# The Expanded Risk Horizon of Accounting Networks Utilizing Wireless Technology

*Volume 4, Number 1*
*2009*
*page 17 - 25*

**David R. Fordham**
James Madison University, fordhadr@jmu.edu, 540-568-3024



## ABSTRACT

One of the major professional responsibilities of accountants and auditors is to identify and evaluate the risks in accounting information systems. More and more accounting systems are utilizing wireless data links, including 802.11 "wi-fi" segments. Because of marketing claims and personal experiences, it is widely believed by both professionals and the public that today's 802.11 wireless equipment has an operational range of well under 500 feet. This paper reports on an experiment which established reliable, high-speed connections across a distance of 56 *miles* using commercial off-the-shelf equipment. The results provide empirical evidence that the risk of undetected eavesdropping on modern Wi-Fi network transmissions extends to at least *a thousand times* as far as the commonly-recognized range of these networks. This experiment vividly demonstrates the possibility that accounting data is at risk well outside the normal sphere of expected vulnerability recognized by auditors and systems evaluators. Without a full understanding of characteristics of wireless data transfer, accountants and auditors could easily fail in their evaluation and assessment of the safety, integrity, and security of the accounting system

***Keywords***
802.11, Accounting Systems Security, Accounting Network Security, Information Security, Wireless Network Range

## INTRODUCTION

According to one popular AIS text, a good accounting system must provide information that is reliable, complete, timely, and accessible (Romney and Steinbart, 2006, p. 6). One of the major professional responsibilities of accountants and auditors is to identify, evaluate, and assess the risks posed within the accounting information system – risks which could interfere with reliability, completeness, timeliness, or accessibility.

Auditing Standard Number 94 (AICPA 2000), for example, specifies the responsibilities of auditors in

"understanding and comprehending the operation of technology" so as to be qualified to identify and evaluate accounting systems. Deficiencies in such knowledge can lead to the oversight of potential threats and vulnerabilities to the integrity, accuracy, and completeness of the accounting data being captured, stored, and reported.

Increasingly, many of today's accounting information systems are incorporating wireless data links. These links carry accounting data as well as other sensitive business information. "Wireless technology" is becoming ubiquitous in business information systems. Many people overlook the fact that "*wireless*" is simply another word for "*radio*". Radio is a broadcast medium. By using wireless devices, a network user is "broadcasting" data to anyone within range of the transmitted signal. Unlike wired segments of a network, an interceptor does not need to have physical access to the network infrastructure or equipment to capture the signal or data moving thereon.

Unfortunately, this fact is generally lost on most accountants, auditors, students, and even accounting systems educators. A recent perusal of eight widely-adopted AIS texts revealed that *none* of them associated the term "wireless" with broadcasting or radio, nor made any mention of the range of wireless radiowaves. Six made no mention of *any* threats or vulnerabilities related specifically to wireless technology.

The most common wireless links in business applications today are the 802.11 family of "Wi-Fi" or "Wireless Ethernet" devices. Available in "a", "b", "g", and the new "n" flavors, the 802.11 standard has become the flagship of wireless interconnectivity for personal as well as commercial LAN applications (Biggs, 2006). In marketing releases, advertisements, technical specifications printed on boxes, in product review literature, and in the popular press, it is widely disseminated that 802.11-based networks are designed, engineered, and optimized for distances between stations of up to a maximum of 100 meters, or about 300 feet (IEEE, 1999; Mathias and Phifer, 2005; Mathias, 2005; Bannon, 2007).

Because of the plethora of media reports, specifications, and literature reporting the present usable distances of 802.11 networks to be around 100 meters, it is logical for auditors and accountants -- as well as the general public -- to misinterpret this as meaning 100 meters is the maximum extent at which such an 802.11 signal can be reliably received. Physicists, on the other hand, know that once any radio signal is transmitted from its antenna, the electromagnetic wave continues to expand, traveling out to the edge of the universe unless stopped by some absorptive material such as a metal shield or earth (Taylor et al, 2003). A sufficiently sensitive receiver might be able to receive the signal reliably at a distance considerably farther than the standard equipment used in typical installations. But this fact is noticeably absent from the literature informing the public of the range of wireless network devices, and even less available in the educational materials aimed at students studying accounting systems and auditing.

There are many factors which determine the useful receivable range of a transmitted signal. The sensitivity of the receiver is one. Directivity of both the transmitting and receiving antennas is another. Other factors include the output power of the transmitter, background noise and interference, type of modulation used, and even the speed of the data transmission. Thus, it is inaccurate to equate the "range" of a wireless signal to the distances over which a particular network component is used in standard installations.

This fact notwithstanding, most business decisionmakers and accountants in particular, including accounting students and AIS educators, may still be under the impression that the "range" of 802.11 networks is not significantly more than several hundred feet (Mathias and Phifer, 2005, 20). Because of this impression, professional accountants and auditors may overlook threats and vulnerabilities existing outside that radius (Campbell et al, 2003).

This paper summarizes the results of a field experiment which established reliable, high-speed wireless connections across a distance of *56 miles* using commercial off-the-shelf 802.11 equipment, without amplification or increased transmitter power. The experiment vividly demonstrates that the risk of undetected eavesdropping on Wi-Fi network transmissions extends to at least *a thousand times* as far as the commonly-recognized "range" of these networks. When these links form an integral part of an accounting system, the accounting data is subject to risks outside the sphere of expected vulnerability anticipated by most auditors and systems evaluators.

This paper is organized into several sections. Section 1 addresses legal framework under which wireless networks operate, and explains how the law actually facilitates legal "eavesdropping". In Section II the results of the experiments are described. Section III explains the difference between network "connections" used in the range experiments and "eavesdropping", highlighting the fact that accounting data is vulnerable at distances *even greater* than the 56 miles demonstrated by this experiment. Finally, the paper concludes with a section on the ramifications of this experiment for accountants, auditors, and AIS educators, repeating the need for students to be informed of the true nature of wireless signals which carry accounting data.

## SECTION I: BACKGROUND ON FCC PART 15 DEVICES

Modern wireless networking equipment operates under what is known as the "Part 15 Radio Service". All 802.11, Bluetooth, RFID, and all other commercially-available wireless data transmission technologies operate under this service. Hence, it is important for accountants and other users of wireless data technology to understand the nature of devices manufactured and operating under these rules.

By international treaty, devices which emit radio waves must be regulated by national governments. Such regulation must address the devices' design, manufacture, and operation to prevent interference to other users. The Communications Act of 1934 is the U.S. implementation of the treaty's mandate. The Act established the Federal Communications Commission and gave the Commission sole authority and responsibility for rules and regulations governing radio frequency emissions within the United States and its territories. The FCC rules govern all devices made, sold, or used which emit radiofrequency (RF) electromagnetic energy (radio waves), regardless of whether such radiation is intentional (as in the case of radio transmitters), or unintentional (as in the case of integrated circuits, computer monitors, fluorescent lights, and any other device which might accidentally emit energy detectable by a radio receiver). The FCC rules are found in the Code of Federal Regulations (CFR) Title 47.

Title 47 is divided into many parts. For example, one part lists the rules, regulations, requirements, and technical parameters governing television broadcast stations. Another addresses public service radio systems, such as fire and police departments. Yet another addresses aviation navigation and communication, and another addresses marine radars. Another addresses unintentional radiators, such as computers, (explaining why computer equipment is labeled with a tag proclaiming "FCC Type Acceptance").

One common thread running through most of these services is the requirement that intentional radio transmitters be *licensed*. Each transmitter is licensed to use a particular frequency (or channel) or a specified set of frequencies, allowing the device to communicate with other devices as intended while at the same time avoiding interference to all other services and users. By issuing licenses individually for every transmitter, the FCC can keep track of who is communicating where, both geographically as well as within the radio spectrum. It is this careful allocation of channels by the licensing process that allows individual radio users to operate without interfering with each other. The local police department radio, for example, can operate free from

interference from the railroad switching crew or transmissions from an aircraft passing overhead.

Licenses are obtained by application to the FCC. A radio wave, once generated, expands out into free space to the edge of the universe. However, it can be blocked by certain shields. One of the most effective shields is the earth itself. Radio waves cannot penetrate very far into the ground. Thus, radio waves are blocked by mountains, high hills, and the curvature of the earth.[1] Because of the shielding provided by the earth, a single radio channel may be re-used in multiple locations: the FCC may assign the same channel to two different users if they are far enough apart that the curvature of the earth (or mountains, or other obstructions) will prevent them from interfering with each other. Hence, a license is granted only for a specific geographic location, such as a street address or latitude/longitude coordinates, and the licensee is forbidden to move the transmitter to a different location without checking with the FCC (or its designate, such as a frequency coordinator) first.

Mobile stations, such as police cars, are licensed to operate within a certain range of their licensed base station. Other mobile stations, such as boats or railroad trains, are licensed to operate on certain channels while on certain waterways, rail lines or within certain geographic boundaries. In a similar manner, cellular phone service providers obtain licenses for their base stations, and then by extension, their subscribers (and subscribers to reciprocal service agreements or roamers) can 'share' the frequency by using handsets licensed to the cellular service.

Obtaining a license is a cumbersome and time-consuming process. Before giving exclusive right to a channel in a particular area, the FCC must ensure that no other user is already using the channel within possible range of the applicant. Because of the efforts involved, obtaining a license can take days, weeks, or even months. It is obvious that such cumbersome licensing procedures would seriously inhibit the deployment of much of the modern equipment we use in day-to-day living. The magnetron tubes in microwave ovens, for example, are radio transmitters, and requiring every microwave oven to obtain an FCC license would practically preclude the use of ovens by the general population. Garage door openers, baby monitors, cordless phone sets, and yes, Bluetooth and 802.11 devices, are all radio transmitters. Requiring each and every one of these devices to be individually licensed would effectively prohibit the general population from deploying this equipment, and place an impractical burden on the FCC.

To allow the convenient widespread deployment of such devices, the FCC has established certain "channels" (frequency bands within the electromagnetic spectrum) to be used *without* a formal license. Part 15 of the CFR Title 47 is the part which establishes the rules, regulations, limitations, restrictions, and parameters of transmitters for which the FCC does not require individual licensing.[2]

As a general rule, in order to be exempt from the individual licensing requirement, a device must emit a very low level of RF energy. Microwave ovens, for example, may generate over a thousand watts of RF energy, but the energy must be confined (by metal shielding) to the interior of the oven. The allowable leakage from a microwave oven (the equivalent of microwatts) to free space outside the oven is millionths of the energy generated by its transmitter. Baby monitors, garage door openers, Bluetooth devices, and all other unlicensed

[1] Some frequencies, generally referred to as the "short-waves", are subject to bending, refraction, and reflection by the ionosphere encircling the earth; these waves bounce around the world in spite of the earth's curvature, allowing direct global communications if conditions are right. But most higher-frequency waves such as VHF, UHF, microwaves, etc. used for modern communications are blocked by geographic features, and are called "line-of-sight" links.

[2] In order to comply with international treaty, these unlicensed devices must be designed so that their transmitted signal cannot possibly interfere with radio services outside the U.S. in any conceivable circumstances. This is another reason for the low power requirement.

radio transmitters are limited by law to very low power levels. Normally the allowable power levels are deliberately set just high enough to enable useful communications within mere feet, perhaps a hundred or so feet, or at most a couple of miles. This is because these devices are designed to be used only within small areas. The effective radius of use is due more to the design and limitations of radio *receivers* meant to accompany the transmitters, rather than the actual range of the radiowaves. By pairing the transmitter power with the receiver design to keep the operational radius small, the FCC reasons that a large number of users can re-use the channels without interference. Remember, the entire idea behind the Part 15 service is to allow a large number of users to deploy wireless devices without licensing or exclusive use by any one user.

All 802.11 wireless networks operate under Part 15 of the FCC rules. Hence, no user has exclusive use of the frequency. **This is critically important to 802.11 network users: anyone, anywhere, anytime, can legally intercept and "listen to" the transmissions of an 802.11 device.** What's more, any 802.11 user has just as much right as any other user to transmit, and *receive*, on the frequency. There is no prohibition against anyone receiving any signal on the channel.

This "sharing" of the medium provides convenience for users, but the non-exclusivity means that *any user* can legally pick up and receive any other user's signals. While this facilitates useful operations like "hot spots" and open-access wireless access points, it also means that anyone within "range" can receive the transmissions, perfectly legally. And since the law specifically provides for a "shared" resource, it is even difficult to claim that such eavesdropping is unethical. (It may be considered rude to listen to someone's conversation in an elevator, for example, but it is certainly not considered "unethical".)

802.11 network devices use channels shared not only with all other 802.11 users, but also by a multitude of other non-licensed devices, including baby monitors, garage door openers, cordless phones, microwave ovens, Bluetooth devices, and countless other equipment. This situation is explained clearly in the front of every user manual of every piece of 802.11 gear sold in the U.S. (and the rest of the world), but is often overlooked, quickly forgotten, or dismissed by the general public, accountants and auditors. This oversight of the shared nature of the 802.11 frequencies is the basis for most of the risks associated with their use.

## SECTION II: RANGE EXTENSION EXPERIMENTS

The research team consisted of a networking technician with a local cable TV company, a former IBM systems engineer, the I.T. technical support director for the local public school system, and the author – an accounting information systems professor at a local university.

The experiments involved two stations. Each station consisted of a portable laptop computer connected to a Linksys WRT54 router operating in 802.11g mode. To test for proper operation and configuration of the equipment and to establish a baseline, the two stations were connected via 802.11 link while the stations were in close proximity (within 30 feet of each other) using the omnidirectional antennas provided with each router. This environment is considered normal for business or personal use. File transfers were conducted and effective file transfer rates determined.

After confirming proper setup, configuration, and operation of the two stations, the equipment was taken into the field. The initial experiment involved replacing the stock omni-directional antennas on one and then both wireless routers with directional parabolic dish antennas. Most 802.11 gear is sold with an omnidirectional antenna. The use of an omnidirectional antenna allows radiation and reception of the signal equally in all directions. Users do not have to consider the orientation (or "aiming") of the antenna, making such antennas convenient and simple to use. But when the equipment is used in a fixed, point-to-point

arrangement, the use of omnidirectional antennas "wastes" the signal. By concentrating the transmission and/or reception of the signal to a single desired direction, an outboard directional antenna enhances the utilization of the electrical radiowave.

Numerous designs of directional antennas are widely available commercially at low cost. Not only does use of a directional antenna concentrate a transmitted signal, but using such an antenna at the receiving station shields the receiver from noise coming from behind the dish. The signal-to-noise ratio of the desired signal is increased. Theoretically, this should increase the distance at which signals can be reliably received, hence increasing the range.

One station (router, antenna, laptop) was taken to an open area on the university campus, while another was taken to a hotel parking lot within line of sight of the first station. The two locations were approximately ½ mile apart which is considerably more than the advertised range of the equipment. The two directional antennas were aimed at each other by sight, since the operators of each station could clearly see the other. Using this setup, reliable high-speed connections were repeatedly established and confirmed by actual file transfers.

To compare the directional antennas to the omnidirectional antennas, the directional antennas were replaced by the omnidirectional antennas which had been originally provided on the devices by their manufacturer. Connectivity could still be reliably established using two omnidirectional antennas, even at 1 Mbps, under the clear path.

Next, the team widened the distance by moving the two stations further apart. At a distance of one mile, connectivity could not be established at all when using the omnidirectional antennas on both ends of the link, but could be easily established by using a directional antenna on one end and the omni-directional antenna on the other. Better connectivity and high throughput was experienced with the directional parabolic antennas on both ends of the link.

The stations were moved to new locations farther and farther apart. After several intermediate distances were achieved, one team was dispatched to the mountain range on one side of a valley, with the other on a mountaintop 34 miles away. Using GPS receivers, compasses, topographic maps and binoculars, the teams carefully aimed the antennas, and were able to establish solid connection, with moderate throughput rates, at a distance of 34 statute miles, even using an omnidirectional antenna at the receiving end of the link with an omnidirectional antenna at the transmitting end.

A month later, another connection was made, this time spanning a distance of *56 miles*, by using directional antennas on both ends of the link. Files were transferred, data exchanged, and although transmission speeds were relatively slow, the network equipment diagnostics concluded the two-way link was solid and perfectly usable.

## SECTION III: ACCOUNTING RISK -- EAVESDROPPING VS. CONNECTION

The 56-mile distance was achieved involved a two-way network connection, utilizing directional dish antennas on both ends of the link. Two-way network operation requires that all transmitted data packets be acknowledged. But what about 'eavesdropping', where a receiving station is merely *listening* to the transmitted data? Copying (e.g., receiving and reading) a one-way transmission is considerably less complex, requires no exchange of overhead signal control transmissions, does not require packet-by-packet acknowledgement, and hence can take place at greater distances.

To judge the possibility of eavesdropping, the team replaced one of the parabolic dish antennas with the stock omnidirectional antenna that came with the equipment. This setup approximated the situation where a

user (such as an accounting system) would be on one end if a link, and an eavesdropper or interceptor would be at the other. The user would probably be using the stock antenna provided with the network equipment, whereas the intentional interceptor would likely be using a gain antenna such as the parabolic dish (perhaps even with a receiver pre-amp amplifier.) To the team's surprise, the signal from the omni antenna was still perfectly readable with the directional receive antenna, although the signal strength was low.

Whether credit card numbers, sales information, payment data, or other information, accounting data must be kept secure and confidential from unauthorized reception. If an intercepting receiving station were interested in merely copying the data being transmitted, the perpetrator could, merely by attaching a directional receive antenna, pick up and capture data transmissions being made from miles away.

While engaged in the experiments on the mountain, the research team was able to reliably copy one-way packets being transmitted from dozens of wireless networks that were located along the line-of-sight between the two research stations. On the day that the 34 mile distance was achieved, seventeen identifiable networks were detected and received in the narrow path of the antenna beamwidth. Eleven of those 17 networks were completely open, broadcasting their SSID in the clear, and transmitting unencrypted data. One of the open networks was recognized as being at the local hospital, one at a local nursing home, another at a restaurant's regional office, one at a car dealership, one at a dentist, and at least two that were apparently maintained and operated by managers of local apartment complexes. These were not open "hot spots" intended for public use, but were private 802.11 networks installed by unknowing, identifiable, commercial users who had not secured their private networks. Any of these networks could have been carrying accounting data.

The networks were likely using the omni-directional antennas that came with the network gear. It is doubtful that any of the operators or users of these networks suspected that their traffic was being intercepted, received, and possibly monitored by someone located on a mountaintop 30 or more miles away.

And this count (17 networks) only included those broadcasting a recognizable SSID. Had the research team desired, a more sophisticated "sniffing" program could have been used to detect the presence of additional networks along the line of sight. Undoubtedly, there existed one or more well-informed users along the line of sight who might have partially obscured their networks but who were still transmitting data – data which could have also been intercepted and received by the research team.

The 56-mile distance link was deliberately engineered to avoid crossing populated area, and hence covered only wilderness within a National Forest. However, even so, while setting up the equipment, the team was able to copy dozens of networks from different directions, many from a town located at least 50 miles away. Undoubtedly, many if not most or all of those networks were using only the stock omnidirectional antenna that came with their equipment.

Can eavesdropping be prevented by the use of encryption? Once again, accountants and auditors who are not fully informed of the nature of wireless networks might assume that if a network is using encryption technology, that network is secure. What many may not realize is that 802.11 equipment manufactured prior to 2003 used security measures which can not be considered truly secure. The WEP encryption method used prior to 2003 was able to be "cracked" using commonly available tools, such as AirSnort (Biggs, 2006). While later equipment has corrected the problem and WEP in modern equipment is considered very secure, the mere use of encryption does not guarantee safety or security. Specifically, if any device on a network was manufactured before 2003, then the *entire network* must utilize the older encryption standard and must therefore be considered unsecure, even if all other equipment is new, since the network cannot use the newer more secure encryption and still communicate with the older equipment.

More importantly, many of those network operators who *can* deploy the advanced encryption techniques do not do so, either because of the trouble necessary to properly set up security on all the equipment, lack of compatibility of equipment, or perhaps lack of understanding or appreciation of the risks. In particular, it would seem logical that a network operator who did not visually observe any eavesdropping threats within a 300-foot radius might not realize that a threat could exist dozens of miles away.

This brings up the essential point made earlier in the discussion of the Part 15 radio service: eavesdropping on 802.11 transmissions is perfectly legal, and probably does not fall outside ethical boundaries either, since the resource (radio frequency) is by law deliberately designed to be shared. The shared nature of the Part 15 frequency band is *intended* for anyone to receive transmissions on the band, at any time, without restriction.

(A clear distinction must be made between merely *listening* to a wireless network, and actually *connecting* to a wireless network. Actually connecting to a wireless network requires two-way transmissions, and can be considered "intrusion" or even "trespass" into another's computer system under the law. By contrast, merely listening (eavesdropping) to transmissions existing on the frequency is unquestionably perfectly legal, just like listening to a conversation in an elevator. While some legislative bodies are making attempts to outlaw the actual *connection* of unauthorized users to wireless networks, the very nature of the Part 15 band in the rules and regulations, by definition, precludes any restriction on eavesdropping on these transmissions.)

## SECTION IV: RAMIFICATIONS FOR ACCOUNTANTS AND AIS PROFESSIONALS

As mentioned in the introduction to this paper, accountants and auditors must adequately assess the risks faced by accounting data on its way from capture to storage, and from storage to reporting. More and more of these "data-transportation" pathways involve wireless links.

Accountants and auditors frequently rely on technical support specialists to provide information about the safety and security of the network. But this is clearly a mistake that could have grave consequences. According to Easttom (2006), these technical specialists are often under-qualified in terms of internal control expertise, and therefore may be overconfident of the integrity of the systems when it comes to internal control sufficiency. To reinforce this view, Wright and Wright (2002) gathered evidence that ***less than five percent*** of education programs in information technology contained ***any coursework*** covering internal control concepts, such as the classical ideas of checks and balances, redundancy of verifications, or professional skepticism. Even in those few instances where internal controls were included, they were often covered within a context unrelated to the operation of the technological systems. They agreed with Eastom and concluded it to be clear that technical support specialists, especially networking technologists, can often overestimate the security of their systems. In any event, it is left to the accountants and auditors to verify the veracity of security claims. The lack of coverage of technological threats in the AIS curriculum would seem troubling.

Financial reporting is the major end-use of accounting data. The Sarbanes-Oxley act adds legal clout to the importance of tight internal control over the accounting system so as to produce reliable financial reporting. Accountants and auditors must be fully aware of *all* risks faced by the data as it travels along the system. If business professionals, especially AIS professionals, believe that threats outside of a radius of 100 meters, or even 1000 meters, need not be seriously considered, they could well be overlooking very real threats. Visual inspection of the physical vicinity of an AIS system, for example, can no longer rule out threats to the integrity, confidentiality, and reliability of the data on that system.

Education in accounting information systems is incomplete without some topical coverage of the risks

inherent in using wireless technology. It is this author's position that accounting information systems education must include coverage of the operation of today's modern networks, both wired and wireless, at a level significantly above that found in most of today's accounting curricula and especially AIS textbooks. Otherwise, tomorrow's accountants and auditors may be ignoring a significant source of potential threats and vulnerabilities to accounting data integrity, authenticity, accuracy, reliability, and availability. We cannot afford to delegate this responsibility to the technical support personnel who are not properly imbued with the "auditor mentality" of professional skepticism and obligation to the public to take pro-active measures against such risks.

The experiment described in this paper shows that wireless 802.11 networks can be received, legally and with commercially-available equipment, at distances at least a thousand times further than the normally-accepted range of network operation. By overlooking or ignoring potential threats existing at such great distances, auditors and accountants can fail in their duty to adequately identify, evaluate, and address risks to accounting data. Such failure can be considered an abdication of responsibility to the public. As educators, it is our responsibility to ensure that today's and tomorrow's accountants and auditors are fully aware of the threats and vulnerabilities existing in locations and areas and at distances not commonly considered.

## REFERENCES


AICPA, 2001. Statement of auditing standards number 94: The effect of information technology on the auditor and consideration of internal control in a financial statement audit. Professional Standards, Vol 1, AV Sec. 319, New York: AICPA.

Bannon, A. L. 2007. Trash your cables. PC Magazine (June 26): 88-92.

Biggs, M. 2005. How to secure the wireless fortress. *Federal Computer Week* (June 26): 24-29.

Campbell, P. B. Calvert, and S. Boswell. 2003. *Security+ Guide to Network Security Fundamentals*. Boston: Cisco Learning Institute/Thomson Course Technology.

Easttom, C. 2006. *Computer Security Fundamentals*. Upper Saddle River (NJ): Pearson/Prentice Hall.

Federal Communications Commission. 2005. *Code of Federal Regulations (CFR) Title 47, Telecommunications, Part 15 as amended.* Washington: Office of the Federal Register.

IEEE. 1999. *IEEE Standards for Information Technology – Telecommunications and Information Exchange between Systems – Local and Metropolitan Area Networks – Specific Requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*. Available on-line for download at: http://standards.ieee.org/getieee802/802.11.html and last accessed June 10, 2007.

Mathias, C., and L. Phifer. 2005. The evolving wireless landscape. *Business Communications Review*. (April): 18-23.

Mathias, C. 2005. MIMO Products boost 802.11g nets. *Network World*. (March 21): 67.

Romney, M., and P. Steinbart, 2006. *Accounting Information Systems 10th edition.* Upper Saddle River: Pearson Prentice-Hall.

Taylor, J., C. Zafiratos, and M. Dubson. 2003. *Modern Physics for Scientists and Engineers, 2nd edition*. Upper Saddle River: Benjamin Cummings-Prentice-Hall.

Wright, S., and A. M Wright. 2002. Information system assurance for enterprise resource planning systems: Unique risk considerations. *Journal of Information Systems* (Supplement): 99-130.