

The Canadian Institute of Chartered Accountants

Information Technology Advisory Committee

SECURITY
FOR WIRELESS SYSTEMS
(revised)



Insights for a changing world



Notice to Reader

The objective of white papers issued by the CICA's Information Technology Advisory Committee is to increase the awareness of CAs and other interested parties on IT topics considered significant to the accounting profession and business community. They are not intended to provide detailed guidance.

This white paper was prepared and updated by Gerald D. Trites FCA, CA•CISA, a member of ITAC and Professor of Accounting and Information Systems, St Francis Xavier University. The views expressed in this paper are those of Professor Trites and have not been formally endorsed by the CICA or ITAC.

Comments on the paper are welcome and should be addressed to researchstudies@cica.ca

This White paper is available in PDF format at the CICA web site (www.cica.ca/itac).

Copyright ©2004
The Canadian Institute of Chartered Accountants
277 Wellington Street West
Toronto, Canada
M5V 3H2

Disponible en français
(www.icca.ca/ccti)

SECURITY FOR WIRELESS SYSTEMS

CONTENTS

INTRODUCTION	2
RISKS OF WIRELESS NETWORKS AND COMMUNICATIONS	3
WIRELESS FIDELITY (WiFi) AND SECURITY TECHNOLOGIES	5
BLUETOOTH WIRELESS TECHNOLOGY	6
DIFFERENCES BETWEEN BLUETOOTH & WiFi	7
WIRELESS ACCESS PROTOCOL (WAP)	8
SECURITY STRATEGY	8
SECURING WIRELESS WEB TRANSACTIONS	10
ASSURANCE	10
CONCLUSION	12
Additional Readings	13

INTRODUCTION

Wireless networks and other communications systems capable of transmitting data on a wireless basis are rapidly becoming a mainstream means of conducting certain types of e-business transactions.¹ These networks are utilized for internal use in many companies, for public use in some areas like airport terminals and railway stations and for the use of customers in certain private establishments, such as coffee shops and hotels.

The most significant of the new wireless devices are personal computers, cell phones and Personal Digital Assistants (PDAs). All of these can be linked to wireless networks, provided they are wireless enabled. While both cell phones and PDAs are available in models that can transmit and receive digital data, their e-business potential has not yet been realized because, so far, the technology has not had enough capacity to accommodate large amounts of data, or screens with multimedia. There are, however, limited e-business applications being used involving these devices.

There are well established wireless technologies, such as satellite and microwave, that have been used for several years, but this paper focuses on new and emerging wireless technologies.

For cell phones, there have been limitations in the speed and capacity of the phones, as well as the capability of the Internet Browsers they use, which employ a system called Wireless Access Protocol (WAP). Industry trends currently indicate that cell phones are moving to 3rd generation systems over the next two or three years, which will include broadband capability. Broadband would facilitate a greater use of cell phones for e-business purposes, such as ordering goods and services and paying for them.

With regard to PDAs, the technology is also improving, through the use of “Bluetooth,” which is a short range wireless technology described in more detail below. Bluetooth can also be used with cell phones and personal computers.

¹ Networks that follow the IEEE 802.11 standard include the equivalents of traditional wired ethernet networks, particularly those that follow 802.11a, 802.11b and 802.11g. The most commonly followed protocol — 802.11b — is sometimes referred to as WiFi.

Wireless systems, particularly wireless networks, are being implemented quickly - some say too quickly in view of the risks involved. This rapid deployment is due, at least in part, to the low cost, the ease of deployment, and the productivity gains that flow from their use. One of the more significant benefits of wireless is the fact that it frees up offices in terms of where people work. With wired networks, people are tied to a workstation. With wireless networks (WLANs), they can be relocated anywhere with ease. Also, wireless networking facilitates the ability of personnel who must be on the move to remain in contact with the office networks. This applies to a wide range of personnel, including, for example, medical people and warehouse staff. It is clear that there are benefits to wireless systems, but it is also clear that they pose risks that need to be addressed.

The primary means to control the risks presented by wireless systems is to implement effective security policies and procedures. Security includes three fundamental elements: availability, integrity and confidentiality.

RISKS OF WIRELESS NETWORKS AND COMMUNICATIONS

Security has been a persistent issue with regard to wireless systems, because they are subject to threats in addition to those involving wired networks. Generally, these additional threats exploit the fact that wireless communications are carried through the air using radio waves, on which unauthorized persons can “eavesdrop.” For example, wireless networks can be subjected to “parking lot” or “drive-by” hacking attacks. These drive-by or walk-by attacks are commonly called war-driving, similar to war-dialing where a hacker automates the dialing of phone numbers to detect unprotected modems. These simply involve a hacker entering an area within the radio range of the wireless network and intercepting data transmissions.

If the transmissions are not encrypted, they can read and record those transmissions. Even if they are encrypted, there are tools available that can analyze them and guess the encryption key. The most common encryption techniques used in wireless systems have been broken many times using such tools and therefore are not necessarily effective in preventing all attacks. Nevertheless, the encryption can provide some protection from unsophisticated attacks - certainly more than if it isn't used at all - and therefore should be deployed.

Wireless networks are also subject to “session hijacking” under which a hacker intercepts a login confirmation being transmitted from a wireless network to a user during the login process. When such a hijacking is successful, the network “thinks” the legitimate user is logged into the session, while in fact it is the hacker, and the legitimate user thinks the login failed for some unexplained reason and logs in again in a different session.

Another exposure open to wireless networks is theft of bandwidth. This occurs when "parking lot" hackers log on to someone's wireless router and surf the net. In recent cases, such hackers have used these illegal connections to download porno using the victim's internet account.

The range of a wireless network is normally confined to five hundred metres, but a computer or other device with a directional antenna can pick up the signals from a wireless network from as far away as twenty kilometres — well outside the parking lot!

Laptop and desktop computers equipped with wireless LAN cards generally can often create *ad hoc* networks if they are within range of one another. The security impact of *ad hoc* wireless LANs is significant because unauthorized users could become part of the network, unknown to the network administrators. Many wireless cards, including some models built-in by computer manufacturers, ship with the *ad hoc* mode enabled by default. Any hacker who is also configured for *ad hoc* mode can be immediately connected to computers using these cards on an unauthorized basis. While it is true that they may have to make their way through a log-on screen, if such a screen has been set up, the point is this will have been presented to them, rather than having to find it, which makes the hacker's job easier.

The main wireless technologies — WiFi, Bluetooth and mobile internet technology using WAP — include security tools intended to address these threats, but are shipped with these security tools turned off. All of these built-in tools, however, have been evaluated as lacking in some respect. Nevertheless, all do provide some degree of protection, and need to be turned on. If additional protection is deemed necessary in particular circumstances, as will often be the case, then additional security measures, such as special security software, will need to be adopted.

WIRELESS FIDELITY (WiFi) AND SECURITY TECHNOLOGIES

Standard Wireless Fidelity (WiFi) LANs using the 802.11(b) and 802.11(g) technology include a security feature called Wired Equivalency Privacy (WEP), which essentially involves a method of data encryption. The stated objective of WEP was to provide a level of privacy equivalent to that of a wired LAN. Several studies have found, however, that the most common threat to wireless LANs is the failure of organizations even to turn on the WEP security. WiFi systems are shipped with WEP turned off. Many people and organizations do not turn it on when they install the network, and therefore do not have security, even though they might think they do.

Numerous instances have been recorded of poor wireless network security being detected by drive-by hackers and computer professionals. One typical report in BBC Online revealed lax security on wireless networks in London's financial centre. Using a wireless laptop loaded with some generic software, the team drove around the City. Within one kilometre, they logged the existence of 12 networks, only four of which had enabled the WEP encryption system built into the software. Similar instances have received prominent media attention in and around Toronto, where home wireless networks have been the focus of attention by drive-by hackers.

While enabling WEP is highly advisable, it often does not provide enough security because of its established and well known weaknesses. The cracker tools that are available on the internet are capable of guessing the encryption keys, even for high encryption (128 bit) systems. They work by scanning encrypted transmissions in sufficient volume to enable patterns and relationships to be identified that can lead to the encryption key being guessed.

This means that, normally, precautions are required in addition to enabling WEP, including changing the encryption key on a regular basis, password protecting drives and folders, changing the default SSID (Wireless Network Name), and using a Virtual Private Network (VPN) system. Situations of higher risk call for additional security methods, such as end-to-end encryption, comprehensive user authentication and password control, Secure Socket Layer (SSL), firewalls and intrusion detection systems etc.

A newer form of WiFi security is called Wi-Fi Protected Access (WPA). This system, standard with the about-to-be-introduced protocols 802.11g and 802.11i, is intended to overcome the security limitations of WEP. WPA enabled software is not widely available as yet, but vendors are beginning to produce WPA enabled software and it is expected to become available very quickly because of the growing interest in wireless networks and the demand for security.

WPA has also been subject to criticism, however, for perceived shortcomings. It makes use of a shared passkey to trigger the encryption, and this passkey is shorter than the encryption key and therefore easier to guess. Also, it reverts back to WEP if any of the workstations cannot support WPA. WPA, however, does offer improvements in security capability. It is likely that both WEP and WPA will need to be combined with additional security measures for the foreseeable future in order to reach a satisfactory security level for wireless networks.

BLUETOOTH WIRELESS TECHNOLOGY

The Bluetooth wireless technology provides short range (normally ten metres) wireless connectivity between devices. Various wireless devices can be “Bluetooth enabled,” including cell phones, PDAs, laptops, printers and other peripheral devices. Therefore, Bluetooth can be used to facilitate interactive communications between devices, or to simply print a document without needing to wire the printer to the computer.

A significant characteristic of Bluetooth is that it can create spontaneous, *ad hoc* networks between Bluetooth enabled devices that are within range of each other. There are security features contained within Bluetooth that can be used to address the risk involved. The degree to which this security is implemented can be varied depending on the sensitivity of the information involved, the needs of the user and the risk exposure. As with any technology, some Bluetooth applications require little or no security, while others require a good deal.

The Bluetooth security system contains a set of profiles that enable the user to define a selection of messages and procedures (referred to as capabilities). These capabilities can then be assigned to particular users or user groups, based on what they need to do their job. This approach, in general, is common to computer security of all kinds. This results in a description of the actions

that users are allowed to carry out on the system. The current Bluetooth system does not provide any security at the applications level, therefore applications security may be an important consideration in building a wireless communications system using Bluetooth.

DIFFERENCES BETWEEN BLUETOOTH AND WiFi

Bluetooth and WiFi are different, complementary technologies. WiFi is used for wireless LANs and has a relatively wide range, while Bluetooth focuses on short range connectivity. Bluetooth is used by small groups of users in communication with each other, within networks referred to as personal area networks (PANs) - essentially the *ad hoc* networks referred to earlier.

The systems do, however, have similarities. Both allow computers to communicate with other devices, both are wireless and both operate in the 2.4 GHz spectrum band. Because of these similarities, Bluetooth is sometimes confused with WiFi. From a security standpoint, Bluetooth is not subject to the same types of attacks as WiFi, such as parking lot attacks, simply because it does not have enough range to be used for large LANs. Bluetooth, however, is subject to unauthorized intervention simply through proximity to another device, unless appropriate precautions are taken in configuring its security. An important method of doing this is to make use of the device authentication features of Bluetooth.

Bluetooth has an authentication feature that makes use of a “shared secret” between devices. This shared secret is called a link key and is established in a special communications session called pairing. All Bluetooth enabled devices that have had a previous connection to establish security procedures, and are therefore paired, share a common link key. There are two types of link keys: unit keys and combination keys.

When a device uses a unit key, it uses the same one for all of its connections. This approach is useful for devices with limited memory or a limited user interface. During the pairing procedure, the unit key is transferred in encrypted form to the other device. Only one of the two paired units is allowed to use a unit key. Combination keys are unique to a particular pair of devices and are only used to protect communications between those two devices.

WIRELESS ACCESS PROTOCOL (WAP)

The Wireless Access Protocol (WAP), mentioned earlier, is a standard format for presenting Web content on mobile devices. Many cell phones are equipped with a “WAP browser” that can be used to gain access to internet content. WAP browsers enable the content to be read, but also enable the user to interact with web sites and execute transactions, such as orders for goods and services. Some of the internet content can be sensitive, as well as some of the data input, depending on the nature of the application. WAP is now widely available in cell phones and, with the prospect of increased bandwidth in newer cell phone technology, there is a likelihood that the use of WAP interfaces for conducting commercial transactions will grow. As organizations enable their customers, mobile workers and business partners to execute transactions and gain access to corporate information and resources using WAP based technology, the security of WAP becomes a critical concern.

In a wired network, a firewall provides the first level of security between the user and the Web server being accessed. In the wireless world, devices called WAP gateways manage access to the Web server. Like firewalls, they provide encryption by using the Wireless Transport Layer Security (WTLS) specification. They also authenticate users to strengthen the security of the connection between the wireless device and the application server. The analogy, however, ends there. WAP gateways are simply network management devices, not firewalls, because firewalls have much stronger security features. The WAP gateway system does provide some data integrity, privacy, authentication and denial-of-service protection for WAP based wireless connections. But additional security, such as that provided by a firewall and encryption, may still be needed.

SECURITY STRATEGY

Like the technology, security strategy for wireless systems is evolving. This being the case, it is worthwhile bearing in mind the ultimate goals of such strategy — the ideals towards which enterprises should be moving. End-to-end protection is the goal of most security strategies. Where there are wireless environments, there normally is a wired network or environment to which it is connected and with which it interacts. Therefore, the end-to-end goal can only be reached if enterprises and service providers address the security challenges across their entire

system, both wired and wireless, controlling user access to both the network and individual resources within the system. Many enterprises have not yet reached this goal, because it is costly.

A good way to approach the management of the security over a diverse system is to make use of an applications level security infrastructure. Such an approach enables an organization to make use of the built-in security features of the wireless devices in use while, at the same time, adding features that are considered necessary in the circumstances for the enterprise-wide management of systems security. Access to the wireless networks should be subject to authentication procedures as rigorous as those that apply to the wired networks. Once a user has been allowed access to the wireless network, the application-level security infrastructure would control which resources the user is authorized to use and which transactions can be executed.

This approach provides an open infrastructure that can integrate with the diverse wireless technologies and security. The ideal system, for example, should support multiple authentication methods so as to accommodate the various types of Personal Identification Numbers (PINs), passwords, certificates and keys that are found in the wireless technologies, as well as those in the wired environment.

Such a system would provide access control for both wired and wireless applications from the same infrastructure. This eliminates the need to deploy and manage a separate security system for wireless systems and provides a single point of control for setting, monitoring and enforcing security policies. The security strategy can be formed and then managed so as to integrate fully with the strategies for the whole organization.

The use of an organizational security infrastructure allows user profiles to be managed for both the wired and wireless at the same time, in a single user profile management module. Users could update their profiles through wired web applications and have these changes conveyed to their wired and wireless Web accounts. This approach to access control provides users with a consistent experience, regardless of the nature of the input device.

A security infrastructure must also be scalable, so as to be able to accommodate growth in the

use of mobile devices. Typically, the introduction of wireless into an enterprise involves high numbers of users, placing potential strain on the security administration system. A good way to handle these volumes is to make use of rules-based user profiles, that minimize the need for human intervention each time a user profile changes. When user needs change, perhaps because of growth in their activity, then users can change their profile to gain access to the newly required resources, provided their activity still accords with the rules. Human intervention would still be required when the rules are not met, but this should occur less frequently.

An effective organizational security management system normally allows the dispersion of routine duties to various points in the enterprise, reducing strain on the central security administration people. This would include tasks such as adding, moving and deleting users; changing passwords; and updating personal profiles. Instead of being carried out by the central security administration, it would be possible for these tasks to be carried out by help desks, individual departments, separate divisions, etc. within a centrally controlled framework.

SECURING WIRELESS WEB TRANSACTIONS

The process of protecting wireless transactions on the web, in general, is similar to that for protecting wired web transactions. Sensitive data must be secured, normally through encryption, throughout the transmission. It is essential to have a security system that authenticates the users, authorizes the transactions and logs the transaction details. There must be strong access control over users entering from the Internet.

As with any system, wireless applications are subject to fraud and error. Automated monitoring of Web and wireless Web user activity is often a good way to deal with the volumes of activity and provide the ability to detect unusual or suspicious activity. If certain preset activity is detected, the system could then take countermeasures, such as sending an alert to an administrator and locking the user out of the application.

ASSURANCE

It is clear that wireless technologies pose risks for an enterprise that should be addressed in order

to reduce the risks of exposure to potential loss as a result of activities of hackers, other criminal activity or simply error by honest users. The audit approaches used by auditors need to address these risks, so their opinions will take into account the implications of the wireless systems being used by their clients.

This section of the white paper addresses the major audit implications of wireless systems at the overview level. It does not go into detail of procedures, but points to the need for auditors to understand the risks and to devise strategies for dealing with them. Since the use of wireless technologies is an emerging area, and rapidly evolving, it may be that a major contribution the auditors can make at this stage is to alert their clients to the need for management to evaluate these risks and to develop strategies internally for addressing them.

As with any audit, the auditors faced with wireless systems must first have an understanding of the systems, so as to be able to identify the threats and risks. To gain this understanding, they would need to identify the wireless technologies being used, what they are used for and how they have been deployed. Their usage is important in assessing the risk involved, since the greater the sensitivity of the data and applications, the greater the risk.

The auditors would determine if the organization has a wireless strategy and assess this strategy in light of the risks to which the organization is exposed. Then they would identify the administrative security structure and conduct tests to determine whether it is actually working. This would include, for example, the arrangements for administering wireless security elements, such as passkeys and security configuration. They would also evaluate the relative strengths and weaknesses of the strategy and administrative structure.

Having identified the relative risks of the wireless technologies being used, the auditors would review the security precautions in place, to assess whether the degree of risk has been appropriately addressed. The auditors would review and evaluate the configuration of the systems to determine which security features are in place. For example, for this part of the review, the auditors would determine whether the defaults have been set properly, such as turning on WPA or WEP security and turning off the *ad hoc* network option of WiFi.

The essential point about wireless is that it poses new security threats that need to be addressed, both by management and the auditors. In addition, they need to be addressed in the context of the overall systems, and the risks evaluated and assurance procedures developed taking into consideration this overall context.

CONCLUSION

The use of wireless communications equipment is a relatively new element of e-business, and poses unique risks and threats to security. It is important for auditors to gain an understanding of this new set of tools, and how it fits into the overall audit. It is also important for businesses and their managers to gain a good understanding of the risks of wireless technology when they are considering its implementation. This does not mean they necessarily should not go ahead with a wireless implementation, but it would mean they would make a more balanced decision, taking into account the risks as well as the benefits. While the general objectives and approach for wireless remain the same as wired environments, the details are considerably different, and the knowledge of the systems is necessary in order to properly audit these systems. Of course, the technology is changing and moving ahead rapidly, and keeping up with the changes will always be a challenge.

Additional Readings

1. *Wireless LAN Risks and Vulnerabilities* by Richard A. Stanley, published by the Information Systems Audit and Control Foundation, 2002.
2. Wireless LAN Security FAQ by Christopher W. Klaus of Internet Security Systems (ISS). (available at <http://www.iss.net/wireless/>).
3. *Securing m-Commerce* by Eric Olden, CTO of Securant Technologies (available at http://e-serv.ebizq.net/mob/olden_1.html).
4. *Security of the WEP Algorithm* by Nikita Borisov, Ian Goldberg and David Wagner (available at <http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html>).
5. *An Initial Security Analysis of the IEEE 802.1x Standard* by Arunesh Mishra and William A. Arbaugh, Department of Computer Service, University of Maryland (available at <http://www.cs.umd.edu/~waa/1x.pdf>).
6. *SAFE: Wireless LAN Security in Depth* by Sean Convery and Darrin Miller, Cisco Systems (available at <http://www.cisco.com/>).
7. *Wireless Network Security: 802.11, Bluetooth and Handheld Devices* (Special Publication 800-48) by the National Institute of Standards and Technology (available at NIST, Computer Security Resource Center, <http://csrc.nist.gov/publications>).

CICA Information Technology Advisory Committee

Chair

Donald E. Sheehy, CA•CISA Deloitte & Touche LLP, Toronto

Committee

Gary S. Baker, CA Deloitte & Touche LLP, Toronto

David Chan, CA•CISA Ontario Government Information Protection Centre,
Toronto

Allan W.K. Cheung, CA•IT, CISA The Canadian Depository for Securities Limited,
Toronto

Henry Grunberg, CA•IT Ernst & Young LLP, Toronto

Ray Henrickson, CA•IT/CISA Scotia Bank, Toronto

Carole Le Néal, CISA Mouvement des caisses Desjardins, Montreal

Erlinda L. Olalia-Carin, CISA KPMG LLP, Toronto

Robert G. Parker, FCA, CA•CISA Deloitte & Touche LLP, Toronto

Robert J. Reimer, CA•CISA PricewaterhouseCoopers LLP, Winnipeg

Douglas G. Timmins, CA Office of the Auditor General, Ottawa

Gerald D. Trites, FCA, CA•CISA St-Francis Xavier University, Antigonish, NS
(also technical consultant for the Committee)

CICA Staff

Andrée Lavigne, CA Principal, Research Studies

David J. Moore, CA Research Studies Director

Bryan C. Walker, CA Principal, Assurance Services

The Information Technology Advisory Committee (ITAC)
is part of the Knowledge Development Group at the CICA. Its role is to provide support
and advice on IT matters to the CA profession and the business community.