HP ProtectTools Windows Mobile

White Paper

Introduction......................................................................................................................................... 2
Risks .................................................................................................................................................. 2
Features.............................................................................................................................................. 3
Password Hashing ...............................................................................................................................4
Password Generation........................................................................................................................... 5
Password Types................................................................................................................................... 5
Strong Alphanumeric Passwords............................................................................................................ 5
Password Lifetime ................................................................................................................................5
Password Input Panel ........................................................................................................................... 6
Memory Erasure .................................................................................................................................. 6
Activesync Validation........................................................................................................................... 6
Event Logging ..................................................................................................................................... 6
Device Locking .................................................................................................................................... 7
Implementation and Use ....................................................................................................................... 7
User Interface.................................................................................................................................. 7
Configuration.................................................................................................................................. 7
Windows Mobile Device Support....................................................................................................... 8
Existing Windows (SE)/HP ProtectTools Environments..................................................................... 8
Configuration Examples.................................................................................................................... 9
Department of Administrative Affairs .............................................................................................. 9
ACME Ltd........................................................................................................................................... 9
For more information......................................................................................................................... 10
Call to action .................................................................................................................................... 10
Introduction

HP ProtectTools Windows Mobile provides enhancements to Windows Mobile primarily in the areas of user authentication, data security and ActiveSync link authentication and device locking. These enhancements were designed originally to meet UK Government requirements, but apply equally in a commercial environment.

Implemented as part of an approved company or departmental security policy, HP ProtectTools Windows Mobile can help achieve BS7799 certification.

HP ProtectTools Windows Mobile fits with the highly desirable HP COTS (Commercial Off the Shelf) products philosophy, which is to provide off the shelf enhancements to standard Microsoft products.

Risks

Windows Mobile devices are highly desirable, this and their small size make them vulnerable to theft and loss.

These devices are designed for ease of use not security. Due to weak password systems, unsecured ActiveSync connections and inclusion of debugging tools for these devices data can be extracted easily. Even the data we ordinarily carry around on these devices could be sensitive, contacts lists could be very valuable to a competitor, email may contain attachments with all kinds of data. Add to this basic data the files that are synchronized; Word documents, Excel spreadsheets, even Access databases and the Windows Mobile device can hold a considerable amount of data.

Theft & Loss

Weak Passwords

Easy Data Access

User Configuration

The password systems in Windows Mobile are optional, even when it is enabled the password hashing algorithm is weak and users are allowed to select their own passwords. When they have the option users will tend to select poor passwords, dictionary words or nouns. As there are no limits in Windows Mobile on the number of password attempts an attacker has a large opportunity to guess the password.

As they are relatively inexpensive Windows Mobile devices are often bought by or for individuals. Frequently it is possible for these users to connect their personal devices to corporate networks, effectively extending the corporate network out to their mobile devices. Even when a user has an approved device there are further problems if they connect this device to their home PC, synchronising corporate data and exposing it to the Internet through Internet Service Provider connections.

Windows Mobile devices are usually provided with debugging and recovery mechanisms that may allow access to the memory. In the iPAQ this mechanism has been termed “Parrot Mode” as on early versions of the device a picture of a parrot was displayed on screen while the device was in the debugging mode. An attacker could use this memory access to view or alter data stored on the device.
Features

HP ProtectTools Windows Mobile offers several features not available in a standard Windows Mobile environment. These include:

- Choice of Password Hashing Algorithms
- Password Generation
- Password Lifetime
- Strong Alphanumeric Passwords
- Password Input Panel
- Secure erasure of memory on failed access attempts
- ActiveSync Validation
- Device Locking
- Event Logging

System managers can choose to install either the entire set of functions or any combination of them, depending on their specific requirements. They may, for example, choose to install Password Hashing but not Generation; alternatively other systems may require only Device Locking.

These enhancements are available as a commodity priced, Commercial Off The Shelf (COTS) product layered on, and as enhancements to Microsoft Windows Mobile security.
Password Hashing

In Windows Mobile, the user password is stored locally on the device in an encoded, hashed\(^1\) form. As the user logs on, the password entered is hashed before it is compared to the stored hash.

The problem with standard Windows Mobile is that the password hashing is compromised, as the algorithm is known. There are various tools freely available on the Internet which allow users to break into computer systems using:

- Password dumping
- Password sniffing
- Dictionary attacks
- Brute-force attacks

Password dumping involves copying all the user account details with password hashes from the machine under attack. This requires physical access to the machine under attack, normally privileges to a computer system are required. However the debugging tools, built into Windows Mobile devices, mean that this is a much greater risk.

Sniffing a network involves reading the network packets as they pass along the wire and collecting the usernames and hashed passwords as they appear. Software is freely available which, when run on an ordinary PC with a network card, will capture network packets. Password sniffing is a limited risk with Windows Mobile as the authentication takes place locally and hence the password hash is not travelling over the network.

Once the usernames and hashed passwords have been collected by dumping or sniffing they can be “cracked” using dictionary or brute-force attacks off-line.

Hashing algorithms are by nature irreversible: the password is encoded into the hash but the hash cannot be decoded to the password. However, if there is sufficient computing power available it is possible to encode all possible passwords and check the hash result against the hash recovered until the correct password is found. This is a brute-force attack. A more subtle attack involves hashing dictionary words until the correct hash is found. Many passwords in common use can be found in a dictionary.

HP ProtectTools Windows Mobile provides replacement password hashing algorithms which are tightly integrated with the Windows Mobile operating system providing a replacement logon authentication system. These algorithms can be seeded, allowing installations for different organisations to be unique. These seed values can be up to 160 bits so can provide up to \(2^{160}\) combinations. Anyone attacking the systems needs to know not just the algorithm but the seed value as well.

The standard algorithm is HMAC, as defined in rfc2104 and rfc2404, providing a seeded implementation based on SHA-1 (FIPS 180-1)

Algorithms are also available which are approved by both UK Government and NATO, and recommended by SECAN.

---

\(^1\) To hash is to map the password to a numerical value by means of a process known as a hashing function; this function uses a mathematical algorithm.
Password Generation

When users are allowed to choose their own passwords they will pick weak or guessable passwords. HP ProtectTools Windows Mobile protects against this by providing the option to enforce generated passwords.

The password change mechanism available at logon or through the Secure Attention Sequence (SAS) Dialog has been modified and integrated with the standard GINA (Graphical Identification and Authentication DLL). Users are presented with three passwords to select from, these passwords are generated using FIPS-181 compliant Automated Password Generator (APG) in the form of random letter or word passwords. Random word passwords are generated in a form where it should be possible to pronounce them making them generally more easily remembered than simple random letter combinations.

Also available are UK Government and NATO approved algorithms used to generate passwords from 8 to 15 characters passwords of the form CVCCVCCVCNN. This format of Consonants Vowels and Numbers is designed to produce pronounceable passwords.

Password Types

A number of Mobile devices incorporate fingerprint recognition hardware for user authentication when accessing the device. These features have been included in HP ProtectTools Windows Mobile and can be combined with the entry of a Password.

For commercial applications the fingerprint can be combined with the password or PIN number so that authentication requires two forms of credentials, for example Fingerprint and PIN number or a choice of credentials, for example fingerprint or PIN number.

For government applications, a Password or PIN number must be used for authentication and may also be combined with a fingerprint for additional security.

Strong Alphanumeric Passwords

This feature has been added to decrease the vulnerability of passwords used by users, in the instance where Password Generation has not been installed. Strong Alphanumeric Passwords allow administrators to specify the minimum number of alphabetic characters, digits and punctuation characters that are required in user supplied passwords.

Password Lifetime

The Password Lifetime feature allows an expiry time to be set on users passwords. The user will be prompted to change their password on the first logon following the expire of the lifetime. This feature ensures that users change their passwords on a regular basis, further reducing the password vulnerability.
Password Input Panel

An additional Input Panel has been included in HP ProtectTools Windows Mobile, specifically for the entering of passwords. The input panel has larger keys than the standard input panel, and they are arranged from a to z instead of the standard qwerty format, making it easier to use.

Memory Erasure

Whilst Windows Mobile devices are relatively inexpensive the value of the data contained on them is very difficult to quantify. Even a contact list could be very valuable to a competitor. In order to avoid this data falling into the wrong hands HP ProtectTools Windows Mobile can be configured to securely erase the memory contents after a number of failed password attempts. If the device is lost or stolen then after a small number of password guesses the device’s memory is erased and it resets to factory settings. Should the user have inadvertently erased the device it can simply be restored and resynchronised and any data lost will be limited to data entered since the last resynchronisation. Authorisation to perform the restore can be limited to only selected users, it can be controlled centrally to grant individuals access only when required.

This memory erasure has been approved to protect data with a UK government protective marking of Restricted.

Activesync Validation

Windows Mobile devices are extremely portable items and can be easily connected to corporate computer systems. It is very straightforward to drop the device into a cradle or even use Infrared to synchronise data from host PCs as a “guest” Windows Mobile device. Users can bring their personal Windows Mobile devices into the office and connect them to the corporate network. As data can be transferred to the Windows Mobile device it effectively becomes an extension of the corporate network. The same Windows Mobile device can be connected to another PC perhaps at the user’s home and data synchronised with an Internet connected system.

HP ProtectTools Windows Mobile provides mechanisms for the host PC to validate that the connected Windows Mobile is an authorised device and also to allow the Windows Mobile device to validate that the connected host PC is authorised.

The host PC challenges the Windows Mobile with a Nonce\(^2\), the Windows Mobile device must return the correct response to this challenge, a shared secret hashed with the challenge. If there is no response within a timeout period the link is terminated. The Windows Mobile device also challenges the host PC with a Nonce and waits for a response and after a timeout period the Windows Mobile device terminates the link and powers off.

The shared secret can be chosen for individual Workstation/Windows Mobile pairs but it would normally be chosen for a group of users perhaps a department or maybe a whole organisation.

Event Logging

The Event Logging feature of HP ProtectTools Windows Mobile has been added to provide tracing and auditing of specific Windows Mobile events. An Administrator can configure which events are logged, these include standard Windows Mobile Events and additional HP ProtectTools Windows Mobile events which are: Logons, Password Changes and Device Lock.

\(^2\) A Nonce is a randomly generated value used to defeat “playback” attacks in communication Protocols.
Device Locking

Windows Mobile devices are designed to be useful, with numerous communication and storage options. These communication and storage features provide the ability for a user to share information stored on the device easily, however this can be a risk, if the information held on the device is sensitive.

HP ProtectTools Windows Mobile controls the access to all devices based on the configuration. It can even control the type of devices that are allowed to connect. For example, a user may be permitted to connect a GPS module via the CF Slot whilst excluding any mass storage device or Bluetooth module. These permissions apply when the device is present as the user logs in or if the device is hot plugged into the logged on running system.

A configuration utility is provided which allows devices to be moved to the permitted devices “White List”. Devices not moved to the “White List” will not be available to the user.

Devices that can be controlled include Compact Flash, SD/MMC, Infrared, Bluetooth and removable devices.

Implementation and Use

Minimum user impact has been achieved by making only minimal changes to the standard user interface. These changes have been tightly integrated with the Windows Mobile Operating System. The enhancements are made through standard interfaces making the system suitable for a wide range of Windows Mobile devices and Operating System versions.

User Interface

HP ProtectTools Windows Mobile is designed to have a very low impact on end users; changes to the Windows Mobile Operating System and GUI are limited to:

- A revised logon screen, showing a replaceable bitmap which defaults to the Windows Mobile (SE) splash screen
- A revised change password screen, again showing a replaceable bitmap, with optional password generation

Configuration

Each HP ProtectTools Windows Mobile implementation is unique; this is achieved using seed values for the password hashing algorithms when the installation is built.

The system administrator builds the installation kit once, tailoring it to suit the organisation’s specific security requirements. The installation kit generated by this process is then distributed and installed on Windows Mobile and ActiveSync workstations within the domain, thus ensuring that the same seed values have been used for each installation.
The installation can optionally be configured for:

- Password Hashing – With unique installer generated seed values and device unique salting
- Generated passwords – Where password generation is selected users are given the choice of three generated passwords when changing their password.
- Number of failed password attempts before the memory is erased
- ActiveSync link protection, with shared secret
- Installation of secure bootloaders
- Device Locking
- Event Logging
- Password Lifetime
- Password Complexity

Windows Mobile Device Support

HP ProtectTools Windows Mobile has been tested on all iPAQ handhelds available as of October 2005.

HP ProtectTools Windows Mobile is designed to support generic Windows Mobile devices, however there are significant variations in the hardware from different manufacturers at present and unfortunately HP cannot offer advice regarding other manufacturer’s equipment. For use on other Windows Mobile devices customers should assure themselves of the compatibility of these devices with HP ProtectTools Windows Mobile.

Existing Windows (SE)/HP ProtectTools Environments

HP and Microsoft recognise the investment already made by customers in Windows (SE)/HP ProtectTools. To protect this investment and to make the implementation of the Windows Mobile environment as integrated as possible the same seed values and algorithms should be used for both the existing Windows (SE)/HP ProtectTools environments and HP ProtectTools Windows Mobile environments.
Configuration Examples

The following examples use fictitious scenarios to illustrate how HP ProtectTools Windows Mobile can be used to meet different security requirements.

Department of Administrative Affairs

A fictitious Government department, "The Department of Administrative Affairs" has previously implemented HP ProtectTools Authentication Services as part of Government security policy. There is now an increasing requirement to allow use of Windows Mobile devices. The IT department needs to satisfy this user demand whilst maintaining the security of the systems.

During a system audit it becomes apparent that some users already have Microsoft ActiveSync installed on their workstations leading to the obvious conclusion that some unapproved Windows Mobile devices are already in use.

Microsoft ActiveSync and the HP ProtectTools Windows Mobile desktop components are installed on all the workstations in the department as part of a planned, automated software update, minimising the effort required. The HP ProtectTools Windows Mobile desktop components act immediately to deny access to the unapproved Windows Mobile devices.

In the roll out design the implementation team decided to use the ActiveSync Protection override to allow users to install the PDA components of HP ProtectTools Windows Mobile on demand. In order to carry out the install an administrator must add the users to a domain security group. When the user has completed the installation they can be removed from the group. As the users need to be added to this group to be allowed to install the software on their Windows Mobile, and hence synchronise data the administrators can now track and authorise Windows Mobile users.

ACME Ltd

The fictitious company, ACME Ltd has offices in several UK cities and a large number of mobile engineers providing services to clients in their own homes. Each engineer will be provided with an iPAQ connected via GPRS to the company network to facilitate task assignment and to allow access to technical information stored centrally.

The management of ACME Ltd are becoming concerned by the threat to the business should someone gain unauthorised access to the network. If confidential company or customer material got into the wrong hands the company could be severely affected. With this in mind, the management ask the IT department to recommend a solution that addresses these issues whilst having minimal impact on the engineers.

The IT department propose implementing HP ProtectTools Windows Mobile throughout the company. The increased security offered by the secure password hashing and the use of generated passwords will prevent a stolen Windows Mobile device from being used to gain access to the network.

With the addition of the Secure Memory Erasure after 3 incorrect password attempts ACME can be certain that any data held on the Windows Mobile device has been removed protecting both customer and company data. In addition, wiping the devices memory will ensure that any software required to access the corporate network, addressing information, etc. has also been removed.

The IT department decide that only a set of authorised issuers should be enabled to install the software set on the Windows Mobile devices, these users are named in Domain Security Group and the devices are returned to these issuers for software installations and updates.
For more information

If you would like to try this software for yourself please visit our Software Depot website (www.software.hp.com) where you can download free 60-day evaluations.

www.hp.com/hps/security/products
HP ProtectTools Security Team, 2004

Call to action

www.hp.com/hps/security/products
email: protecttools@hp.com
Tel: +44 (0) 1925 841881