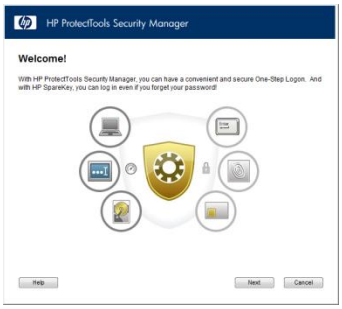
2008 Business Notebook Security Features

Just a few short weeks ago, the Personal Systems Group's Business Notebook GBU announced its new platform lineup for 2008. Among the many enhancements to the commercial notebook platforms were those of several new security features.

In this article we will briefly discuss five new security elements that not only expand PSG's innovative HP ProtectTools security suite, but also add a valuable security tool for end-users who are confronted with lost or forgotten passwords.

It is important to note that these features described within this article are specific to HP Business Notebooks. Information pertaining to HP Business Desktops and its security related security features will be addressed separately at a later date.

Set-Up Wizard for HP ProtectTools



HP began devoting resources towards solving mobile security issues several years ago. Adopting a holistic approach to security, HP introduced HP ProtectTools Security Manager to combine multiple solution areas, helping to ensure not only that PCs are protected but also that the PCs themselves do not become points of vulnerability that can threaten the entire IT infrastructure.

At the heart of HP's security strategy for business notebooks, desktops and workstations is the HP ProtectTools Security Manager, a client console application, operated under a single-screen interface that unifies security capabilities under a common architecture.

For 2008 a Setup Wizard has been added, designed to make user protection setup easy, requiring just a few mouse clicks. The user simply selects the level of security desired along with the means of authentication; the wizard does the rest, a color coded dial-type indicator illustrates the overall level security selected.

Enhanced Pre-Boot Security – (One Step Logon)

Pre-boot has been enhanced by combining security tokens (such as biometrics, smart cards and passwords) and enablement of multi-user access. HP business notebooks offer a range of pre-boot authentication solutions, allowing businesses to provide an additional layer of protection against unauthorized access, including attackers attempting to boot the system from a device other than the primary hard drive.

Enhanced pre-boot security is an integral component of the overall authentication process; user accounts created in Windows are also automatically made available in the pre-boot environment. With multi-factor pre-boot authentication, once the notebook is powered on, the end-user is required to provide a user name, then authenticate using one or more factors (such as a password, a fingerprint swipe or smart card). The notebook then logs the user all the way into Windows, a process known as **One-Step Login**.

HP business notebooks support the following authentication factors at boot-up:

- Power-on password
- Fingerprint reader (integrated on most business notebooks)
- Smart card (Java Card)
- TPM – (Trusted Platform Module)

File Sanitizer for HP ProtectTools

Sensitive information left on the hard drive when a PC is recycled or otherwise disposed of may pose a significant security threat. Simply deleting data does not permanently remove stored information. Files dropped into the Recycle Bin are easy to recover even if the bin has been emptied or if the hard drive has been reformatted, the files would still remain on the drive and may be recovered using one of the many utilities available online.

To help counter this threat, HP has introduced File Sanitizer for HP ProtectTools, which allows the end-user to permanently sanitize individual files, folders and personally identifiable information. Using this tool files can be sanitized manually, or the File Sanitizer can be set to automatically sanitize selected information.

File Sanitizer places an icon on the desktop. Simply drag and drop target files onto the icon; alternatively, target files and folders can also be sanitized automatically with defined schedules. Additional controls also allow the selection of the types of information to delete, such as cookies and temporary files.

Sanitizing is more time-consuming than deletion, with the amount of time taken being in direct relation to file size. As a result, sanitizing should not be used as a replacement for deletion but, rather, as a complement.

File sanitization is based on specifications such as U.S. Department of Defense 5220.22-M

HP SpareKey

Robust security can now be established for business notebooks without the risk of the end-user being locked out if their password happens to be forgotten. HP SpareKey, which is enabled by the Setup Wizard, will prompt the end-user to select three personal questions out of a possible ten, which will be used to permit them to regain immediate access to the system.

By using HP SpareKey and responding correctly to the pre-selected three personal questions an individual can quickly recover his Windows password without the need to contact the IT helpdesk for assistance, thus saving considerable time for the user and helpdesk expense for the business.

Privacy Manager for HP ProtectTools

When it comes to information security, concerns typically revolve around lost or stolen notebooks, or unauthorized access to the network. However, information can easy fall into the wrong hands through normal everyday communications tools such as instant messaging (IM) and email. Privacy Manager for HP ProtectTools can provide protection in these areas.

Privacy Manager for HP ProtectTools helps protect the user from identity theft while online. Access to end-user identity and personally identifiable information are managed while they are browsing, chatting and buying.

Chat

Instant messages are typically transferred in clear language (unencrypted) to remote servers, as are files transferred using instant messaging. As a security precaution, many businesses disable instant messaging in their environments. Yet, while disabling instant messaging does eliminate a security exposure, it also removes the potential benefits of a very useful communications tool.

Used in conjunction with the notebook's integrated fingerprint sensor, however, the Chat feature of Privacy Manager for HP ProtectTools can provide protection for instant messages. Chat allows the request of an identity confirmation from the intended recipient, which requires the recipient to establish their identity using a fingerprint reader.

Chat also adds a secure communications mode where all messaging and files are encrypted before they are transferred. Only the recipient of these messages has the ability to decrypt and view them. If intercepted by an unauthorized person, these messages are effectively unreadable.

Sign

Nearly all of us have received junk email with addresses crafted to appear as if having been sent from friends or associates. This can occur because the header information on a standard email message is unprotected and can be filled with anything.

By using the Sign feature of Privacy Manager for HP ProtectTools an e-mail will be digitally signed with the swipe of a finger. This simple process lets the recipient know that they can be assured that the e-mail message originated from its true address owner.

In closing, this article has provided a very brief overview of the new security features supported on 2008 Business Notebooks, however, there is much more to PSG's commercial security portfolio than can be shared here. To gain a more detailed perspective of this important area we suggest that you please refer to the following resources.

For Additional Information:

Please visit the HP Business PC Security Solutions website - www.hp.com/products/security and view supporting Flash Demos.