GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

iPAQ 4150 Security in the Corporate Environment – Some of the Basics

Authored by Andrew Hobbis
21st January 2004

Practical Assignment – GSEC Certification
Version 1.4b Option 1

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Abstract

The use of Personal Digital Assistants (PDAs) as a tool of choice for users of mobile computing has escalated exponentially over recent years. PDAs are being shipped with the functionality and potency of larger desktop and notebook devices. The convenience of their size makes them the perfect toy or weapon of choice that is capable of more than many information security officers and IT managers realise.

This paper will begin to analyse some of the significant security risks of PDAs, specifically the HP iPAQ 4150 to the corporate environment. Once the risks have been identified, basic policy requirements to mitigate these risks will be considered. In addition, the paper will address the implementation of policy requirements on the HP IPAQ 4150 using the standard software bundle.

© SANS Institute 2004, Author retains full rights.

Contents

Risks of the iPAQ 4150 to the Corporate Environment 4

Corporate PDA Policy Considerations 6

Implementing Policy Requirements - iPAQ 4150 10

- Configuring the “Welcome” Message 11
- Password Controls 12
- Network Connections 14
  - Active Sync 14
  - Infra-Red 14
  - Bluetooth and Wireless 15

References 20

© SANS Institute 2004, Author retains full rights.

Risks of the iPAQ 4150 to the Corporate Environment

The iPAQ 4150 is a highly capable personal digital assistant. To identify the security risks of the iPAQ 4150, consideration should first be given to the communication capabilities of the device. The standard communication features of the iPAQ 4150 include:

- Wireless 802.11b
- Bluetooth
- iR
- USB docking station

The full specifications of the iPAQ 4150 are available at http://h50025.www5.hp.com/hpcom/au_en/11_26_60_2343_FA174A.html. Other communication capabilities can be added to the device. For this practical assignment, only the risks associated with the standard capabilities have been examined.

The standard operating platform is Windows Pocket PC 2003 edition (Windows CE 4.20.1081). However, other operating systems can be loaded onto the device. For this practical it is assumed the operating system in use is Windows Pocket PC 2003 with the standard software bundle.

Security risks include threats to the confidentiality, integrity and availability of corporate information.

Many of the unique risks associated with PDAs are due to their small size, allowing them to be easily lost or stolen. PDAs are often used to store information including email, personal contacts, files and documents such as Word and Excel, and calendar details such as important dates, appointments and meeting times. In addition, a PDA configured to connect to a corporate environment may contain sensitive configuration details about the corporate network, such as usernames, network addressing, domain names even the corporate SSID where an 802.11x network is used.

If the PDA was lost or stolen, as a minimum, the user and corporation will be inconvenienced as the information contained on the PDA would no longer be available. The user information may be sensitive and assist in an inference attack against the corporation. Sensitive configuration information may provide an attacker with foothold to gain unauthorised access to the corporate environment.

As an example, suppose a corporation was in the process of tendering for a large contract. One of the staff working on the tender uses their PDA to store emails, contacts, calendar information and a backup of the tender document. These types of data may give details about sensitive correspondence between the owner and his colleges, or tenderer with details about their tender, compromising the confidentiality of their proposal.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

The device may contain contact details which would possibly include contacts within the corporation and contacts in the tendering organisation. This may be used by a malicious person to perform a social engineering attack to gain access to other sensitive information. Even the contact details of the tenderer could be used to perform an inference attack to determine who the corporation is tending to and what type of work the corporation is targeting.

In addition, the types of information discussed above may also provide a great starting point for the theft of the owner's identity, which could result in their identity within the corporation being compromised, particularly in larger organisations.

In addition to data loss or theft, the iPAQ 4150's size also allows it to be easily concealed within a work area or on an individual for malicious use. The device could be used to facilitate a number of potential internal security breaches, including covertly recording sensitive conversations, being deployed as an unauthorised wireless access point, or capturing internal network traffic.

One of the other significant risks associated with connecting an iPAQ 4150 to a corporate network comes from viruses, malware, worms, trojans and other malicious code. These may or may not impact the iPAQ 4150 itself, but they could be transmitted from the iPAQ to other devices on the corporate network. The standard software bundled with the iPAQ 4150 does not include anti-virus software. Many of the large anti virus solution providers have products designed for mobile devices such as PDAs. These products are not addressed in this paper.

From an IT governance perspective, it is always necessary to know what devices are attached to the corporate environment to be able to manage them properly. One of the biggest questions facing corporations is whether to allow personal PDAs to connect to corporate environment, or only allow access to company provided devices. It is difficult for a corporation to control a device it does not own.

Company provided devices can be managed through policy, a standard operating environment and regular auditing.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Corporate PDA Policy Considerations

The first step to reducing the risks described above is to develop a corporate policy on PDA usage and security. A PDA policy should not be specific to a particular device. Instead the policy should be applicable to all PDA devices. Otherwise every time a new model or feature is release, the policy will be out of date.

The policy should be clear, strict and enforceable. Policies for PDAs are often very similar to laptop or mobile phone policies as many of the threats and risk are similar.

As policy can only be reasonably enforced on company provided devices, the policy considerations below do not consider privately owned devices.

As minimum a PDA policy should include:

- Guidelines about what data can and cannot be stored on a mobile device
- Rules about storing and accessing corporate data using registered company provided PDAs only
- Outlining employee responsibilities for the protection of the data
- Rules and configuration requirement detailing what security measures need to be employed before a device can be used to store corporate data.
- Consequences of breaching the policy[1]

The decision about what data is allowed to be stored on a mobile device must be made by the information owners. The type of data allowed to be stored on a PDA can vary greatly between corporations. To begin with data should be appropriately classified, using agreed classification guidelines. Once the data is classified, the decision about whether it is allowed to be stored on a mobile device should become clear.

As a general rule PDAs should be limited to storing only data which is classified for public use and contains no sensitive information.

All staff, including permanent, temporary and contract employees should be aware that personal PDAs are not to be used to access or store corporate information. If they staff member requires a PDA, they should acquire a company provided device through the appropriate processes.

Outlining the employees' responsibilities for the protection of data ensures that all mobile device users are aware of the requirements and expectations placed on them. If the mobile device stores sensitive corporate information, the PDA user should be aware that they are responsible for the security of the data while it is on the device. The device user should be given strict guidelines on their responsibilities in ensuring the security of the device. For example, mobile devices should not be left unattended especially in public areas, cars,

[1] Hayday, Graham. p.1.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

unsecured office areas or in easily accessible areas at the users' home. Physical access to the device should be the responsibility of the device user.

The security rules and requirements need to be included in the policy. When considering the initial security rules and requirements, a deny everything approach should be taken as a starting point. Functionality of the PDA that is not required should be disabled.

One of the fundamental security controls is the user password. This provides authentication of the identity of the user. A password should be configured to be a sufficient length to increase the permutations of possible character combinations to deter password guessing attacks. The password should be comprised of a combination of alpha, numeric and punctuation characters. In additional to a long password, the device should be configured to require a password every time it is turned on.

The use of password hint features to remind the owner of the password should be discouraged as it can provide an attacker with information to guess the actual password.

Passwords should be changed regularly to reduce the length of time a compromised password is useful for.

A mechanism to prevent or deter repeated attempts to guess the password (brute force attacks) should also be considered.

A welcome message should be set to warn any unauthorised users against using the device. This should be shown as soon as the device is turned on before proceeding to the password prompt.

In addition to the welcome message, if the device can be configured to provide the owners details on the start-up screen, care should be taken when configuring the information to be presented. If a device was found with the owner details of a CEO of a major corporation, the finder of the device may be more curious of the contents of the device, than if the owner details were not provided. On the other hand, if a device was found with no owner information, there is no easy way to identify how to return the device. The balance is to provide return details for the device without increasing the interest or curiosity of the contents with to much information about the owner.

The data communication between the device and the corporate network should also be appropriately secured. One of the best means of securing the communications between the PDA and other devices is to minimise when communication services are open. This can be achieved by only allowing manual connections to be established and for the connections between the PDA and other devices to be disabled when not in use.

In addition, where possible the communication should be encrypted to prevent eavesdropping based attacks using SSL or other secure communication technologies.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Other standard means of communication on many PDA devices includes:

- Infra-red,
- Bluetooth
- WLAN 802.11X

To maximise security of the device, all three of these features should be disabled to minimise exposure from attacks in the wireless spectrum. If these services are required, they should be disabled when not is use.

Infra-red is rarely used as most applications of infra-red are more reliable using one of the other two means of wireless communication. The infra-red port should be disabled or prevent from accepting connections without prompting for authorisation from the user.

If Bluetooth is required, connections should only be established with pair or trusted devices. Connections should be initiated by the PDA. The device should not broadcast its presence allowing other devices to discover it easily. All communications between the PDA and the receiving Bluetooth device should be encrypted to prevent eavesdropping. To connect to the PDA through Bluetooth, authorisation should also be required.

Similarly WLAN devices should only connected to preferred or trusted devices. Care should be taken to ensure the PDA is not accidentally connected to networks that the user is no authorised to access. In Australia, this may result in legal action against the user, even if the intent of the user was not malicious. All WLAN communications should be secured and encrypted using, the EAP and WEP functionality. The static shared-key Wireless Equivalent Privacy (WEP) algorithm can be easily defeated as proven by researchers at the University of California, Berkley[2]. As a result, alternative approaches to wireless security are necessary to help secure connections over 802.11X WLANs.

If these features are not available on the device, the corporation should consider purchasing third party software to meet these requirements.

The PDA policy should address all aspects of security for the device, including but not limited to, password and user authentication controls, data communication controls, virus protection, the use of automatic deletion software, use of third party PDA security tools, use of encryption, unlicensed software and malware.

In addition to the requirements for using and securing a PDA, the policy should include information about the consequences for breaching the policy. Employees should be aware of the consequences of non compliance to ensure they can be held accountable for their actions if required. Disciplinary action may vary depending on the severity of non-compliance, and may vary from an official reprimand through to dismissal.

[2] Dedo, Douglas. p.11.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

With any policy, it is important to ensure the staff actually understand the requirements of the policy and agree to be bound by them. Once the policy has been finalised and endorsed by senior management, an awareness program of the policy should be initiated. All staff should be required to sign an agreement to be bound by the policy before they are provided with a PDA.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Implementing Policy Requirements - iPAQ 4150

The configuration of the device can dramatically impact the security of the information stored on it, and the networks the device is connected to. Most corporate PDA policies require the standard features on the iPAQ 4150 to be securely configured. These may include requiring “authorised access only” welcome messages, passwords and secure data communication. The standard software bundled with the iPAQ 4150 does not include antivirus protection or automatic deletion software.



To begin, the basic security settings must be configured, including the welcome message, the password controls and some of the fundamental connectivity settings. These can both be configured in the device settings as follows:

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

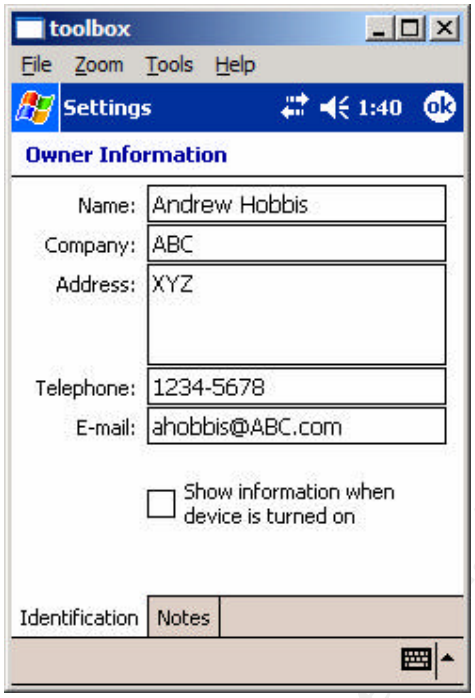
Configuring the "Welcome" Message

Configure the Welcome message on the iPAQ 4150 as follows:

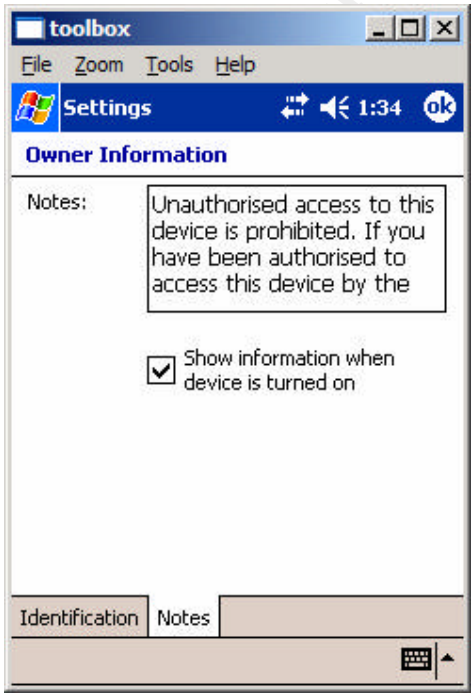
From the Start menu select Settings > Owner Information

The Owner Information has 2 tabs:

- Identification
- Notes



The identification tab allows the Owner of the device to enter in their personal details, including Name, Company, Address and other contact details. These details can be completed. However, the check box option to show the information when the device is turn on, should be left unchecked. If the box is checked, the owner's details will be provided before any user authentication takes place. This would provide a malicious user with details about the identity of the owner, providing a basis for inference and social engineering attacks.



The notes tab provides the owner a free text box to edit. This should be used to enter an "authorised users only" warning message. This message should not welcome the user in anyway. To display this message, check the "Show information when device is turned on" check box, as shown below. To pass on to the authentication screen the user needs to tap the screen. The warning message should indicate that by tapping the screen the user accepts the warning message, and believes he or she is an authorised user of the device. In addition, the message should contain return information in case the device is lost. This should include a return address (preferably a secure post office box) and phone number to be contacted if the

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

device is found. Personal details about the user or their employer should not be included, as that type of information may be used as a basis for inference or social engineering attacks.

Once these settings have been completed, select the ok button on the top right corner of the screen.

Password Controls

Configure the Welcome message on the iPAQ 4150 as follows:

From the Start menu select Settings > Personal > Password >
The Password configuration has 2 tabs:

- Password
- Hint



The Password configuration tab allows configuration of password settings.

An inactivity lockout time can be set. The check box “Prompt if device unused for” box should be selected to enable this functionality. The inactive time before the device requires the user to re-authenticate can be selected by using the drop down box. A period of 5 minutes or less should be selected. For stronger security a period of 0 minutes should be selected.

This lock out feature only activates on power-off and does not activate while the device is on. For example, if you set the inactive time to 5 minutes, the device must be off for 5 minutes, before it will request a password when it is next turned on. For stronger security, a setting of 0 minutes will require a password every time the device is turned off. The iPAQ 4150 does not turn off automatically when it is in the docking station. Users should be required to turn off their device when it is not being used or it is left unattended. This will force the requirement to enter the password before access is granted to the user. In this state the device should still provide calendar reminders, so user functionality should not be dramatically impacted by this requirement.

Once a password is configured, the password will be required every time the owner attempts to connect the device to a PC using ActiveSync.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

The Password settings also allow the owner to select between two types of passwords:

- Simple 4 digits
- Strong alphanumeric password



The strong alphanumeric password option should be selected requiring the owner to create a password of at least 7 characters long using a combination of uppercase and lowercase letters, numbers and special characters. An error message confirming the password policy is shown when a password is selected which does not meet the criteria.
The strong alphanumeric password option should be selected requiring the owner to create a password

The hint tab allows the owner to configure a clue to help them remember their password.



As shown, this provides the owner with a free text box to enter a hint. This hint is not secure and should not provide information about the password to anyone except the owner.

A good clue will have not relationship to the answer, but will still serve as a reminder of the password to the owner. For example, suppose you used your child's name and their birthday as your password. The hint should not say "child's name and birthday". Instead, you should use something which makes you remember you child's name and birthday, like the type of birthday cake they like, e.g. "chocolate cake". This would provide minimal information to a 3rd party about the password.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

For increased security the hint should not be used, or it should be configured as a “red herring”. The later option may increase the time taken to guess the users password. However, where a systematic brute force attack is used to break the password, this tactic will not cause a delay.

There is no available option to set a self destruct mode, time delay or account lockout in the event of a series of unsuccessful log in attempts.

Network Connections

Active Sync

Active Sync manages the synchronisation of data between the IPAQ and the owners PC or server. This can be performed using the USB docking station (wired) or using one of the standard wireless networking features such as Bluetooth, IR or 802.11X.

The synchronisation settings should be set to only manually synchronise and to drop the connection when not synchronising. If the owner synchronises their data to a server, the option to always synchronise using SSL should be selected in addition to the above configuration setting discussed above.

This can be done as follows:
From the start menu select ActiveSync > Tools > Options

The options should be configured depending on the synchronisation methods used (e.g. PC, Server or Mobile).

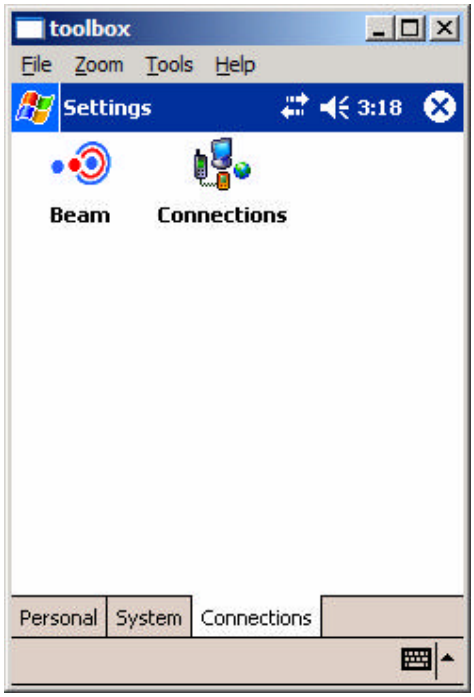
Infra-Red

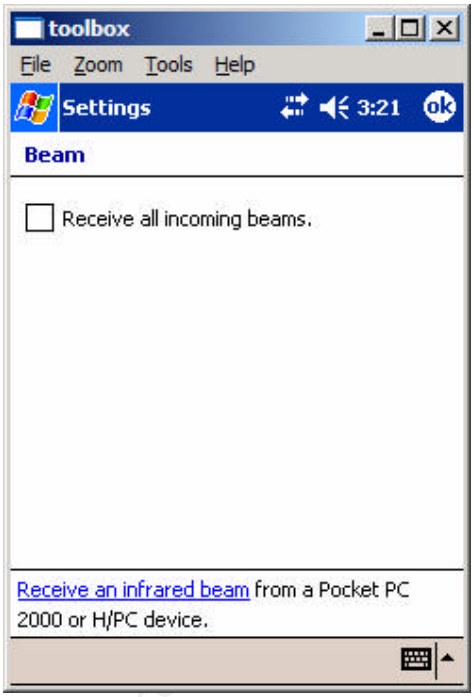
The wireless connectivity on the iPAQ 4150 can be configured in a variety of different ways depending on the requirements of the owner. If wireless connectivity is not required, the functionality should be switched off.

Disable the infra-red from accepting incoming beams, as follows:

From the Start menu select Settings > Connections > Beam

© SANS Institute 2004, Author retains full rights.

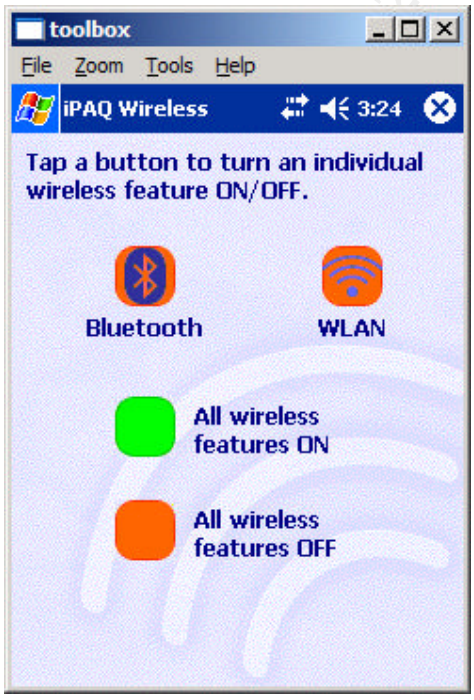




Ensure the check box “Receive all incoming beams” is not checked and then choose ok to make the change effective.

Bluetooth and Wireless

Disable the Bluetooth and 802.11X, as follows:
From the Start menu select iPAQ Wireless



This screen allows the owner to disable or enable both the Bluetooth and WLAN (802.11X) features. The orange colour indicates the feature is currently switched off. The green colour indicates the feature is on.

To disable both WLAN and Bluetooth, select the orange, “All wireless features OFF” button.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.



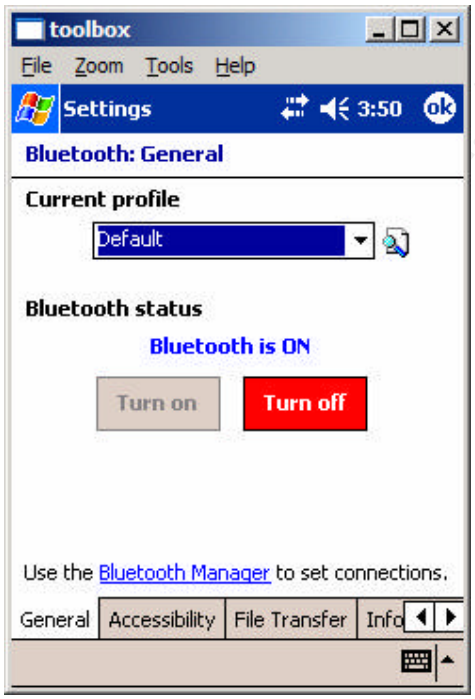
Where the Bluetooth or WLAN functionality is required the owner should ensure the connections are secured in the most appropriate manner.

Configure the Bluetooth settings as follows:

From the Start menu select Settings > System > Bluetooth

Bluetooth has 8 configuration tabs:

- General
- Accessibility
- File Transfer
- Information Exchange
- Serial Port
- Dial-up networking
- Personal Network Server
- About



The General tab provides the owner with the ability to select profiles, turn Bluetooth on or off and manage their Bluetooth connections using the Bluetooth Manager.

The Bluetooth manager can be used to configure a number of Bluetooth tools using wizards. These setting have not been addressed in this paper as they vary considerable depending on the users needs.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.



The Accessibility tab allows the configuration of the device identification and accessibility settings.

The Name field should be set to something meaning full to allow the Owner of the other Bluetooth device to identify the iPAQ 4150 and allow the connection.

The Accessibility options should be configured as necessary. Where possible, the “Allow other devices to connect” check box should not be selected.

If other devices need to be able to connect the iPAQ 4150, the “Allow other devices to connect” check box should be selected. Preferably, if the other devices are configured correctly, accessibility should be limited to Paired devices only, and the “Other devices can discover me” check box should not be selected.

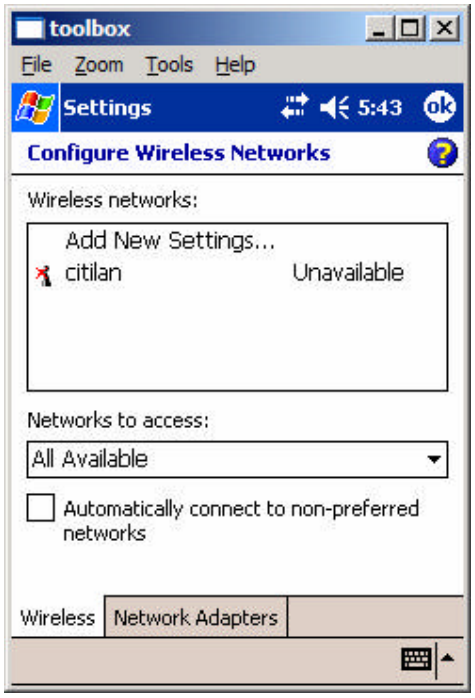


If the owner uses the file transfer, information exchange, serial port, personal network server or Bluetooth dialup features, the service should require authorization, authentication (Passkey), and encryption.

The other settings should be configured with security in mind to ensure they are the most appropriate. As they can vary substantially depending on the owner’s needs, they have not been discussed in this document.

Once these settings have been completed, select the ok button on the top right corner of the screen.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.



Appropriately securing a WLAN 802.11X wireless connection can be difficult. The iPAQ provides the owner with the additional options of using a VPN connection or using the Extensible Authentication Protocol (EAP).

Configure the WLAN settings as follows: From the Start menu select Settings > Connections > Connections > Advanced > Network Card

These settings enable the owner to manage the WLAN settings. Depending on the type of WLAN that the owner is connecting to, the owner should select from the “Networks to Access:” drop down menu whether the device should connect to only access points, only computer-to-computer or all available networks.

The check box “Automatically connect to non-preferred networks” should not be selected. This option is dangerous and should never be selected.



When a connection is configured or available it will be displayed in the “Wireless networks:” box in the top half of the screen. By selecting the network the owner can configure the network authentication security options.

The “Data encryption (WEP Enabled)” check box should be selected. Even though WEP is able to be defeated is still provides a delay before an unauthorised user can gain access to the network.

The “Network Authentication (Shared mode)” should be selected. Where possible, the key should be manually entered and should not be provided automatically.

In addition, EAP should be selected to provide stronger authentication.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.



To use a VPN connection, from the Start menu select Settings > Connections > Connections > Add a new VPN server connection.

This provides the owner with a choice between IPSec / L2TP and PPTP VPN types. Other configuration details are available depending on the type of VPN selected.

© SANS Institute 2004, Author retains full rights.

References

Hewlett-Packard Company “hp iPAQ™ H4150 Pocket PC with integrated wireless LAN 802.11b & Bluetooth (FA174A).“ URL: http://h50025.www5.hp.com/hpcom/au_en/11_26_60_2343_FA174A.html (10th Jan. 2004)

Dedo, Douglas. “Security on the Pocket PC.” Windows Mobile. May 2002. URL: http://www.microsoft.com/windowsmobile/resources/whitepapers/security.mspx . (26th Dec. 2003)

Posey, Brien M. “Creating a Solid PDA use policy.” ZDNet Australia: Wireless. 5th May 2003. URL: http://web.zdnet.com.au/techcentre/wireless/tips/story/0,2000050975,20274228,00.htm? . (27th Dec. 2003)

Hayday, Graham. “Revealed: PDA security risks - and what to do about them (part two).” silicom.com. 1st Mar. 2002. URL: http://www.silicon.com/software/security/0,39024655,11031917,00.htm. (27th Dec. 2003)

McMillian, Oba. “PDA Security Policy – Worth Its Weight in Gold.” 20th March 2002. URL: http://www.infosecnews.com/opinion/2002/03/20_02.htm (10th Jan. 2004)

Defence Signals Directorate. “Australia Communications-Electronic Security Instruction (ACSI 33), Government IT Security Manual, Final Draft.” 16th Jan. 2004. URL: http://www.dsd.gov.au/library/acsi33/acsi33_unclassified_draft.pdf (17th Jan. 2004)

Fraser, B. ”Site Security Handbook” IETF RFC 2196. Sept. 1997. URL: http://www.ietf.org/rfc/rfc2196.txt?Number=2196. (10th August 2003)

Orantia, Jenneth. “Handheld Security.” Australian Personal Computer. November 2003 (2003): 128-129.

Caelli, William. Longley, Dennis. Shain, Michael. “Information Security Handbook” London. Macmillian Press Ltd. 1996.

International Organisation for Standardization. “Information technology - Code of practice for information security management” ISO / IEC 17799:2000. 10TH September 2001.

© SANS Institute 2004, Author retains full rights.