HP ProtectTools:

Authentication technologies and suitability to task

Introduction

The concept of information security is based on ensuring that only authorized users have access to information. The process of verifying a user's identity is simply referred to as user authentication. User authentication is based on three traits that can be uniquely tied to an individual. These are:

1. Knowledge - What the person knows (e.g. password)
2. Possession - What the person has (e.g. USB token, smartcard)
3. Physical characteristic - Who the person is (e.g. Biometrics)

Passwords depend on knowledge that only an authorized person should have. An unauthorized person who gains access to another person's password can also gain access to that person's secure information. However, if user authentication is based on the combination of two or more of the above traits, unauthorized access becomes that much harder.

A number of authentication technologies currently exist that combine the above traits to provide a varying degree of balance between security, usability and cost. HP ProtectTools Security Manager supports a broad range of hardware authentication devices, such as smart cards, USB tokens and biometric fingerprint authentication, among others.

Each authentication device has its strengths and weaknesses, and therefore these devices cannot be ranked in order. The appropriateness of an authentication device depends on it's suitability to task.

The purpose of this white paper is to help identify the authentication devices most appropriate for a given environment by listing the authentication devices currently supported by the HP ProtectTools security manager, and describing their strengths and suitability to task.

Authentication technologies in HP ProtectTools

HP client PCs support a breadth of authentication devices in the Microsoft® Windows® operating system environment, as well as the pre-boot environment. This breadth of support for authentication devices gives customers a range of choices on which authentication technology to deploy.

Authentication support in the Windows environment is provided by HP ProtectTools Security Manager using the Credential Manager for HP ProtectTools add-on module. Credential Manager supports multiple authentication technologies centrally, and has the capability right out of the box to combine the different authentication devices to provide multifactor authentication policies.

The ability to manage multiple authentication technologies centrally from within a single application means that customers can deploy different authentication technologies across the enterprise depending on suitability to task. This also means customers can create complex authentication processes by combining two or more authentication devices for stronger security via multifactor authentication.

It also raises questions for customers on what is the right technology for their environment, and the purpose of this white paper is to help answer those questions.

Credential Manager for HP ProtectTools currently supports the following authentication technologies:

Credential	Description
Password	Requires the user to create a unique passphrase and use it for identification.
Trusted Platform Module (TPM)	A cryptographic security chip embedded in a client PC or other computing device that is able to protect credentials and cryptographic functions.
Smart card	A type of token that, used properly, provides strong user authentication where credentials and cryptographic operations are contained within the smart card chip.
USB token	An external device connected to a USB or other port interface that uses an integrated security chip to protect credentials and sensitive cryptographic functions.
Biometric Fingerprint	Uses fingerprint matching technology to provide a more convenient alternative to passwords and tokens.
Virtual token	Enables virtually any storage device to be used as an authentication credential, including USB flash drives, where a protected file stored on the device is required to authenticate.

Password authentication

Passwords are the most common form of user authentication currently in use. Passwords require little or no unique infrastructure to implement and are useful for deterring casual access. Passwords can also be cost effective and a good level of protection can be achieved by utilizing simple and established policies for the creation of strong passwords.

Many users however do not create strong[1] passwords, and instead use passwords that have a personal significance. While these passwords are easy to remember for the user, they can also potentially be guessed by someone determined to break into the system.

Stronger policies can be enforced by an IT administrator. However, doing so can sacrifice usability, and cause users to employ unsafe practices that can compromise security such as writing down the password in a location where it can be seen by someone else.

Even strong and carefully protected passwords can be compromised via contact with keyboard monitoring viruses or other forms of commonly used network attacks.

To compound the problem, a compromised password can go undetected, which means timely steps cannot be taken to protect the network. This can expose a corporate network to unauthorized access over longer duration and result in greater damage over time.

[1] Weak passwords are referred to as such because they are easy to guess. Weak passwords may consist of sequential numbers or letters, or be derived from a user's personal information such as spouse name or birthday.

Strong passwords on the other hand follow a set of criteria designed to ensure that the password is difficult to guess. These criteria allow users to create passwords that are not derived from personal information, and are therefore difficult to guess for the unauthorized user, yet easy to remember for the authorized user.

If implemented correctly, passwords provide good baseline security. However, in order to protect sensitive data, stronger authentication is required.

Pros	Cons
Broad acceptance	Lost passwords can be costly
No learning curve	Easier to compromise
Universally deployed	Strong (complex)password policies adversely affect usability

TPM embedded security chip authentication

A Trusted Platform Module (TPM) is a cryptographic security chip embedded in a computing client, and can protect digital credentials and perform cryptographic functions. The TPM was conceptualized and designed primarily for device authentication, and while the TPM is not inherently a user authentication device, HP has enabled user authentication using the TPM. HP ProtectTools technology builds on industry standards set by the Trusted Computing Group (TCG) and uses the TPM for strong user authentication in the pre-boot environment as well as with the OS, in addition to the device authentication function.

TPM-enhanced pre-boot user authentication allows an administrator to set a pre-boot user authentication policy utilizing the TPM and the user's TPM basic user key password. When such a policy is enabled, the BIOS will prompt the user for their personalized TPM authentication data when the computer is booted (instead of using a commonly shared BIOS system startup password) and then use the TPM to validate the authentication data. Upon successful authentication, the BIOS will proceed through system startup and ultimately boot to the operating system.

HP also utilizes TPM authentication to enhance Drivelock security, by utilizing the TPM to generate a strong 2048 bit Drivelock password. In addition to improving security, this feature also improves overall system usability as authenticating to the TPM during boot also unlocks Drivelock, effectively linking the hard drive to the platform.

TPMs lend themselves to easy integration with PKI[2] deployments and provide functionality such as email signing and data encryption.

Pros	Cons
Can enable stronger device and user authentication	Lost TPM passwords can be costly
Integrated into clients	User credentials are not portable
Enhanced hardware based security for encrypted data	

Smart card authentication

Smart cards combine two factors, possession and knowledge, and in doing so, provide a higher level of security compared to authentication devices that use only a single factor. In the case of smart cards, authentication requires that the user be in possession of the smart card and know the secret PIN unique to that smart card.

With smart card authentication, unauthorized access can be prevented by keeping the smart card separate from the system. Smart Card Security for HP ProtectTools adds a further layer of protection

[2] Public Key Infrastructure (PKI): Technology that employs encryption to help protect and secure communications and data transfer over the Internet.

by becoming permanently disabled after 5 incorrect PIN entries. This is a standard feature, and it ensures that even with access to both the smart card and the system, the PIN cannot be guessed. Unlike passwords, loss of smart cards can be detected and steps can be taken to prevent access to the system and the network.

Smart cards provide for mobility (stronger, portable user authentication on devices). This allows users to authenticate on multiple systems. This feature is important in environments where users are not tied to any single client. Smart cards can also provide a limited amount of secure, mobile storage, which can be used to securely transport user credentials and keys.

Many smart cards also contain a cryptographic chip/engine which can perform data encryption. Such smart cards can therefore naturally integrate with Public Key Infrastructure (PKI) deployments in a corporation, and provide functionality such email signing and data encryption. Note: In addition to PKI support, HP ProtectTools also provides the means to more securely store user authentication credentials like passwords and therefore does not require additional PKI infrastructure elements.

Pros	Cons
Utilizes two personal traits, possession and knowledge, to provide a higher level of security	Most smart card implementations are vendor unique
Strong cryptographic capabilities, enables PKI integration	Lost smart cards can result in manageability costs
Mobile user authentication	Require deployment of a smart card reader
Intuitive and user friendly. Usage similar to an ATM	General implementation requires expensive PKI infrastructure

USB token authentication

Like smart cards, USB tokens also combine two factors, possession and knowledge, and can therefore provide a higher level of security compared to authentication devices that use only a single factor. USB tokens also require that the user be in possession of the USB token and know the secret PIN unique to that USB token. USB tokens plug into any open USB port and provide an authentication token identical to the one provided by a smart card.

With USB token authentication, unauthorized access can be prevented by keeping the USB token separate from the system. Unlike passwords, loss of USB tokens can be detected and steps can be taken to prevent access to the system and the network.

USB tokens provide for mobility (stronger, portable user authentication on devices). This allows users to authenticate on multiple systems. This feature is important in environments where users are not tied to any single client. USB tokens can also be used to securely transport a limited amount of user credentials and keys.

Many USB tokens have a cryptographic chip/engine which can perform data encryption. These USB tokens can therefore naturally integrate with PKI deployments in a corporation and provide functionality such as email signing and data encryption. Note: In addition to PKI support, HP ProtectTools also provides the means to more securely store user authentication credentials like passwords and therefore does not require additional PKI infrastructure elements.

Pros	Cons
Utilizes two personal traits, possession and knowledge to provide a higher level of security	Most USB token implementations are vendor unique
Lower cost deployment compared to Biometrics and smart cards	Lost USB tokens result in manageability costs
Strong cryptographic capabilities, enables PKI integration.	General implementation requires expensive PKI infrastructure.
Mobile user authentication	

Biometric fingerprint authentication

Biometric devices utilize a physical characteristic in order to authenticate a person. The most commonly available biometric technology currently in use is the biometric fingerprint reader. Biometric fingerprint authentication provides convenient, easy to use authentication that is more secure than passwords alone.

Biometric fingerprint technology continues to improve; however, unlike cryptographic authentication which is extremely precise, Biometric authentication has to be approximated. This inherent attribute of Biometric technology requires a constant tradeoff between false positives and false negatives. Taking into consideration that a person's biometric characteristics are not secrets, as long as the probability of false positives exists, biometric characteristics can be faked, resulting in a security vulnerability. For best results, biometric devices should be used in combination with other authentication technologies.

Biometric technology is also susceptible to unavoidable external factors such as cuts, dry fingers, high humidity, etc. These can result in a high incident of false negatives causing user dissatisfaction.

Enterprises should also take into account that fingerprint authentication is suited primarily for client authentication, and has limited network authentication capabilities[3]. Large scale deployment of fingerprint readers requires some infrastructure considerations and can place limits on functionality and flexibility.

Pros	Cons
Convenient alternative to passwords and tokens	Uses mathematical approximations, requiring tradeoffs between false positives and false negatives
Easy to use	Susceptible to unavoidable external factors (cuts, dryness, humidity)
	A person's biometric characteristics are not secrets, and should be used in combination with other technologies.

[3] While network authentication for biometrics can be implemented, the flexibility would be limited and the solution would require all deployed biometric devices to be from the same manufacturer.

Virtual token authentication

Virtual tokens provide stronger authentication than passwords and are similar in operation to smart cards and USB tokens. Virtual tokens however are not cryptographic devices. The token is generated on the system and can be stored in a user specified location.

Credential Manager for HP ProtectTools allows the creation of Virtual tokens on any storage device connected to the system. These include but are not limited to:

1. SD cards
2. Diskettes
3. Hard drive
4. Registry
5. USB drive keys

Once a token has been created, Credential Manager for HP ProtectTools can use it to authenticate the user. Example: A user can create a virtual token on a USB drive key, and configure Credential Manager for HP ProtectTools to require that virtual token for authentication.

Virtual tokens are a cost effective way for individual users to achieve multi-factor authentication. However, distribution of Virtual tokens cannot be controlled and therefore Virtual tokens should not be used to implement enterprise grade security.

Feature Comparison and suitability to task

The following table summarizes the functionality available with HP ProtectTools Security on HP Client PC's with each of the authentication technologies discussed.

Functionality	Password	TPM	Smart card	USB token	Biometric fingerprint	Virtual token
Requires multiple traits for authentication[4]	No	No	Yes	Yes	No	Yes
Pre-boot Authentication on HP clients[5]	Yes	Yes	Yes	No	No	No
Drivelock protection on HP clients[6]	Yes	Yes	No	No	No	No
Windows Logon via Credential Manager	Yes	Yes	Yes	Yes	Yes	Yes
Can be combined in credential manager to provide multifactor authentication	Yes	Yes	Yes	Yes	Yes	Yes
Single Sign-on authentication access	Yes	Yes	Yes	Yes	Yes	Yes
Identity backup	No	No	Yes	Yes	No	Yes

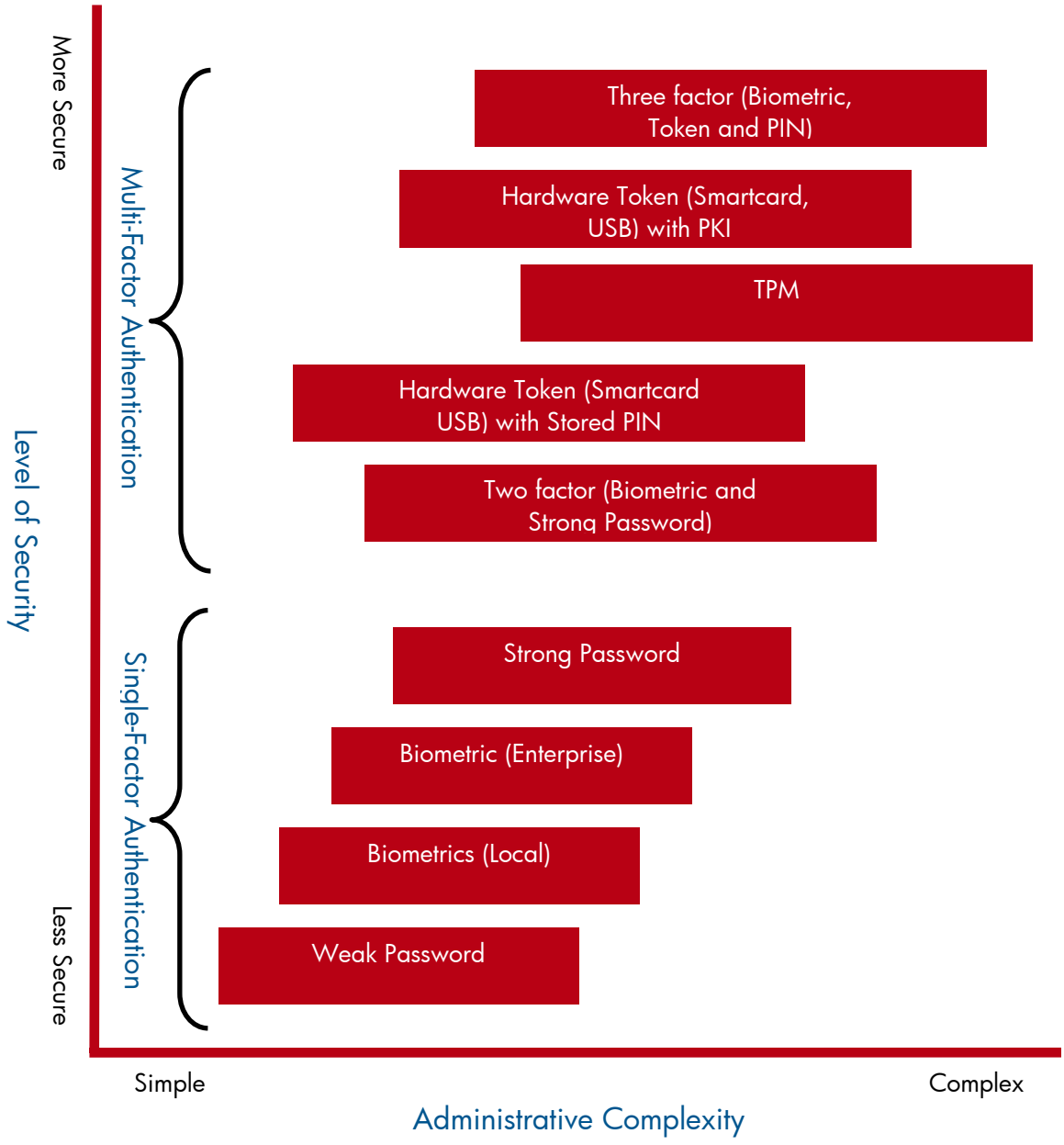
[4] User authentication is based on three traits that can be uniquely tied to an individual. What the person knows, what the person has and who the person is. Utilizing two or more traits to authenticate offers a higher level of security compared to utilizing a single trait.

[5] Pre-boot authentication requires user authentication before the operating system is allowed to load.

[6] Drivelock technology requires a hard drive password to be entered before any data on the hard drive can be read.

Suitability to Task

Each authentication device provides a tradeoff between ease of use, administrative complexity and level of security. The following graph visually represents where these devices fit in the administrative complexity versus level of security spectrum.



Conclusion

All authentication technologies provide a level of protection against unauthorized access. The determining tradeoffs are level of security, cost, and usability.

In making a decision on which authentication technology to deploy, all three factors should be taken into consideration. It is important that the selected technology provide the level of protection appropriate for an environment. It is also important that the selected technology be usable and not result in user dissatisfaction.

For more information

www.hp.com
www.hp.com/products/security

© 2005 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Microsoft and Windows are U.S. registered trademarks of Microsoft Corporation

5983-1956EN, Revision 2, 06/2005