLAN Deployment

Although the above reasons provide compelling justifications for deploying WLANs, quite often a sound business case needs to be made before deployment can proceed. Making a business case for a WLAN implementation, however, is not a simple task, especially when things like return-on-investment (ROI) calculations are involved (Worthen, 2002). The problem with ROI is that it forces one to focus on financial factors such as cost savings, increased savings, increased revenues, and the like (DeGiglio, 2001; Sawhney, 2002). One assumes, therefore, that the benefits a firm derives from the use of WLANs are of a tangible nature, which can then be directly related to the financial factors mentioned above. Tangible benefits notwithstanding, quite often, the benefits of a WLAN implementation are intangible and cannot necessarily be related to financial gains or savings (Korostoff, 2003).

Several articles have appeared in the popular press that outline the benefits – some tangible, some intangible – of using WLANs. These are summarized in table 2. The benefits of using WLANs are many and include, among others, increased productivity, increased sales, and improved customer satisfaction. In an academic environment, benefits include turning-in assignments any time, the ability to use laptop labs, and being able to compute in class.

Table 2 Benefits of Deploying and Using WLANs

Source & Setting	Tangible Benefits	Intangible Benefits
Cosgrove (2002) *Corporate*	• Increased productivity • Increased sales • Reduced expenses/costs of doing business	• Improved customer satisfaction (internal & external customers) • Reduced sales cycle • Streamlined processes/greater efficiencies
Cox (2002) *Hospital*	• Boosting the number of patients served • Speeding payments and billing cycles	• Improving quality of physician diagnosis
Dubie, Jacobs, and Ohlson (2002) *Hospital, Hotel, & Corporate*	• Productivity gains • Immediate access to patient records • Efficiency • Safety (without wires) • Reduce pricing errors	• Spend more time with patients • Convenience • Help conduct business better
Gaspar (2002) *University*		• Stretching student learning beyond the classroom • Turning-in assignments any time • Ability to use laptop labs • Access to resources in class enhances productivity • Working anywhere using a wireless laptop

Tools and resources are now available that allow firms to compute ROI of WLAN implementations. One example of a tool is the *WLAN Benefits Calculator* available on the Internet from the Wi-Fi Alliance at http://www.wi-fi.org/OpenSection/WLAN_Calculator.asp. The tool is in the form of a Microsoft Excel spreadsheet and "calculates ROI based on the productivity gains associated with increased access to the corporate network" (Wi-Fi Alliance, 2003B). The tool's primary focus is on financial factors that, as stated above, fail to consider other tangible and intangible benefits that result from WLAN implementations.

An example of a resource to consider is a recent white paper from Intel Corporation (Intel Corporation, 2002). The document describes the process that Intel used to develop a business case for WLAN implementation in the entire company. Intel's IT group successfully completed "the difficult task of linking return on investment (ROI) to productivity gains from wireless LANs" (Intel Corporation, 2002; p. 2). Although the group cautions that WLAN deployments in other organizations may differ from that of Intel's, it provided a somewhat planned approach to quantifying benefits of wireless initiatives.

Problems With Wireless Deployment

There are several problems one needs to be aware of when contemplating deployment of WLANs. Of the several that have been discussed in the literature, security weaknesses have received the greatest attention (Cam-Winget, Housley, Wagner, and Walker, 2003; Housley and Arbaugh, 2003; Karygiannis and Owens, 2002). Several of these issues relate to vulnerabilities of the encryption protocol, referred to as *Wired Equivalent Privacy (WEP)*, used to encrypt information traveling between the computer and the AP; other issues relate to authentication mechanisms used to allow users and computers to connect to the network. Each of these is now briefly discussed.

Problems with Authentication and WEP

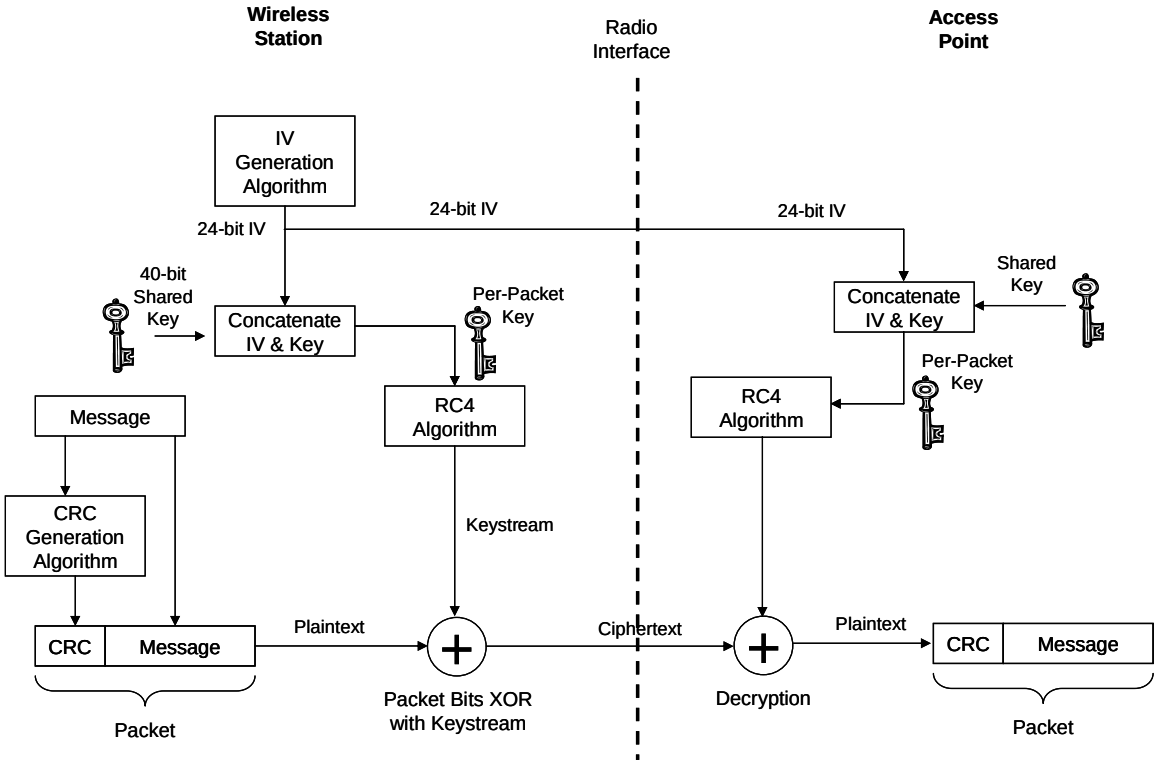
WEP, as the name suggests, is supposed to, in a wireless environment, provide security equivalent to that inherent in a wired network. In practice, though, it falls rather short of providing that security. WEP will stop a casual hacker but someone equipped with the right tools that are available free on the Internet will be able to easily

defeat WEP. To understand the vulnerabilities associated with WEP, a close look at the encryption process (see Figure 2) is necessary.

As is well-known, a *key* is needed to perform the process of encryption. The original specification for 802.11 networks specifies a 40-bit key that is concatenated with a 24-bit initialization vector (labeled IV in the figure) to give a 64-bit key. Application of the *RC4* algorithm to the 64-bit key results in a stream of bits referred to as a *keystream*. The encryption process involves performing an *exclusive-OR* operation (labeled XOR in the figure) between the data packet and the keystream, the output of which is the encrypted data (labeled ciphertext in the figure). Once the encrypted packet gets to the AP, it is decrypted using the same 64-bit key that was originally used to encrypt it. Herein lie several problems.

No user and mutual authentication. This vulnerability relates to the technique used to allow computers to join a wireless network. APs and NICs use a *Service Set Identifier (SSID)* as a password for *associating* with a network (Blackwell, 2002). Quite often, it is left unchanged from its default setting which is widely known (for e.g., *tsunami* is the default SSID used in Cisco equipment). The SSID is also broadcast by APs on a regular basis and can be *sniffed* easily with software tools available free on the Internet. In addition, Windows XP is able to sniff available wireless networks based on the SSID broadcast from an AP.

Figure 2 WEP Depicted



Source: Karygiannis and Owens (2002).

Once the SSID is known, a user equipped with a computer and a wireless NIC can easily connect to a WLAN because no user authentication is performed. Of course, a user needs to have the encryption key to be able to join the network. As will be discussed shortly, the key can be easily discovered. Once discovered, any user can join the network without being authenticated at all. Further, computers and APs do not authenticate each other prior

to establishing communications, which could lead to a user to unknowingly connecting to a *rogue* (unauthorized) AP.

Key is static and shared. The 40-bit key used to encrypt data is *static* in nature. That is, once it is entered into the computers and APs, it does not change. Changing the key involves manually modifying it in all computers and APs, a very time-consuming and difficult job (to say the least) in large networks. The 802.11 standard also did not provide mechanisms for automatically changing encryption keys. The result is that keys are rarely changed. Further, the key is shared among all devices on the network. A shared key, per se, is not a security risk; it is a risk only when it is discovered. Once discovered, it becomes easy to connect any device to the WLAN.

Encryption algorithm is flawed. It has been recently shown that the RC4 algorithm is flawed (Fluhrer, Mantin, and Shamir, 2001). The algorithm results in a large number of *weak keys*. Information encrypted with such keys is easily compromised. Further, wireless traffic can be easily intercepted and keys easily discovered with tools available free on the Internet. A determined person can then intercept and decrypt messages as they travel between a computer and an AP.

IV is short. In the 802.11 standard, how the IV is generated has, unfortunately, not been standardized (Network World, 2002). With a 24-bit size, the maximum number of unique IVs that can theoretically be generated equals 2^{24}, i.e., 16,777,216. Practically, though, far fewer IVs may be generated. For a given WEP key, different IVs will result in different keystreams. A large network, however, could generate enough traffic for the IV and, consequently, the keystream to be repeated, leading to easy discovery of the key (Network World, 2002).

Key is short. The original 802.11 specification supports only a 40-bit key size. Although the 40-bit key is concatenated with a 24-bit IV to produce a 64-bit key for encryption purposes, the IV is sent in the clear with every packet of data. The IV can, thus, be easily *sniffed* using easily available tools. Of the 64 bits, therefore, 24 bits are known; the remaining 40 bits are too few in number to foil a determined hacker. A case can be made for having longer keys because, generally, the longer the key, the more difficult it is to crack it. However, no matter how long the key is, the number of unique keystreams will be restricted to the number of unique IVs generated.

WEP is disabled by default. WEP is turned off by default in WLAN equipment. For unwary users, this default setting is dangerous. Although hackers are not sitting outside every building and office complex trying to intercept signals, several websites on the Internet (see, for example, http://www.wardriving.info and http://www.warchalking.org) list locations of unprotected wireless networks around the U.S. and the globe. Needless to say, the efforts of determined hackers who may exploit the availability of such networks could easily lead to major disasters within any organization. One should, therefore, endeavor to make sure that, at the minimum, WEP is turned on when setting up a network because *some* encryption is better than no encryption at all!

To summarize, there are a variety of security problems related to WLANs. It is a given that signals that travel through the air are easily intercepted. An easy, but unrealistic, way to avoid signal interception is to actually disband a wireless network! However, the industry and standards bodies are addressing the need for better encryption mechanisms and overall security of wireless transmissions, a topic that we now turn to.

Solutions To WLAN Security Vulnerabilities

Although there are a multitude of vulnerabilities related to WLAN deployment, several companies such as Cisco, Colubris, 3Com, and Avaya offer proprietary solutions that "plug holes" in 802.11 networks (see Janss, 2001). However, the Wi-Fi Alliance[1] recently ratified a set of standards-based interim enhancements, collectively

[1] "The Wi-Fi Alliance is a nonprofit international association formed in 1999 to certify interoperability of wireless Local Area Network products based on IEEE 802.11 specification. Currently the Wi-Fi Alliance has 205 member companies from around the world, and 915 products have received Wi-Fi® certification since certification began in March of 2000. The goal of the Wi-Fi Alliance's members is to enhance the user experience through product interoperability" (http://www.wi-fi.com).

referred to as *Wi-Fi Protected Access (WPA)*; the IEEE, too, is working towards a standard, 802.11i, that will alleviate the security problems. We now briefly outline these standards-based solutions.

Standards-Based Solutions

In October 2002, the Wi-Fi Alliance, working in conjunction with the IEEE, announced Wi-Fi Protected Access (WPA), a replacement for WEP. The goal of WPA was to address all the security deficiencies of WEP and provide a user authentication mechanism that was missing from the original 802.11 standards.

The authentication protocols are based on the use of the IEEE 802.1x protocol (802.1x uses Extensible Authentication Protocol - EAP) that relies on a RADIUS[2] (Remote Authentication Dial-In User Service) server to mutually authenticate a client and server, and also provide user authentication using a variety of credentials, such as digital certificates and smart cards, in addition to usernames and passwords (Wi-Fi Alliance, 2003A). For small office and home office (SOHO) environments that may not able to configure and maintain a RADIUS server, authentication is based on the use of a "pre-shared key (PSK)" or password. Unlike in WEP, the PSK here is not an encryption key; it is a password used to allow clients to connect to a WLAN. Unique encryption keys are still dynamically generated and assigned to each user and for each session (Griffith, 2002).

For encryption, WPA uses the same RC4 algorithm used in WEP but adds the Temporal Key Integrity Protocol (TKIP) that specifies a key size of 128 bits instead of the 40-bit size specified in WEP. The keys are also dynamically generated and assigned by the authentication server that overcomes the problem with static keys in WEP. In addition, a Message Integrity Check (MIC) is calculated and compared by both the sending and receiving devices to see if packets have been tampered with. Table 3 summarizes the major security vulnerabilities of WEP and how they have been addressed by WPA.

Table 3. Summary of WEP Problems Addressed by WPA

Problems With WEP	How WPA Addresses WEP Problems
No mutual and user authentication	Uses 802.1x authentication (EAP with a RADIUS server) for both device and user authentication. User authentication can occur using a variety of credentials
Key is static and shared	Uses TKIP where each user on the network is assigned a different key. Also, unique session keys are dynamically generated for each session
Encryption algorithm is flawed	TKIP extends the RC4 algorithm to include per-packet keys along with a message integrity check. Distribution of keys is no longer manual
IV is short	Increased the size if IV from 24 bits to 48 bits
Key is short	Key size increased from 40 bits to 128 bits
WEP is disabled by default	Manufacturers plan to have WPA enabled by default

WPA is just an interim step towards, and a subset of, a set of security standards that the IEEE is working on; these are collectively referred to as 802.11i or WPA2 (Wi-Fi Alliance, 2003A). A major change in WPA2 will be the use of a new and more robust encryption scheme, the Advanced Encryption Standard (AES). Upgrading to AES will require a hardware upgrade, unlike just a software upgrade required for migration from WEP to WPA. Yet, WPA2 will allow the use of both WPA and WPA2 clients on a network, thus making WPA forward-compatible with WPA2.

[2] According to webopedia.com (http://www.webopedia.com/TERM/R/RADIUS.html), although RADIUS is "not an official standard, the RADIUS specification is maintained by a working group of the IETF." The task of the RADIUS server is to provide authentication services through the use of usernames and passwords. Unless a user provides the correct combination of username and password, s/he is not allowed access to the network and its resources.

Wireless Deployment At The University Of Akron[3]

The Genesis of the WLAN

The University of Akron is the third largest state university in Ohio with over 25,000 students enrolled in a variety of programs. In January 1999, Dr. Luis M. Proenza arrived as the 15th President of the university with a vision of making it a leader in a variety of areas. His vision was embodied in a document titled *Charting the Course: A Strategic Planning Report* (Proenza 2000) that focused on two strategic priorities: *Student Success* and *Information Technology Leadership*. Given the impact of IT on the "knowledge" economy, the report acknowledged that IT leadership was vital to student success in the future. The initiative employed to attain leadership in IT was appropriately dubbed *Technology Without Boundaries*SM (The University of Akron, 2000) which "ensures that both students and faculty have access to technology that will promote and enable education, communication, and collaboration."

In March 2000, Dr. Thomas Gaylord was tapped to be the Chief Information Officer (CIO) of the university. His appointment coincided with the creation of the Vice President/Chief Information Officer (VP/CIO) Division. Among Dr. Gaylord's top priorities was to set IT strategy to help achieve the strategic IT vision that Dr. Proenza had begun to outline. One of the outcomes of their efforts was the campus-wide wireless laptop initiative.

The State of IT

When Dr. Gaylord arrived as the CIO, computer access and use by students was an issue at the university. There were eight general-purpose computer labs spread across various buildings on campus; one of the labs was in Bierce Library, the main library on campus. Each lab had about 24 to 30 computers that were beginning to be obsolete. Further, the labs were starting to be overcrowded, especially during the last two weeks of the semester. Each college also had its own computer labs but they were generally reserved for students enrolled in those colleges.

During the last decade of the 20th century, the university had not been investing money into the development of Information Technology (IT) on campus due to the lack of funds caused by declining enrollment. The network architecture was not up-to-date and over-utilized. The library building could quite possibly accommodate another computer lab but simply did not have adequate power supply and network "drops." In commenting about the inadequacy of power supply at the library, Dr. Gaylord indicated that adding another lab in the library would have been like "putting one too many lights onto the Christmas tree!" Something out of the ordinary had to happen, something along the lines of "thinking outside the box."

Dr. Gaylord's began his quest for a solution by doing several assessments of the computer and network infrastructure on campus. In addition, he studied the situation at the library by spending an entire day there in the computer lab. His assessment was that the space in the library was much underutilized – "no people, a lot of space" – and that the lab atmosphere was unproductive – "there is no way you could get any work done in the lab." A cost analysis was performed to find out the possibility of housing an additional computer lab in the library. The fixed cost for hardwiring and providing power outlets alone would total $800,000! A determination was made to investigate the possibility of implementing a wireless system in the library with a view to rolling it out campus-wide.

The Beginning of the Wireless Infrastructure

The process of designing a wireless infrastructure included a site survey performed by a local company. The site survey was a vital step in designing the infrastructure because it dictated the locations of APs that would provide uninterrupted wireless service across campus. Interestingly, analysis indicated that installation of APs in the

[3] This section is an agglomeration of information gleaned from a variety of sources: interviews and conversations with the Chief Information Officer (CIO) and WLAN Administrator, documents available on the university web site, and a term paper written by graduate students in a graduate Telecommunications Management class taught by one of the authors. We would like to express our gratitude to the CIO and WLAN Administrator for taking the time to talk to us, and to the graduate students for permitting us to use selected information from their term paper.

library to provide wireless service coverage would cost only $80,000, exactly one-tenth of the estimate of $800,000 to hardwire and provide power outlets!

In December 2000, a campus-wide task force was formed to help begin the implementation of the wireless infrastructure. Around the same time, Cisco Systems purchased a small Akron-based wireless equipment company called Aironet that developed and started manufacturing, among other things, APs and NICs for 802.11b WLANs. Having a long-standing networking relationship with Cisco, the university proposed to become a beta testing site for this new technology. After beta testing, and a series of meetings and discussions, Cisco Systems agreed to provide all of the necessary equipment (APs and PC cards) to showcase the wireless LAN on the entire 162 acres of the university campus.

Before campus-wide rollout, a pilot was conducted in the library and in the Law School beginning with the spring 2001 semester. The main idea behind the pilot study was to gather information from a small group, establish a controlled test area, create a positive marketing environment, and gradually start getting people familiar with the new technology. About 346 IBM ThinkPad laptops equipped with Cisco Aironet wireless NICs were utilized for this pilot effort and distributed among various entities as shown in table 4. Various security mechanisms were put in place to assure physical security of the hardware. A customer satisfaction survey was also conducted during pilot testing. A majority of users were satisfied with the new technology as well as with the operational issues. It was not surprising that mobility, ease of use, and convenience were most often mentioned as benefits by users. Battery life and limited connectivity (limited to locations where APs were installed for the pilot), among others, were mentioned as disadvantages by users.

Table 4. Laptop Distribution for Pilot

School of Law First-Year Students (160), Faculty (30), & Staff (30)	220
Library (For Lending to Students for Use Within the Library)	60
Faculty Senate Computing Committee	11
Delta Gamma Sorority	15
VP/CIO Division	30
Maintenance Stock	10

Source: O'Connor and Richert (2001).

Campus-Wide Rollout

After a successful completion of the pilot, and analysis of user feedback, plans were set in motion for a campus-wide rollout of the WLAN. As the pilot was underway, the campus networking staff was busy installing wireless APs and upgrading switches to take the university to the next level of network connectivity. Meantime, the Faculty Senate Computing Committee (included in the pilot program) voiced support for the wireless initiative. The committee also endorsed plans for leasing wireless NIC-based IBM laptops and providing them to all full-time tenured and tenure-track faculty members.

By the fall semester of 2001, the campus wide wireless rollout was already in full swing. The installation of approximately 600 APs neared completion. Faculty laptops were being phased-in by college. By the Spring semester of 2002, the rollout was complete. No outside consultants were hired for the rollout; only existing professionals and internal personnel were recruited for the management and implementation. Within a span of two years from the time Dr. Gaylord arrived, a patchwork of network technology was converted into state-of-the-art technology.

Along the way, in October 2001, the university received accolades for its wireless initiative from Yahoo! Magazine; it recognized Akron as the best wireless campus in Ohio. At the university, Internet use spiked to three

times its previous level after the wireless implementation (Harmon, 2002). According to Dr. Gaylord, what really made an impact was the fact that all the technology was implemented campus-wide over a very short period of time.

The Wireless Infrastructure on Campus

Currently, about 750 Cisco Aironet 340, 350, and 1200 Series APs are positioned strategically throughout the campus, providing links between the wireless network and the 100 percent Cisco wired network. As new buildings are constructed, additional APs will be added. A total of about 1,200 APs are expected to be eventually available on campus "to create a wireless infrastructure that will encompass all instructional space, residence halls, houses, the library, campus centers, the alumni association, arenas, and other places where students congregate. Upon completion, the wireless LAN (WLAN) system will cover 75 buildings and will serve 35,000 people" (The University of Akron, 2001).

All APs on campus are connected to the pre-existing wired infrastructure that, in turn, is connected to a 10 Gbps fiber-optic backbone. The power to these APs is provided through the category 5 cables that connect them to the campus network, thereby eliminating the need to run electrical cable to the APs. Each AP provides an appropriate sphere of connectivity that is needed to connect to campus network resources and the Internet.

The use of Cisco APs and NICs provided a level of security that was not available in equipment based on the original 802.11b standard. Cisco's proprietary suite of WLAN security mechanisms specified LEAP (Lightweight Extensible Authentication Protocol) authentication using a RADIUS server and per-session encryption keys. The equipment used on campus relies heavily on these mechanisms. Every university student and employee (faculty included) is assigned an e-mail ID (referred to as a UANET ID) that is used to sign-on to a variety of network resources. To connect to the campus WLAN, users have to use their UANET IDs and passwords to be authenticated against a RADIUS server. If a user cannot be authenticated, s/he will not have any network connectivity. Also, unique 128-bit session keys are dynamically generated as users are authenticated; re-authentication occurs on a periodic basis or when a session times out, thus providing an increased level of security. Equipment and mechanisms are in place to detect and shut down any rogue APs. In all, Cisco's suite of security mechanisms provides users with a high level of confidence that their information will not be compromised.

Benefits of Wireless

When the pilot program commenced in January 2001, the general-purpose computer lab in the main library was shut down. By summer semester 2001, just as the campus rollout was to begin, five more of these labs were shut down, leaving only two labs open. Eventually, one of the remaining two labs was closed, too. To offset the shortfall of hard-wired labs, 90 more laptops (in addition to the 60 that were available during the pilot) were added in the library, 30 in the new Student Union building, and 30 in the Science & Technology library. In addition, two *mobile* labs for classroom instruction were brought online, one with 75 laptops in the College of Business Administration and another with 20 laptops in the College of Education. The Department of Biology is also scheduled to bring a mobile lab online in the very near future (The University of Akron, 2003).

The benefits of being wireless are many (DiRenzo and O'Connor, 2003). To the university, the almost complete elimination of wiring costs, as mentioned earlier, probably comes out ahead of every other benefit. Also, the wireless initiative in the library and other locations obviated the need for having dedicated lab space to house what may have been hard-wired desktop computers. Hardware and software standardization that accompanied the laptop distribution made "providing technical support better, faster, and easier" (DiRenzo and O'Connor, 2003; p. 5). For the faculty, having all material available on the laptop obviates the need to copy files to a floppy disk to take to class lectures. A sizeable number of classrooms are now equipped with ceiling-mounted projection systems, making it very convenient to project slides using the laptop. Since a sizeable number of faculty desktop computers were beginning to be obsolete, the wireless laptop initiative provided them with state-of-the-art machines.

Implications And Conclusions

This paper has provided an overview of WLAN technology and discussed several issues related to it. Issues such as benefits of WLANs and making a business case deserve attention when WLAN implementations are considered. Yet, the issue that has received the greatest attention is security problems. The paper provided an explanation of the major security problems that firms will encounter as they deploy WLANs. The WLAN industry and standards organizations are beginning to address the major security concerns of the technology. WPA, and the soon to be ratified 802.11i (WPA2) standard, will adequately address the privacy needs of organizations.

At the University of Akron, it is clear that going the wireless route rather than wiring for network access was more appropriate. The expenses involved in wiring just the main library would have been prohibitive and would have involved setting up a room to house an additional lab. Expenses notwithstanding, every time someone needed access to the network, s/he would have had to go the lab. With wireless laptops available for check out at the library and other locations on campus, students can take the laptop to an area in the building where they are more comfortable working, and where they can sit together with their classmates to work on group projects and other assignments. In an educational environment, such interactions could possibly lead to higher productivity on the part of both students and faculty alike.

On a philosophical note, the use of WLANs allows every classroom and training space to be connected to information sources and to each other. WLANs enhance in-class instruction, and provide tools to facilitate new ways of learning and sharing. According to Dr. Gaylord, as the members of the faculty create content and students increasingly adopt *wireless mobility*, a synergy will be created between faculty and students. He believes that the students and faculty can assist each other directly if they have problems with the technology. It should also greatly reduce the amount of paper exchange that is involved in the teaching and learning processes.

The corporate world is also benefiting from the convenience, flexibility, and cost savings of WLANs. The ability to look-up information during a meeting, and not having to "get back" later with information, has the potential to save time and increase productivity. Though many of the apparent benefits of WLANs are intangible and cannot be directly equated to financial factors, the risks of overlooking such benefits may be high. One cannot always anticipate all the benefits of a wireless deployment nor can one completely understand the ways in which certain activities or tasks can benefit from the use of the technology. Wireless technology, for example, allows doctors to retrieve and view patient x-ray and other images at a patient's bedside in a hospital without having to summon those records. Or, wireless technology may allow one to provide valuable information to clients while meeting with them in a location where WLAN connectivity is available. It is exactly these benefits that may add value. Just because these benefits cannot be equated to traditional financial factors may not be a sufficient reason to overlook these benefits.

Finally, although we have not discussed how small businesses can benefit from wireless technology, it is clear that these firms stand to gain much from its use. With falling prices of wireless equipment used in a small office home office (SOHO) environment, the cost of setting up a small-office network is no longer prohibitive as was the case with wired networks. Also, manufacturers have begun providing features (for e.g., the ability to set up Virtual Private Network connections between offices) that were once included only in more expensive equipment. Thus, small businesses, too, can reap the benefits of wireless technology – higher productivity and the like – that at one time were exclusively available only to larger companies.

References

1. Blackwell, G. Serious WLAN Security Threats. *http://www.80211-planet.com/columns/article.php/949891*, January 7, 2002.
2. Botelho, G. The Next Information Age. *http://www.cnn.com/SPECIALS/2003/wireless/*, October 15, 2003.
3. Cam-Winget, N., Housley, R., Wagner, D., and Walker, J. Security Flaws in 802.11 Data Link Protocols. *Communications of the ACM*, 46(5), May 2003, p. 35-39.

4. Cosgrove, L. Wireless Update – Slow and Steady Progress: Executive Summary. *http://www2.cio.com/research/surveyreport.cfm?id=36*, September 30, 2002.
5. Cox, J. Wireless Woos Doctors. *http://www.nwfusion.com/research/2002/1209sector.html*, December 9, 2002.
6. DeGiglio, M. Finding Real ROI. *http://www2.cio.com/analyst/report278.html*, 2001.
7. DiRenzo, S. and O'Connor, P. Wireless Laptop-Lending Program at The University of Akron. *http://www3.uakron.edu/library/ulsys/presentations/oln/laptopOLNarticle.pdf*, 2003.
8. Dubie, D., Jacobs, A., and Ohlson, K. Wi-Fi @ Work. *http://www.nwfusion.com/wifi/2002/sideonline.html*, March 25, 2002.
9. Fluhrer, S., Mantin, I., and Shamir, A. Weaknesses in the Key Scheduling of RC4. *Proceedings of the 4th Annual Workshop on Selected Areas of Cryptography*, 2001.
10. Gaspar, S. Going Wireless at Framingham State College. *http://www.nwfusion.com/research/2002/1125fram.html*, November 25, 2002.
11. Geier, J. Wireless LAN Installation Steps. *http://www.80211-planet.com/tutorials/article.php/1718161*, February 27, 2003.
12. Green, K. C. Tracking the Digital Puck into 2004. *Syllabus*, December 2003, p. 10-13, 38.
13. Griffith, E. WPA: New Protection for 802.11. *http://www.wi-fiplanet.com/news/article.php/1491771*, October 31, 2002.
14. Harmon, A. Technology: Good (or Unwitting) Neighbors Make for Good Internet Access. *The New York Times*, March 4, 2002, Section C, p. 1.
15. Housley, R. and Arbaugh, W. Security Problems in 802.11-Based Networks. *Communications of the ACM*, 46(5), May 2003, p. 31-34.
16. In-Stat/MDR.3Q2003WLANMarketAnalysis. *http://www.instat.com/Catalog/NQcatalogue.asp?id=160#IN030901WL*, 2003.
17. Intel Corporation. Wireless LANs: Linking Productivity Gains to Return on Investment. *http://www.intel.com/eBusiness/pdf/it/pp024801.pdf*, December 2002.
18. Janss, S. Wireless LAN Security. *http://www.nwfusion.com/reviews/2001/1217rev.html*, December 17, 2001.
19. Karygiannis, T. and Owens, L. Wireless Network Security. *National Institute of Standards and Technology Special Publication 800-48, http://cs-www.ncsl.nist.gov/publications/nistpubs/800-48/NIST_SP_800-48.pdf*, November 2002.
20. Korostoff, K. The ROI of Wireless LANs. *http://www.nwfusion.com/techinsider/2003/0519techinsiderroi.html*, May 19, 2003.
21. Lingblom, M. 802.11g Sales Up In Second Quarter, Fuel WLAN Market Growth. *http://www.channelsupersearch.com/news/crn/43914.asp*, Aug. 13, 2003.
22. Network World. What's Wrong with WEP? *http://www.nwfusion.com/research/2002/0909wepprimer.html*, September 9, 2002.
23. O'Connor, P. and Richert, P. Wireless Laptop Pilot: Spring 2001 Semester Initiatives. *http://www3.uakron.edu/library/laptops/presentations/ua-42501.html*, 2001.
24. Proenza, L. M. Charting the Course: A Strategic Planning Report. *http://www3.uakron.edu/home/chart/letter.html*, 2000.
25. Sawhney, M. Damn the ROI, Full Speed Ahead. *http://www.cio.com/archive/071502/netgains.html*, July 15, 2002.
26. The University of Akron. Technology Without Boundaries: The University of Akron Laptop Initiative. *http://www3.uakron.edu/laptop/*, 2000.
27. The University of Akron. The University of Akron Chooses Cisco Aironet 350 Series For Full Wireless Coverage. *http://www.uakron.edu/its/network/wireless.php*, 2001.
28. The University of Akron. In Touch with Wireless Computing at The University of Akron. *http://www.uakron.edu/its/docs/wireless_computing.pdf*, 2003.
29. Varshney, U. Wireless I: Mobile and Wireless Information Systems: Applications, Networks, and Research Problems. *Communications of the Association for Information Systems*, Vol. 12, 2003, p. 155-166.

30. Wi-Fi Alliance. Wireless LAN Research Study. *http://www.wi-fi.org/opensection/pdf/wireless_lan_research_a.ppt*, October 2001.
31. Wi-Fi Alliance. Wi-Fi Protected Access. Strong, Standards-Based, Interoperable Security for Today's Wi-Fi Networks. *http://www.weca.net/OpenSection/pdf/Whitepaper_Wi-Fi_Security4-29-03.pdf*, April 29, 2003A.
32. Wi-Fi Alliance. WLAN Benefits Calculator. *http://www.wi-fi.org/OpenSection/WLAN_Calculator.asp*, 2003B.
33. Worthen, B. When Wireless Works. *http://www.cio.com/archive/120102/wireless.html*, December 1, 2002.

Notes

Notes