HP PROTECTTOOLS AUTHENTICATION SERVICES

Business white paper

Strong user authentication is the key to securing a computer system, users must be reliably identified to ensure they are granted appropriate access, that audit records are correct and maintain individual accountability.

One of the worries with computer systems is unauthorised access and the difficulties in detecting this. There are now a range of easy to use downloadable utilities that allow individuals with minimal skill and experience to begin attacking Windows systems. These people are often referred to in the press as "Script Kiddies" implying some spotty teenager in their bedroom. However, these same tools have been used by insiders, disgruntled employees and are a menace to system security.

The most significant tools to gain unauthorised access all rely on the same basic attacks.

Password dumping
Password dumping involves copying all the user account details with password hashes from the machine under attack to a disk or tape. This normally requires physical, privileged access to the machine under attack and is a limited risk. It is important to remember that the emergency repair disk will contain these password hashes and must be protected carefully not left on top of the server or in a disk file on the administrator's desk.

Password sniffing
Password sniffing is a much more significant 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.

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.

Dictionary & 'Brute-force' attacks
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 and the hash algorithm is known 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. More complex passwords containing non alphanumeric characters are better but the cracking tools are becoming more sophisticated and can attempt common substitutions such as 5 for 's', @ for 'a' and so on. In a recent test the apparently complex p@ssword;l was cracked in 14 minutes.

The problems with user-selected passwords are well documented; users will select weak passwords, family names, pet names, common passwords, all the kinds of things that are easily guessed or obtained through the attacks described above.

Denying users the use of passwords that may appear in a dictionary provides additional protection against unauthorised access. Providing passwords that have been generated in a memorable form but are not dictionary words is a common solution to this problem, these are sometimes provided as a password book but this book in itself could become a source for a dictionary attack, a real time password generation solution is required.

A significant legal requirement for computer systems is individual accountability; essentially each user must have an individual identity that is only available to them. In standard Windows there is no way of enforcing single access to an identity and features such as "connect as" in network connections allow a different identity to be used to access a resource. These issues can be a significant obstacle to accreditation at IS017799 or BS7799.

Strong passwords

Individual accountability
Management of Local Administrators' Passwords
Multiple Login Denial

The problems don't end once the user has been identified and authenticated. When PC's are shared users can cause a workstation to become locked and unavailable to other users either deliberately or accidentally by allowing the screen saver to run.

Another common security issue with large rollouts of Windows desktops is the control of local account passwords on these workstations. The Local Administrators password is of particular concern and is frequently a common password throughout the network with no tools to change it.

HP ProtectTools Authentication Services provides configurable components designed to mitigate against these risks.

This solution is designed to enhance the authentication by using a customer unique password hashing system, ensuring managed change of administration passwords, providing last successful and unsuccessful login information, enabling multiple login denial and timed auto log-out.

Password Hashing

In Microsoft Windows, the Domain Controller stores passwords in encoded form, and as a logon takes place the password is hashed before it is passed over the network. This is a very

reasonable approach and forms the basis of many authentication systems. There is a problem though in that the password hashing may be compromised if the algorithm becomes known, and this has happened with Windows. There are various tools freely available on the Internet that could allow users to break into Windows systems using the password cracking techniques described earlier.

HP ProtectTools Authentication Services provides replacement password hashing algorithms that are tightly integrated with the Windows operating system modifying both the NTLM and Kerberos security models. The algorithms may also be seeded with up to 64 bits of information, allowing installations for different customers or projects to be unique. Authentication Services can optionally be configured to use password "Salting" whereby password hashing may also include a unique user salt value (the Windows username). The inclusion of this salt value will ensure that two users with the same passwords will have unique password hashes.

The replacement hashing algorithm used by Authentication Service is HMAC as defined in rfc21 04 & rfc2404. This algorithm is based on SHA-1, as defined in FIPS 180-1, with 160 bits of Seeding.

Other algorithms are available which are approved by both UK Government and NATO, and recommended by SECAN.

Password Generation

When users are allowed to choose their own passwords they will pick weak or guessable passwords. HP ProtectTools Authentication Services 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 character passwords of the form CVCCVCCVCNN. This format of Consonants, Vowels and Numbers is designed to produce pronounceable passwords.

A utility is supplied to allow administrators to generate passwords as required for setting up new accounts, resetting user passwords, etc.

Password Preprocessing

In a standard Windows environment, a user can access resources on the network even if they have not been permitted. This is achieved by using the "connect as" facility and a username and password with permissions. A user with access to a resource enters their credentials on another users workstation granting access with the knowledge of the system administrators.

With HP ProtectTools Authentication Services, the password entered at logon or when changing their password, is passed through an obfuscation process before it is passed onto the authentication subsystem. This modified form of the password is then hashed and used in the authentication process. The password known to the user is therefore different from the one stored by the system. The users password is only valid when used through the GINA and, if used elsewhere, will not be recognised, effectively stopping the use of the "connect as" feature and unauthorised password changing mechanisms.

Last Logon Information

Last Logon Information is the first line of detection of unauthorised access attempts. The system presents the user with the date, time and workstation of the last successful logon and unsuccessful attempt along with the number of failed logons, since last logon. If the user notices that this information does not match what they expect, they can alert the system administrator to a potential security breach. This is a feature common to most multi-user operating systems brought to Windows by HP ProtectTools Authentication Services.

The user interface for the last logon information is integrated with the GINA and uses a central repository for the last logon data and provides a central audit trail for successful and failed logon attempts. In Authentication Services last logon information can be stored and maintained by one of two mechanisms. Firstly, the Discoverer Service can store the information in its own repository. The second mechanism uses the Windows Active Directory as the storage location for the last logon information, the "Discoverer Client" becomes a client to the Active Directory on all configured servers. Using the Active Directory as the storage location provides the benefits of data replication amongst

the servers, better integration into the Windows Enterprise infrastructure and allows the use of Active Directory tools to manage and view that data.

Multiple Logon Denial

With a centralised database of currently logged on users, maintained by the Discoverer Server, it is possible to enforce multiple logon denial preventing users from logging on from multiple PCs and helping to maintain individual accountability. If a user gives their passwords to another user who attempts to logon on elsewhere in the domain, a warning is given that they are already logged on in the domain. At this point if multiple logon denial is enabled the second logon will not be allowed.

Forced Logout

In normal operation of Windows systems it's very common for screensavers to be setup and configured to automatically lock the workstations after a period of inactivity. This strategy works well when PCs are assigned to individual users but can cause problems when PCs are shared. In a shared PC environment PCs that are locked without a current user are a waste of resources. A solution to this problem would be to force logout the PC when it has not been used for a period of time.

HP ProtectT ools Authentication Services provides an Auto logout Meta Screensaver that can be configured to automatically log the user out after a predetermined duration of inactivity. This Meta Screensaver allows other normal screensavers to run and lock the workstation.

Local Password Management

During the rollout of a large system it is common for the workstations to be created from an image with all the software installed and configured. Frequently included in this image are the passwords used for the local administrator account and service accounts. What is needed is a mechanism to ensure that each individual workstation has a unique set of local account passwords that are changed on a regular basis.

HP ProtectTools Authentication Services provides a service that is installed on workstations and ensures that local account passwords are changed automatically at regular intervals. The password is created using a hashing algorithm feed with the Username, Workstation Name, Date and a Shared Secret. This process generates a number that is used to drive the password generation system.

A management utility allows the regeneration of these passwords should they be required for maintenance purposes, providing the same information to the management utility will generate the same password.

Conclusion

Unauthorised access to your company's computer systems presents a major threat to security. Individuals with limited skills and experience can download tools which can be used to spearhead all kinds of attacks on your systems. HP ProtectTools Authentication Services can be deployed with minimal impact on users and features such as Password Hashing, Password Generation and Password Preprocessing can be utilised to prevent unauthorised access. If you want to toughen up your security systems HP ProtectTools Authentication Services can provide the help you need.

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

4AA3-4600EEE, Created May 2011