CMSGu2012-03

National Computer Board

Mauritian Computer Emergency Response Team

Enhancing Cyber Security in Mauritius

Guideline on Wireless Security

CERT-MU

National Computer Board
Mauritius

March 2012

Issue No. 3

Version 1.1

Table of Contents

1.0 Introduction 5
1.1 Purpose and Scope 5
1.2 Audience 5
1.3 Document Structure 5
2.0 Background 6
3.0 Wireless Devices and Network Threats 7
3.1 General Wireless Security Threats 7
3.1.1 Theft 7
3.1.2 Denial of Service (DoS) 7
3.1.3 Malicious Hackers 7
3.1.4 Malicious Code 7
3.1.5 Theft of Service 7
3.1.6 Industrial and Foreign Espionage 7
3.2 Home Wireless Threats 8
3.2.1 Piggybacking 9
3.2.2 Wardriving 9
3.2.3 Unauthorised Computer Access 9
3.3 Public Wireless Threats 10
3.3.1 Evil Twin Attacks 10
3.3.2 Wireless Sniffing 10
3.3.3 Peer-to-Peer Connections 10
3.3.4 Unauthorised Computer Access 10
3.3.5 Shoulder Surfing 11
4.0 Securing Wireless Networks 12
4.1 Securing Your Organisation's Wireless Network 12
4.1.1 Management Countermeasures 12
4.4.2 Operational Countermeasures 12
4.4.3 Technical Countermeasures 14
4.2 Securing Your Home Wireless Network 16
4.2.1 Make Your Wireless Network Invisible 17
4.2.2 Rename Your Wireless Network 17

4.2.3 Encrypt Your Network Traffic 17
4.2.4 Change Your Administrator Password 17
4.2.5 Use File Sharing with Caution 17
4.2.6 Keep Your Access Point Software Patched and Up to Date 18
4.2.7 Check Your Internet Provider's Wireless Security Options 18
4.3 Using Wireless Networking Safely in Public Spaces 18
4.3.1 Watch What You Do Online 18
4.3.2 Disable File Sharing 18
4.3.3 Be Aware of Your Surroundings 19
5.0 Conclusion 20
6.0 References 21
Appendix A 22
List of Acronyms 22
Appendix B 23
A. MyT Livebox Installation 23
Ethernet Cable Installation 23
Wifi Installation 23
B. ADSL Installation 23

DISCLAIMER: *This guideline is provided "as is" for informational purposes only. Information in this guideline, including references, is subject to change without notice. The products mentioned herein are the trademarks of their respective owners.*

1.0 Introduction

1.1 Purpose and Scope

This guide, while generic in nature, is focused towards helping organisations secure their wireless networks while they are open to attacks and users stay safe while using wireless networks to surf at home and in public places.

1.2 Audience

The target audience for this guide is organisations that make use of use wireless connections, wireless home users, including parents and teachers, and the public in general.

1.3 Document Structure

This document is organised into the following sections:

Section 1 includes the document's content, the targeted audience and the document's structure.

Section 2 gives a background on wireless networking.

Section 3 presents wireless devices and network threats.

Section 4 discusses ways to secure wireless networks.

Section 5 concludes the document.

Section 6 comprises a list of references that have been used in this document.

Appendix A defines a set of acronyms used in this document.

2.0 Background

Wireless networking enables computing devices with wireless capabilities to use computing resources without being physically connected to a network. The devices simply need to be within a certain range of the wireless network infrastructure. Wireless communications are mainly known for the benefits that they bring to users, namely portability, flexibility, increased productivity and lower installation costs. Wireless technologies cover a broad range of distinct capabilities adapting to different uses and needs.

- **Wireless Local Area Network (WLAN)**
  Wireless Local Area Networks (WLAN) for example; allow mobility of laptops within users' office without the need for cables and wires without losing network connectivity.

- **Ad Hoc Network**
  Ad hoc networks, such as those enabled by Bluetooth, on the other hand, allow data synchronization with network systems and application sharing between devices. Bluetooth functionality eliminates cables for printer and other peripheral device connections.

- **Handheld Devices**
  Handheld devices such as personal digital assistants (PDA) and cell phones allow remote users to synchronize personal databases and provide access to network services such as wireless e-mail, Web browsing, and Internet access.

The above technologies can offer enormous cost savings and new capabilities to diverse applications ranging from retail settings to manufacturing shop floors to first responders. However, risks are inherent in any wireless technology. Some of these risks are similar to those of wired networks; some are worsen by wireless connectivity; some are new. Perhaps the most significant source of risks in wireless networks is that the technology's underlying communications medium, the airwave, is open to intruders, making it the logical equivalent of an Ethernet port in the parking lot.

3.0 Wireless Devices and Network Threats

3.1 General Wireless Security Threats

The major concerns for wireless communications are device theft, denial of service, malicious hackers, malicious code, theft of service, and industrial and foreign espionage.

3.1.1 Theft

Theft is likely to occur with wireless devices because of their portability. Authorised and unauthorised users of the system may commit fraud and theft; however, authorised users are more likely to carry out such acts. Since users of a system may know what resources a system has and the system's security flaws, it is easier for them to commit fraud and theft.

3.1.2 Denial of Service (DoS)

A DoS attack can occur unexpectedly, such as other electronic devices causing interference, or it can occur deliberately, such as an attacker sending large numbers of messages at a high rate to flood the wireless network.

3.1.3 Malicious Hackers

Malicious hackers, sometimes called crackers, are individuals who break into a system without authorization, usually for personal gain or to do harm. Malicious hackers are generally individuals from outside of an organisation; however users within an organisation can also be a threat. Such hackers may gain access to the wireless network access point by eavesdropping on wireless device communications.

3.1.4 Malicious Code

Malicious code involves viruses, worms, Trojan horses, logic bombs, or other unwanted software that is designed to damage files or shut down a system.

3.1.5 Theft of Service

Theft of service occurs when an unauthorised user gains access to the network and consumes network resources.

3.1.6 Industrial and Foreign Espionage

Industrial and foreign espionage involves gathering proprietary data from corporations or intelligence information from governments through eavesdropping. In wireless networks, the

espionage threat stems from the relative ease with which eavesdropping can occur on radio transmissions.

Attacks resulting from the abovementioned threats, if successful, place an organisation's systems and, more importantly, its data at risk. Ensuring confidentiality, integrity, authenticity, and availability are the prime objectives of all organisation security policies and practices.

Risks in wireless networks practically equals to the risk of operating a wired network, in addition to the new risks introduced by weaknesses in wireless protocols. To mitigate these risks, organisations need to adopt security measures and practices that help bring their risks to a manageable level. For instance, they need to perform security assessments prior to implementation to determine the specific threats and vulnerabilities that wireless networks will introduce in their environments.

In performing the assessment, they should consider existing security policies, known threats and vulnerabilities, legislation and regulations, safety, reliability, system performance, the life-cycle costs of security measures, and technical requirements. Once the risk assessment is complete, the organisation can begin planning and implementing the measures that it will put in place to safeguard its systems and lower its security risks to a manageable level. The organisation should periodically reassess the existing policies and measures because computer technologies and malicious threats are continually changing.

3.2 Home Wireless Threats

By now, people should be aware of the need to secure traditional, wired internet connections. If you are planning to move to a wireless connection in your home, for instance, you should consider whether it will bring you more risks than benefits. Having wireless connection at home involves a device to your DSL or cable modem that broadcasts your internet connection through the air over a radio signal to your computers. If traditional wired connections are prey to security problems, you should think of the security problems that arise when you open your internet connection to the airwaves. The following sections describe some of the threats to home wireless networks.

3.2.1 Piggybacking

If your wireless network is not secured, anyone with a wireless-enabled computer within range of your wireless access point can access the internet over your wireless connection. The typical indoor broadcast range of an access point is 150 – 300 feet. Outdoors, this range may extend as far as 1,000 feet. So, if your neighborhood is closely settled, or if you live in an apartment, failure to secure your wireless network could potentially open your Internet connection to a surprising number of users. In so doing, you invite a number of problems:

- **Service violations**: You may exceed the number of connections permitted by your Internet service provider.
- **Bandwidth shortages**: Users piggybacking on your Internet connection might use up your bandwidth and slow your connection.
- **Abuse by malicious users**: Users piggybacking on your Internet connection might engage in illegal activity that will be traced to you.
- **Monitoring of your activity**: Malicious users may be able to monitor your Internet activity and steal passwords and other sensitive information.
- **Direct attack on your computer**: Malicious users may be able to access files on your computer, install spyware and other malicious programs, or take control of your computer.

3.2.2 Wardriving

Wardriving is a specific kind of piggybacking. The broadcast range of a wireless access point can make internet connections possible outside your home, even as far away as your street. Savvy computer users know this, and some have made a hobby out of driving through neighbourhoods with a wireless-equipped computer, sometimes with a powerful antenna searching for unsecured wireless networks. This practice is known as "wardriving." Wardrivers often note the location of unsecured wireless networks and publish this information on web sites. Malicious individuals' wardrive to find a connection they can use to perpetrate illegal online activity using your connection to mask their identities. They may also directly attack your computer, as noted in the "Piggybacking" section above.

3.2.3 Unauthorised Computer Access

An unsecured wireless network combined with unsecured file sharing can give rise to a disaster. Under these conditions, a malicious user could access any directories and files you have allowed for sharing.

3.3 Public Wireless Threats

A wireless-enabled laptop can make you more productive outside your office or home, but it can also expose you to numerous security threats. The following sections describe some of the security threats you face when using a public access point.

3.3.1 Evil Twin Attacks

In an evil twin attack, the attacker gathers information about a public access point and then sets up his or her own system to impersonate the real access point. The attacker will use a broadcast signal stronger than the one generated by the real access point. Unsuspecting users will connect using the stronger, fake signal. As the victim is connecting to the Internet through the attacker's system, it is easy for the attacker to use specialised tools to read any data the victim sends over the internet. This data may include credit card numbers, username and password combinations, addresses, and other personal information.

3.3.2 Wireless Sniffing

Many public access points are not secured, and the traffic they carry is not encrypted. This can put your sensitive communications or transactions at risk. Because your connection is being transmitted in cleartext, malicious users can use "sniffing" tools to obtain sensitive information such as passwords, bank account numbers, and credit card numbers.

3.3.3 Peer-to-Peer Connections

Many laptop computers, particularly those equipped with 802.11-type Wi-Fi wireless networking cards, can create ad hoc networks if they are within range of one another. These networks enable computer-to-computer connections, a situation that creates security concerns. An attacker with a network card configured for ad hoc mode and using the same settings as your computer may gain unauthorised access to your sensitive files. You should note that many PCs ship from the manufacturer with wireless cards set to ad-hoc mode by default.

3.3.4 Unauthorised Computer Access

As is the case with unsecured home wireless networks, an unsecured public wireless network combined with unsecured file sharing can lead to disasters. Under these conditions, a malicious user could access any directories and files you have allowed for sharing.

3.3.5 Shoulder Surfing

In public wireless areas, the bad guys do not even need a computer to steal your sensitive information. The fact that you may be conducting personal business in a public space is opportunity enough for them. If close enough, they can simply glance over your shoulder as you type. Or, they could be peering through binoculars from an apartment window across the street. By simply watching you, they can steal all kinds of sensitive, personal information.

4.0 Securing Wireless Networks

4.1 Securing Your Organisation's Wireless Network

4.1.1 Management Countermeasures

- **Risk Assessment**

  Information security officers and network administrators should conduct a risk assessment before handheld devices are introduced into the organisation's computing environment.

- **Education and Awareness**

  The organisation should educate the users about the proper use of their handheld devices and the security risks introduced by their use by providing short training courses or educational materials to help users use these devices more productively and more securely.

- **Security Policies**

  Network administrators should establish and document security policies that address their use and the users' responsibilities. The policy document should include:

  - The approved uses
  - The type of information that the devices may store
  - Software programs they can install
  - How to store the devices and associated modules when not in use
  - Proper password selection and use
  - How to report a lost or stolen PDA
  - Any disciplinary actions that may result from misuse

- **Audit**

  Organisations should also perform random audits to track whether devices have been lost or stolen.

4.4.2 Operational Countermeasures

- **Due Diligence**

  Operational countermeasures require handheld device users to exercise due diligence in protecting the handheld devices and the networks they access from unnecessary risks. Most operational countermeasures are common sense procedures that require

voluntary compliance by the users. Operational countermeasures are intended to minimise the risk associated with the use of handheld devices by genuine users. Although a determined malicious user can find ways to intentionally disclose information to unauthorised sources, the handheld security policy and the organisation's operational countermeasures should make clear the user's responsibilities.

- **Proper Labeling**

  The back of the PDA device should always be labeled with the owning organisation's name, address, and phone number in case it is lost. Handheld device users should be provided with a secure area to store the device when not in use. A desk with drawers that lock or a file cabinet with locks are available in most offices and should provide sufficient physical security against theft from within the office environment.

- **Cables and Locks**

  Galvanized steel cables and locks should be used to secure handheld devices to the user's desktop if other physical controls are not available. Although these measures cannot ensure that a determined thief will not cut these cables or locks, it does prevent an opportunistic thief from walking away with an unattended handheld device. While employees are on travel, fireproof safes should be used to store handheld devices.

- **Inventory Checks**

  Security administrators should have a list of authorised handheld device users, to enable them to perform periodic inventory checks and security audits. Individuals that use their handheld devices for other than business uses should comply with the organisation's security policy or be restricted from accessing the organisation's network.

- **Secure data on handheld devices**

  In general, users should not store sensitive information on handheld devices. However, if sensitive information is stored on the handheld device, users should be encouraged to delete sensitive information when no longer needed. This information can be archived on the PC during synchronisation and transferred back to the PDA when needed.

- **Disable Infrared and Bluetooth**

  Users are recommended to disable Infrared and Bluetooth ports during periods of inactivity to deter them from leaking information from their handheld devices.

4.4.3 Technical Countermeasures

Technical countermeasures should address the security risks identified during the risk assessment and should ensure that the organisation's security policy is being enforced.

- **Authentication**

  Handheld device users must be able to authenticate themselves to the handheld device by providing a password, a token, or both. At the most basic level, organisations should require PDAs to be password protected. Password protection is already included with most handheld devices, but is usually not enabled in the default setting. Users should be prompted for a password when accessing the handheld device or the desktop PC synchronization software.

  Biometric user authentication technologies are also available for handheld devices. Fingerprint readers can be attached to the handheld devices through a serial or USB port and can be set to lock the whole device, to lock an individual application, or to connect to a remote database over a network or dial-up connection. Tamper-proof smart cards, which contain unique user identifying information such as a private key, can also be used to authenticate the user to the device.

- **Encryption**

  Encryption software can be used to protect the confidentiality of sensitive information stored on handheld devices and mirrored on the desktop PC. The information on add-on backup storage modules should also be encrypted and the modules securely stored when not in use. This additional level of security can be added to provide an extra layer of defense to further protect sensitive information stored on handheld devices.

  Many software programs are freely available to help users encrypt these types of files for an added layer of security. Handheld device users may also choose to encrypt files and messages before the files and messages are transferred through a wireless port.

- **Antivirus Software**

  Antivirus software is another important security measure for handheld devices. All organisations, regardless of their security requirements, should incorporate PDA antivirus applications to scan e-mail and data files and to remove malware from files upon transmission to the device. The software should scan all entry ports (i.e., beaming, synchronizing, e-mail, and Internet downloading) as data is imported into the device, provide online signature update capabilities, and prompt the user before it deletes any suspicious files.

  The organisation should further require regular updates to the antivirus software and require associated workstations (i.e., the PCs with which users synchronize their PDAs) to have current, properly working virus-scanning software. Most major PC antivirus software vendors have handheld device antivirus software that can be downloaded directly from their Web sites.

- **Public Key Infrastructure (PKI)**

  Many handheld devices are beginning to offer support for PKI technologies. PKI is one of the best available methods for meeting confidentiality, integrity, and authenticity security requirements. A PKI uses an asymmetric encryption method, commonly known as the "public/private key" method, for encrypting and ensuring the integrity of documents and messages. A certificate authority issues digital certificates that authenticate the claimed identity of people and organisations over a public network such as the Internet. The PKI also establishes the encryption algorithms, levels of security, and the key distribution policy for users. PKI support is often integrated into common applications such as Web browsers and e-mail programs by validating certificates and signed messages. The PKI can also be implemented by an organisation for its own use to authenticate users that handle sensitive information.

  The use of PKI counters many threats associated with public networks, but also introduces management overhead and additional hardware and software costs that should be evaluated while performing the risk assessment and selecting the appropriate countermeasures to meet the organisation's security requirements. If PKI has already been deployed to provide security services in the wired network of an

organisation, users compromise of the enterprise data in the event of a lost or stolen PDA.

- **VPN and Firewalls**

  Handheld devices are beginning to offer support for personal firewalls and VPN technologies and to offer network administrators effective countermeasures against threats to the confidentiality, integrity, and authenticity of the information being transferred. A packet filter firewall, for example, screens Internet traffic based on packet header information such as the type of application (e-mail, ftp, Web, etc.) and by the service port number.

  A VPN creates a virtual private network between the handheld device and the organisation's network by sharing the public network infrastructure. VPN technology offers the security of a private network through access control and encryption, while taking advantage of the economies of scale and built-in management facilities of large public networks. Network administrators should look for the following features when purchasing VPN technologies: interoperability with existing infrastructure, support for wireless and dial-up networking, packet-filtering or stateful-inspection firewall, automatic security updates, and a centralized management console.

- **Enterprise Solutions**

  Enterprise handheld device management software allows network administrators to discover handheld devices, install and remove applications, backup and restore data, collect inventory information, synchronize data with corporate servers and databases, and perform various configuration management functions from a central location.

  Enterprise security solutions have been introduced that allow the organisation to set policies on all handheld devices under the organisation's control. Some of the options that are available include defining the type of encryption to use, which application databases to encrypt, password protection, and port protection.

4.2 Securing Your Home Wireless Network

While the security problems associated with wireless networking are serious, there are steps you can take to protect yourself. The following sections describe these steps.

4.2.1 Make Your Wireless Network Invisible

Wireless access points can announce their presence to wireless-enabled computers. This is referred to as "identifier broadcasting." In certain situations, identifier broadcasting is desirable. For instance, an internet cafe would want its customers to easily find its access point, so it would leave identifier broadcasting enabled.

However, you are the only one who needs to know you have a wireless network at home. To make your network invisible to others, see your access point's user manual for instructions on disabling identifier broadcasting. While this kind of "security through obscurity" is never guaranteed, it is a starting point for securing your wireless network.

4.2.2 Rename Your Wireless Network

Many wireless access point devices come with a default name. This name is referred to as the "service set identifier" (SSID) or "extended service set identifier" (ESSID). The default names used by various manufacturers are widely known and can be used to gain unauthorised access to your network. When you rename your network, you should choose a name that will not be easily guessed by others.

4.2.3 Encrypt Your Network Traffic

Your wireless access point device should allow you to encrypt traffic passing between the device and your computers. By encrypting wireless traffic, you are converting it to a code that can only be understood by computers with the correct key to that code.

4.2.4 Change Your Administrator Password

Your wireless access point device likely shipped with a default password. Default passwords for various manufacturers are widely known and can be used to gain unauthorised access to your network. Be sure to change your administrator password to one that is long, contains a combination alphanumeric and special characters (such as #, $, and &), and does not contain personal information (such as your birth date). If your wireless access point does not have a default password, be sure to create one and use it to protect your device.

4.2.5 Use File Sharing with Caution

If you do not need to share directories and files over your network, you should disable file sharing on your computers. You may want to consider creating a dedicated directory for file

sharing, and move or copy files to that directory for sharing. In addition, you should password protect anything you share, and use a strong password. Never open an entire hard drive for file sharing.

4.2.6 Keep Your Access Point Software Patched and Up to Date

From time to time, the manufacturer of your wireless access point will release updates to the device software or patches to repair bugs. Be sure to check the manufacturer's web site regularly for any updates or patches for your device's software.

4.2.7 Check Your Internet Provider's Wireless Security Options

Your Internet Service Provider may provide information about securing your home wireless network. Check the customer support area of your provider's web site or contact your provider's customer support team.

4.3 Using Wireless Networking Safely in Public Spaces

Accessing the Internet via a public wireless access point involves serious security threats you should guard against. These threats are compounded by your inability to control the security setup of the wireless network. Furthermore, you are often in range of numerous wireless-enabled computers operated by people you do not necessarily know. The following sections describe steps you can take to protect yourself.

4.3.1 Watch What You Do Online

You are likely to have an unsecured, unencrypted network connection when you use a public wireless access point, so you should be careful about what you do online. There is always the chance that another user on the network could be monitoring your online activities, such as:

- Online Banking
- Online Shopping
- Sending Email
- Typing passwords or credit card numbers

4.3.2 Disable File Sharing

File sharing in public wireless spaces is even more dangerous than it is on your home wireless network. This is because you and your wireless-enabled laptop are likely to be even closer to other wireless computers operated by people you do not know. Also, many public

wireless networks feature peer-to-peer networking in which other computers will attempt to connect directly to yours. To leave file shares open in this kind of environment is to attract risks. To prevent attackers from gaining access to your sensitive files, you should disable file sharing when connecting to a public wireless access point. Consult the help file for your operating system to learn how to disable file sharing.

4.3.3 Be Aware of Your Surroundings

When using a public wireless access point, you should be aware of what is happening around you. Ask yourself the following questions:

- Are others using their computers in close proximity to you?
- Can others view your screen?
- Are you sitting near a window through which someone, using binoculars, could get a view of your screen?

If you answered "yes" to any of the above questions, your sensitive data might be at risk. Consider whether it is essential to connect to the Internet. If an Internet connection is not essential, you are recommended to disable wireless networking. If you do need to connect, use caution and follow the steps noted above.

5.0 Conclusion

Wireless security faces a number of hurdles, especially the challenge of adapting wired technologies to the wireless world, which has more constrained resources. Hence, it is important that organisations put in place realistic policies and measures to that their employees do not expose internal information to potential threats. It is also essential that home users follow some safety principles on their wireless networks and that they be very cautious when connecting to public wireless networks to access sensitive information.

6.0 References

- Wireless Network Security, 802.11, Bluetooth and Handheld Devices, NIST
- Using Wireless Technology Securely , US-CERT
- Guidelines for Securing Wireless Local Area Networks (WLANs), NIST

Appendix A

List of Acronyms

DoS	Denial of Service
ESSID	Extended Service Set Identifier
PDA	Personal Digital Assistant
PKI	Public Key Infrastructure
SSID	Service Set Identifier
VPN	Virtual Private Network
Wi-Fi	Wireless Fidelity
WLAN	Wireless Local Area Network

Appendix B

A. MyT Livebox Installation

Ethernet Cable Installation

1. For installation by Ethernet/Network Cable, verify that you have a free Ethernet port on your computer.
2. Check if you have all the required tools and cables in the installation pack.
3. Insert the installation CD in your CD drive and follow the instructions until installation is complete.
4. A window will appear if you are using Windows Vista. Click on “Home”
5. Click on continue
6. Finally, click on close.
7. Wait until the installation is complete and you will then be able to access the Internet.

Wifi Installation

1. For wifi connection, go to Network and Sharing Centre
2. Click on connect to a network
3. Choose your Livebox name
4. Enter your network key (at the back of your router)
5. You should now be able to connect to the Internet via wifi

B. ADSL Installation

1. Run installation CD
2. Connect your telephone cable to your modem
3. Enter your username and password
4. You will then be able to connect to the internet.