HP ProtectTools

Firmware security features in HP Compaq business notebooks

Embedded security overview

A computer system is only as secure as its weakest component. Creating a secure system involves looking at all areas of vulnerability and creating solutions to address each of those areas. HP ProtectTools provides a solution for all points of vulnerability, including:

- Securing the device against unauthorized access
- Securing the network
- Protecting the data

Security solutions installed at the operating system (OS) level can provide a high level of protection against unauthorized access. In order to truly address each of these points of vulnerability, security has to also be built into not only the operating system, but also the hardware and firmware. This is often referred to as embedded security.

Unlike OS level security software, embedded security features can only be provided by the system manufacturer. Knowing this, HP has devoted considerable resources into creating a rich set of embedded security features that work together to enable enhanced security.

This document explores the embedded security features built into HP Compaq business notebooks.

Basics of protection

A typical computer system stores sensitive data on a local hard drive, and may also have access to network resources containing sensitive information. In order to help secure this computer, the following need to happen:

- Protect against unauthorized access -- helps ensure that an unauthorized person does not access the information stored on a local hard drive, and does not use the computer to gain access to network resources.
- Protect local storage -- helps ensure that information cannot be accessed by simply removing the hard drive from a secure computer and inserting it into a non-secure computer.
- Secure devices -- primarily helps ensure that the computer does not boot using a device other than the primary hard drive, and access sensitive information by completely bypassing the operating system authentication.

While these objectives can be achieved at the OS level, HP provides embedded security features that enhance user authentication, data protection and device protection.

Embedded layers of protection

Protecting against unauthorized access – user authentication

User authentication on current operating systems is password based, granting access based on the correct entry of a user name and password.

Externally, software tools can require devices other than passwords for user authentication, such as hardware tokens and biometrics, but the underlying authentication is still password based. This means that the login software installed to support Smart Cards forces a user to authenticate using a Smart Card, but passes that authentication to the operating system using a password. This operating system password is then stored on the system, and can be manipulated to gain unauthorized access. Currently, software tools exist that can reset an operating system password, unlocking the user account.

In order to help protect the computer from such an intrusion, another layer of authentication is added. This authentication is referred to as "pre-boot authentication" and occurs immediately after turning on the computer and before the operating system is allowed to load.

Pre-boot authentication on HP Compaq business notebooks

Pre-boot authentication requiring passwords has been available on computers for some time. HP has now expanded this functionality to allow authentication using other devices. This allows the same device to be used for both pre-boot and operating system level authentication, making the process easy and convenient for authorized users.

HP Compaq business notebooks feature support for three types of authentication at boot-up:

1. Power-on password – the user is required to enter a password on boot.
2. Smart Card authentication – the user is required to present the correct Smart Card and PIN on boot. This feature requires a supported Smart Card such as the HP ProtectTools Java Card or the HP ProtectTools Smart Card.
3. Embedded security chip authentication – On notebooks containing the TPM embedded security chip, the user is required to enter their basic user key pass phrase on boot.

All three of these features provide layers of protection against unauthorized access to the notebook including attacks that take advantage of the ability to boot to a device other than the primary hard drive.

Power-on password authentication overview

Power-on password authentication is a simple but effective implementation of pre-boot security. In their simplest form, power-on passwords require a user to enter a password that gets stored in the system's non-volatile memory. At power-on, the system prompts the user for the stored password and allows the boot process to continue if the correct password is entered.

If an incorrect password is entered three times, no further retries are permitted until the system is powered down and restarted. This feature further protects the system from unauthorized access by forcing the password to be entered manually.

If care is taken to choose a strong password, power-on passwords are an effective way to enhance system security and help protect systems against unauthorized access. The drawback to power-on passwords is that typically a computer can only have one. This means power-on passwords are effective only on single user systems.

Enabling power-on password

Power-on password can be enabled through the BIOS by pressing F10 as the system starts. Enter the BIOS setup and select Power-On Password from the Security menu.

Power-on passwords can also be enabled through the BIOS Configuration for HP ProtectTools module. In the BIOS Configuration for HP ProtectTools utility, select Power-on Password from the Passwords page.

Best Practice
To ensure that the power -on password cannot be easily guessed, passwords should be created using established guidelines, and personal information should never be used as a password.

Smart Card authentication overview

The ability to use a Smart Card for pre-boot authentication adds the security of multifactor authentication to pre-boot security and gives the added convenience of having to remember only the PIN and not a password. Smart Card pre-boot feature requires a supported Smart Card such as the HP ProtectTools Java Card or the HP ProtectTools Smart Card.

Smart Card authentication works by storing the BIOS pre-boot password on the Smart Card. At pre-boot, once the Smart Card is inserted and the correct PIN has been entered, the BIOS password is released, and the boot process then continues.

Since the user has to enter a PIN only the system administrators have the freedom to create extremely strong BIOS passwords, making unauthorized access even more difficult while at the same time making authorized access simpler.

With Smart Card pre-boot authentication, multi-user access becomes possible. While the same power-on password is stored on every Smart Card, each Smart Card is unique, with a unique user name and unique PIN.

Enabling Smart Card pre-boot authentication

Enabling Smart Card pre-boot authentication is a two step process.

1. Smart Card power-on support should be enabled. This can be done either in the BIOS setup by pressing F10 at start up, or through the BIOS Configuration for HP ProtectTools module. To enable, enter BIOS setup and from the Security menu, select and then enable Smart Card Security.
2. The BIOS password should be stored on the Smart Card. This is done through the Smart Card Security for HP ProtectTools module. To complete this step, select the BIOS tab on the Smart Card security module and enable Smart Card security. If the card has not already been initialized, the Smart Card Security for HP ProtectTools module will automatically walk the user through card initialization.

Best Practice
In order to use Smart Card pre-boot security, it is best to create both an administrator card and a user card. The administrator card should be kept in a safe location away from the computer, and the user card should be used for daily access. This will allow user access if the user card is lost or stolen, and the administrator card can be used to create another user card.

TPM embedded security chip pre-boot authentication overview

Embedded security chip pre-boot authentication uses the Trusted Platform Module (TPM) embedded security chip to authenticate the user prior to allowing the system to boot. The BIOS administrator must enable the use of the feature through the BIOS setup by pressing F10 as the system starts or through the BIOS Configuration for HP ProtectTools module. When enabled, the user is prompted for the TPM embedded security chip basic user key password at boot-up and the TPM embedded security chip validates what the user enters. If the authentication succeeds, the BIOS continues to boot the operating system. Otherwise, it may allow several more retries but ultimately shuts down or halts the system when all allowed retries are exhausted.

TPM embedded security chip pre-boot enhances system security in a number of ways:

- Using the same TPM embedded security chip basic user key password to boot the system, as well as to access security features at the application level. This provides the benefits of user authentication in the pre-boot environment without requiring the user to remember an additional password (assuming that the user is using the TPM embedded security chip for other applications).
- Protecting the password with TPM embedded security chip hardware and eliminating the need to save the password in the BIOS flash for comparison. With TPM embedded security chip pre-boot authentication, an encrypted version of the basic user key password is stored, and this password can only be decrypted by the TPM embedded security chip used to encrypt it, effectively tying the password to the system.

Enabling TPM embedded security chip pre-boot user authentication

Similar to Smart Card pre-boot setup, the TPM embedded security chip pre-boot setup is also a two step process.

1. Before the TPM embedded security chip can be used for pre-boot authentication, ownership has to be established by initializing the TPM embedded security chip and creating an owner password and a basic user password. TPM embedded security chip initialization is handled by a wizard invoked automatically during the operating system login.
2. After TPM embedded security chip initialization, the ability to enable the TPM embedded security chip pre-boot authentication is controlled in the BIOS setup, which requires administrator access. This new setting is added as a field in F10 setup under the Embedded Security menu. It is also accessible through the BIOS configuration for HP ProtectTools, again requiring the BIOS administrator password.

Protecting local storage

One way to bypass strong user authentication is to remove the hard drive from a secure system and insert it into an un-secure system. By using the primary hard drive from a secure system as a secondary hard drive on an un-secure system, virtually all data becomes accessible. On an unprotected hard drive that is.

HP Compaq business notebooks enable a hard drive security feature called DriveLock. DriveLock, if enabled, locks the hard drive with a password. At power-on, the user is prompted for the DriveLock password. The hard drive is accessible only after the correct DriveLock password is entered.

DriveLock hard drive protection

DriveLock does not require the user to remember another password. DriveLock integrates with power-on password, and if both are the same, the user is required to enter only a single password in order to unlock the system as well as the hard drive.

The DriveLock password is stored inside the hard drive itself, and cannot be read; it can only be authenticated against. In practical terms, this means that an unauthorized user does not have any means to read the DriveLock password stored on a hard drive. In order to unlock the hard drive, the correct password has to be entered.

A hard drive protected with a drive lock password stays protected even if removed from one system and inserted into another.

DriveLock can be enabled in BIOS setup by selecting DriveLock Passwords from the Security menu. This will prompt the user to create a master password and a user password before enabling DriveLock.

Best Practice
Always select a strong master and user password. Ensure that the master password is different from the user password. In the event that the user password is lost, the master password can be used to access the hard drive and to reset the user password.

TPM Enhanced DriveLock

TPM Enhanced DriveLock adds a level of security to the computer without sacrificing usability for the authorized user.

TPM Enhanced DriveLock ties pre-boot TPM embedded security chip authentication to DriveLock by automatically using a TPM embedded security chip generated 32-character DriveLock user password. This DriveLock user password is a random number and is not stored anywhere.

At pre-boot, once a user has successfully authenticated to the TPM embedded security chip, the 32-character DriveLock password is automatically entered and the boot process continues.

For an authorized user, the login process is completely transparent. However, unauthorized access is now even more difficult due to the randomly generated DriveLock user password.

TPM Enhanced DriveLock protection can be enabled through BIOS setup, in the Security menu. It can also be enabled in the BIOS Configuration for HP ProtectTools module in the Security section.

HP Disk Sanitizer

Information left on a hard drive when a system is recycled or disposed poses a security threat that is often not taken into consideration. Large enterprises tend to use external services that wipe hard drives before they are disposed, but a large number of users have no processes or solutions in place.

This lack of process can result in a significant security threat. In Q1 2005, 200 used hard drives were bought on a popular website. Of the drives that were not defective, 72% contained confidential personal and company information.

To counter this threat, HP has included Disk Sanitizer as a standard BIOS feature in all HP Compaq business notebooks. Disk Sanitizer deliberately removes or destroys data on the notebook primary hard drive using a data removal algorithm documented in the Department of Defense (DOD) 5220.22-M specification. Once executed, destroyed data cannot be easily recovered even with advanced data recovery tools.

How does Disk Sanitizer work?

Disk Sanitizer eliminates data in every sector, every cluster, every byte, and every bit with no damage to the hard drive. Once executed, data cannot be easily recovered even when using advanced tools and techniques (i.e. file slack information, analyze data using Forensic Recovery of Evidence Device, DriveSpy, etc.)

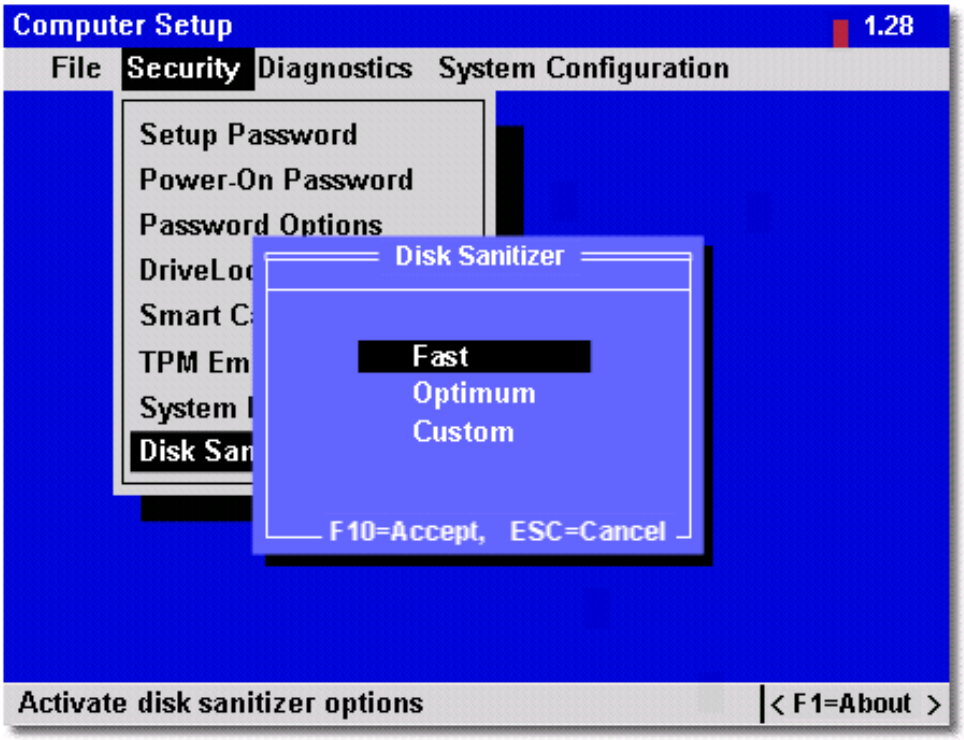
Disk Sanitizer work by writing multiple patterns on every cluster, byte and bit of the hard drive. One Disk Sanitizer pass results in the following data being written to the hard drive. The number of Disk Sanitizer cycles is user configurable.

Single HP Disk Sanitizer cycle	
First pass	'00000000' (all zeros)
Second pass	'11111111' (all ones)
Third pass	random write '1 or 0' & verify
Fourth pass	'00000000' (all zeros)

Enabling Disk Sanitizer

Disk Sanitizer is accessed from the pre-boot setting accessed by pressing the F10 key as the system starts. Disk Sanitizer is located in the Security Menu of the BIOS. Selecting Disk Sanitizer launches the feature. As the system starts, the user is given a choice to run Disk Sanitizer in one of three modes.

- Fast: 1 Cycle
- Optimum: 3 Cycles
- Custom: User configurable cycles



The US Department of Defense internal process require 5 cycles. For most users Fast or Optimum Cycles is sufficient.

The amount of time it takes for Disk Sanitizer to run depends on both the hard drive size and the number of cycles. On a 40 GB hard drive, a single pass can take upto 3 hours and 10 minutes. Due to the long run time, it is strongly recommended that Disk Sanitizer is run with the notebook plugged into an AC outlet.

Securing devices

If a computer is allowed to boot from a device other than the primary hard drive, the user authentication built into the operating system can easily be bypassed. HP Compaq business notebooks provide sophisticated functionality that gives users control over multi-boot capability and boot order, in addition to control over individual ports.

The device security features of the BIOS are split into two categories, controlling boot order and boot devices and enable / disable devices.

Boot options

This feature allows users the ability to control multiboot, which is the user's ability to choose boot order. Boot order can be prioritized among the following devices:

a. hard drive (primary, secondary)
b. diskette drive
c. optical drive
d. USB storage devices (hard drive, diskette drive, optical drive)
e. network

The BIOS can provide finer control over the ability to boot by giving users the ability to enable/disable boot from the following devices:

a. optical device
b. diskette drive
c. network boot

Best Practice
If there is no regular need to boot from devices other than the primary hard drive, then the system should be configured to not allow the user to boot from the optical drive, diskette drive or the network.

Device control

Device control options are intended to give users control over the computer's external ports. Disabling an external port helps ensure that the port isn't used by unauthorized users to transfer sensitive information from the client system or to gain unauthorized access to the client system.

Device disabling options can be accessed in BIOS setup, as well as the BIOS Configuration for HP ProtectTools module, where the following ports can be configured when applicable.

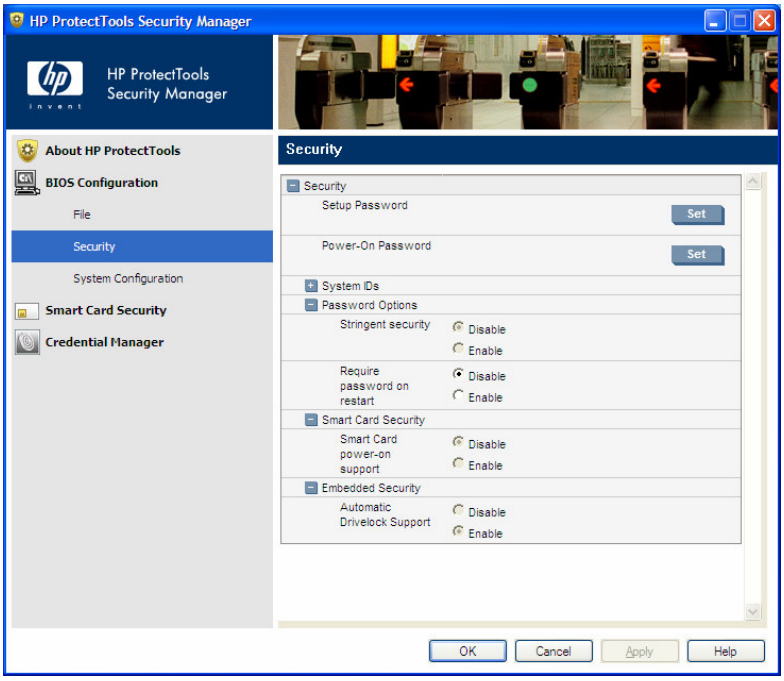
a. serial port
b. infrared port
c. parallel port
d. SD slot
e. Cardbus Slot
f. 1394 Port
g. USB Ports

Accessing BIOS security features from Microsoft Windows

Security features serve their purpose only if used as intended. For this reason, usability is extremely important in order to have a secure system. If computer security is easy to use and does not interfere with a user's ability to be productive, they will not try to bypass it.

Because of this, HP ProtectTools focuses on usability, and it is also the primary focus of the BIOS Configuration for HP ProtectTools module. All security features provided by the BIOS Configuration for HP ProtectTools module are available in the BIOS setup. However, the BIOS configuration module makes these features available directly from within the Microsoft® Windows® environment.

With BIOS Configuration for HP ProtectTools, authorized users can get access to power-on user and administrator password management, and they can configure pre-boot authentication features, such as Smart Card, power-on password and the TPM embedded security chip.



BIOS configuration for HP ProtectTools

With BIOS Configuration for HP ProtectTools, authorized users can:

- Manage power-on user and administrator passwords
- Configure pre-boot authentication features such as Smart Cards, power-on passwords, and DriveLock
- Configure the ability to boot to devices other than the primary hard drive

Table 1 -- BIOS Configuration for HP ProtectTools features and benefits

Feature	Benefit
Works with HP ProtectTools Security Manager	User interface is fully integrated into the HP ProtectTools Security Manager.
Provides access to BIOS security and configuration features from within the operating system	Provides an easier to use alternative to the pre-boot BIOS setup.
Enhanced security feature set that takes advantage of other HP ProtectTools supported security technologies such as Smart Cards and TPM embedded security chips	Provides better protection against unauthorized access to the PC through features that help protect the system from the moment power is turned on. TPM embedded security chip pre-boot authentication requires that users securely authenticate to the chip prior to allowing the system to boot, which helps protect against attacks that exploit the ability to boot to alternative operating system environments. TPM Enhanced DriveLock protects a hard drive from unauthorized access even if removed from a system without requiring the user to remember any additional passwords beyond the TPM embedded security chip user pass phrase. Working with Smart Card Security for HP ProtectTools, pre-boot Smart Card authentication requires users to present their Smart Card prior to allowing the system to boot.

Enabling access to BIOS security configuration from within the HP ProtectTools Security Manager creates an integrated security solution and enables authorized users to control every aspect of security management from a single application with a common user interface. The following table describes the key BIOS security features[1] that become accessible from the HP ProtectTools Security Manager using the BIOS Configuration Module.

Table 2 - Key BIOS security features made accessible by the BIOS Configuration for HP ProtectTools Module

Feature	Description	Benefit
TPM embedded security chip pre-boot authentication	Uses the TPM embedded security chip for user authentication. Users need to input the basic user key pass phrase	Helps protect against unauthorized access to the PC by preventing access to the computer by booting from a device other than the primary hard drive. Provides security benefits similar to a power-on password; however, by allowing the user to use their TPM embedded security chip pass phrase, users are not required to remember an additional password.
TPM Enhanced DriveLock	Requires a user to authenticate to the TPM embedded security chip before a DriveLock protected hard drive can be accessed. A separate DriveLock password is not required.	DriveLock helps protect a hard drive from unauthorized access even if physically removed from a system. Allows very strong, random DriveLock passwords to be automatically set in a way that is completely transparent to the user and does not require the user to remember another password. Ties a hard drive to a specific system with a specific TPM embedded security chip, preventing other systems from accessing the hard drive if it is physically removed from the original system.
Smart Card pre-boot authentication	Requires the user to insert a Smart Card and, optionally, enter a PIN to authenticate prior to an operating system being allowed to load	Protects a system from unauthorized access by requiring the user to insert their Smart Card to boot the system. The same Smart Card used to authenticate the user in the pre-boot environment can also be used with HP ProtectTools to login into Microsoft Windows XP or Windows 2000.

BIOS Configuration for HP ProtectTools is supported on most HP business notebooks, desktops and workstations.

[1] Pre-boot authentication features are available on select platforms. Refer to platform specific specifications for more details.

Security features support

The following table lists the security features mentioned in this white paper, and maps those features on to the supported notebook PCs.

Notebook Model	Power-on password	Pre-boot Smart Card authentication	TPM embedded security chip pre-boot authentication	TPM Enhanced DriveLock	Disk Sanitizer	BIOS Configuration for HP ProtectTools
nc2400	Y	Y	Y	Y	Y	Y
nc4000	Y	N	N/A	N/A	N	N
nc4010	Y	N	Y	Y	N	Y
nc4200	Y	Y	Y	Y	N	Y
nc4400	Y	Y	Y	Y	Y	Y
tc4200	Y	Y	Y	Y	N	Y
tc4400	Y	Y	Y	Y	Y	Y
nc6000	Y	N	Y	Y	N	Y
nx6110/nx6120/ nx6130	Y	Y	N	N	N	Y
nx6115/nx6125	Y	Y	N	N	N	Y
nc6200	Y	Y	Y	Y	N	Y
nx6310/nx6315	Y	Y	N	N	Y	Y
nx6325/nx6320/ nc6320/nc6330	Y	Y	Y	Y	Y	Y
nx7400	Y	Y	N	N	Y	Y
nc6400	Y	Y	Y	Y	Y	Y
nc8000	Y	N	Y	Y	N	Y
nw8000	Y	N	Y	Y	N	Y
nc8200	Y	Y	Y	Y	N	Y
nx8200	Y	Y	Y	Y	N	Y
nw8200	Y	Y	Y	Y	N	Y
nc8400	Y	Y	Y	Y	Y	Y
nw8400	Y	Y	Y	Y	Y	Y
nx9400	Y	Y	Y	Y	Y	Y
nw9400	Y	Y	Y	Y	Y	Y

For more information

1. *HP ProtectTools Security Manager*, Hewlett-Packard Company, 2006
2. *HP ProtectTools Embedded Security – the HP Trusted Computing Implementation*, Hewlett-Packard Company, October 2003.
3. *HP Embedded Security for ProtectTools*, Hewlett-Packard Company, January 2005.
4. *HP ProtectTools Smart Card Security Manager*, Hewlett-Packard Company, July 2003.
5. Pearson, Siani, et al, *Trusted Computing Platforms: TCPA Technology in Context*, Prentice Hall PTR, July 2002.

4AA0-0697ENW, Rev 2, 07/2006