PASSWORD MANAGEMENT

February 2008

TABLE OF CONTENTS

SUMMARY

Password is the most common method for users to authenticate themselves when entering computer systems or websites. It acts as the first line of defence against unauthorised access, and it is therefore critical to maintain the effectiveness of this line of defence by rigorously practising a good password management policy. This paper aims to provide a set of guidelines and best practices for handling and managing passwords.

I. THE CHALLENGES OF PASSWORD MANAGEMENT

With the ever-increasing use of information technology in our daily lives, there are also an ever-increasing number of user accounts and passwords we have to remember and manage. The choice of passwords used for different information systems presents a dilemma. On one hand, an intruder could gain access to ALL the systems if the same password used for accessing these systems is compromised. On the other hand, when different passwords are used for different systems, users may have the tendency to choose easy-to-remember or weak passwords, or even write them down, which would again jeopardise the security of the systems concerned. There is also a higher chance of users forgetting their passwords, increasing the associated user support and operation overheads for password resets.

THE SECURITY THREATS TO PASSWORDS

A password is a convenient and easy method of authentication for users entering a computer system. The system simply requires the user to present something he knows as a proof that he is actually who he claims to be. This is easily implemented, but at the same time the password approach is subject to a number of security threats. The following are common security risks where a legitimate user may lose his or her password:

1. Over the shoulder attack: when a person types in his or her password, someone might be able to observe what is typed and hence steal the password by looking over the person's shoulder, or by indirect monitoring using a camera.

2. Brute-force attack: because a password has a finite length, usually 8 alphanumeric characters, an attacker can use programs that automatically

generate passwords, trying all possible combinations until a valid password is found. With recent advances in computing power, the time needed to execute a successful brute force attack has dropped considerably.

3. Sniffing attack: when a password is sent over a network, it could be captured by network sniffing tools if the network channel is not properly encrypted. In addition, certain malicious tools (such as a keylogger) might be able to capture a user's password when the password is typed in during the authentication process.

4. Login spoofing attack: this is where an attacker sets up a fake login screen that is similar in look-and-feel to the real login screen. When a user logins to the fake screen, his password will be recorded or transmitted to the attacker.

All these attacks, if successful, can help unauthorised users harvest the passwords of legitimate users. Systems using passwords as the only authentication method will be unable to differentiate whether the holder of the password is a valid user or not.

II. TRENDS AND IT GOVERNANCE

SINGLE PASSWORD VS MULTIPLE PASSWORDS

From the user's perspective, memorising one single password is easier than managing multiple passwords, even if the single password is a complicated one. In addition, if only one password is enough to authenticate all systems, there is higher awareness among users in protecting their passwords. However, using a single password for all systems might not be technically feasible, in particular on legacy systems, or across multiple operating system platforms.

For systems that a user accesses only occasionally, it is quite possible for the user to forget a rarely used password. This generates increased workload for support staff who have to reset passwords. In addition, users tend to find ways to bypass difficult controls, such as writing down passwords, or selecting a weak and easy-to-remember password.

For attackers, the single-password approach means that all systems will automatically be compromised once passwords in a weakly protected system are successfully hacked. Therefore, when an organisation decides to use the single-password approach, all systems must be protected at the same level of security.

CONSIDERATIONS FOR USING DIFFERENT PASSWORDS FOR DIFFERENT APPLICATIONS

General Systems

Different information systems will have different security requirements, depending on the functional characteristics and classification of data on each system. As a general rule, authentication mechanisms should be deployed with different levels of sophistication, commensurate with the value of information assets that need to be protected. For instance, an internal application handling classified information requires tight access control, whereas an Internet application for general information searching may allow anonymous logins.

Following this line of thinking, different passwords should be used for different systems with respect to their security requirements and the value of information and assets that need to be protected. If a single password is used for accessing multiple systems, all user accounts should be as secure as the systems with the highest security requirement. If not, intruders may be able to hack into a weakly protected system and in turn gain multiple access to all the other systems that need higher security requirements.

Critical Systems and Resources

For critical systems or applications with classified information, strict access control should be adequate to prevent unauthorised access. Passwords for accessing these critical internal systems should be different from each other with respect to their associated risks.

Internal and External Applications

For external applications, it is often hard to implement tight access control when compared to internal applications, because an organisation might not have complete

control over the external environment. For instance, users may access a company's web applications from a public machine, home PC or other sites where there is no control over security. There is therefore a greater risk of exposing passwords to outsiders. If the same password is used for both internal and external applications, there will definitely be less security protection for internal systems. Once the password for an external application is compromised, intruders may use it as a stepping stone to breach internal applications.

In general, internal and external applications have different levels of significance and importance, and therefore security requirements. A multiple password policy should be implemented. Identical passwords should not be used for accessing both internal and external applications. In addition, the recommended practice is to separate passwords used to access critical applications or privileged accounts from passwords used for general purpose applications. This is a practice that is widely adopted in password guidelines used by a number of government bodies and organisations.

Systems with the Same Security Requirements

To strike a balance between convenience and security, it may be acceptable to use the same password for applications that have the same security requirements, provided that the security policy and usage of the account is properly defined. For instance, you may use the same password to access a timesheet entry system and a leave application system because they are both human resource related systems, managed under a common security policy.

IT GOVERNANCE: GOOD PASSWORD MANAGEMENT POLICIES & USER EDUCATION

It is sometimes difficult to develop a mechanism to enforce the use of different passwords for different applications if the passwords are not managed under a centralised database or system. Therefore, standards on using different passwords for different applications should be clearly stated in security policies. As password is the first line of defence against unauthorised access, it is critical that this line of defence is made effective with a good password management policy.

In addition, users should also be educated and aware of the best practices in choosing and handling passwords. The use of an insecure password may have a direct impact on the security of the whole system. As such, all users need to be responsible for taking appropriate steps to select and secure their passwords.

III. TECHNOLOGY TO FACILITATE PASSWORD MANAGEMENT

Apart from implementing a security policy and guidelines to enforce good password management, some of the technologies highlighted below offer effective and user-friendly password management.

PUBLIC KEY INFRASTRUCTURE

Public Key Infrastructure (PKI) is a technology that uses mathematical algorithms and processes to facilitate secure transactions by providing data confidentiality, data integrity and authentication. PKI makes use of digital certificates to provide proof of identity for the individual. A digital certificate is a kind of digital document that binds a public key to a person for authentication, rather like a personal identity card. A trusted Certificate Authority (CA) creates the certificate and digitally signs it using the CA's private key, thereby authenticating the identity of the requestor. A person can use his or her certificate for authentication with different applications, and the applications then check the user's identity by verifying the digital signature with the issuing CA.

PKI is particularly useful for user authentication in on-line transaction and public applications, because there is no advance pre-registration process required for each application. Users only need to apply for a certificate from a trusted CA to authenticate themselves with various applications.

Deploying PKI requires some worth noting security considerations as follows:

1. The private key must be protected and stored in a safe place, such as in a security token or smart card secured by a PIN.

2. Relevant password restrictions should be imposed on the PIN of the security token / smart card to prevent unauthorised access to the private key inside.

3. There should be proper procedures in place to handle key life-cycle management, issuing and revoking of certificates, storing and retrieving certificates and CRLs (Certificate Revocation Lists).

4. For private key backup, the key must be copied and stored in an encrypted form and protected at a level not lower than that of the original private key.

5. As not all applications support the use of PKI, there may be interoperability issues.

SINGLE SIGN-ON

With the use of Single Sign-On (SSO) technology, users are able to identify themselves with the authentication server only once to access a variety of applications, including both internal and external systems. Users can enjoy the benefit of choosing one password to access multiple applications, instead of memorising many different passwords. However, compromise of one authentication event could result in the compromise of all resources that the user has access rights to.

Implementing SSO requires the following worth noting security considerations:

1. As one single authentication controls access to all resources, it is important that the authentication process is secure enough to protect those resources. This protection should satisfy the requirements of the most critical application. The single authentication process should not be weaker than the original authentication method used by the various applications, otherwise, the result is a downgrade in security level.

2. A second factor of authentication, such as a security token and smart card, can be used to strengthen the authentication process.

3. Relevant password restrictions, such as the minimum password length, the password complexity, the maximum number of trial attempts and the minimum time for renewal, and so on, should be imposed.

4. As the authentication server may become an attractive target for attack, it should be well protected so that intruders cannot access authentication information which could then be used for unauthorised access to all the systems.

5. Auditing and logging functions should be used to facilitate the detection and tracing of suspicious unsuccessful login attempts.

6. Encryption should be used to protect against authentication credentials transmitted across the network.

ONE-TIME-PASSWORD TOKEN

Another technology that may be used to facilitate password management is the one-time-password token. Users authenticate themselves with two unique factors, something they have (the token) and something they know (the PIN). Users do not need to choose or memorise passwords. The token will generate a unique, one-time-use password for each authentication process, based on the PIN and other factors, granting access to protected resources.

The following are some considerations when implementing one-time-password tokens:

1. A token is needed for each user of the authentication process, which implies additional investment.

2. Users must carry the token at all times, and they will not be able to access the system if they lose the token or forget to bring it with them. Unlike software-based access control systems, which only require a password reset, users may not be able to use the system for hours or days if the token is lost.

3. Users should be aware of the physical security of the token and ensure that the token is properly protected at all times.

4. Most of the current one-time-password authentication schemes only authenticate the initial connection. Connections thereafter are assumed to be authenticated, and these connections are susceptible to being hijacked.

5. Security tokens may not support all applications or servers.

IV. BEST PRACTICES

HOW TO CHOOSE A GOOD PASSWORD

Examples of Bad Passwords

The following are examples of badly chosen passwords that can be easily guessed or cracked using password crackers freely available on the Internet.

- "password" - the most easily guessed password

- "administrator" - a login name

- "cisco" - a vendor's name

- "peter chan" - a person's name

- "aaaaaaaa" - repeating the same letter

- "abcdefgh" - consecutive letters

- "23456789" - consecutive numbers

- "qwertyui" - adjacent keys on the keyboard

- "computer" - a dictionary word

- "computer12" - simple variation of a dictionary word

- "c0mput3r" - simple variation of a dictionary word with 'o' substituted by '0' and 'e' substituted by '3'

To avoid falling prey to attackers, there are a number of simple rules that can be followed when creating a password:

DON'Ts

1. Do not use your login name in any form (as-is, reversed, capitalised, doubled, etc).

2. Do not use your first, middle or last name in any form.

3. Do not use your spouse's or child's name.

4. Do not use other information easily obtained about you. This includes ID card numbers, license numbers, telephone numbers, birth dates, the name of the street you live on, and so on.

5. Do not use a password that contains all digits, or all the same letters.

6. Do not use consecutive letters or numbers like "abcdefgh" or "23456789".

7. Do not use adjacent keys on the keyboard like "qwertyui".

8. Do not use a word that can be found in an English or foreign language dictionary.

9. Do not use a word in reverse that can be found in an English or foreign language dictionary.

10. Do not use a well-known abbreviation e.g. HKSAR, HKMA, MTR.

11. Do not use a simple variation of anything described in 1-10 above. Simple variations include appending or prepending digits or symbols, or substituting characters, like 3 for E, $ for S, and 0 for O.

12. Do not reuse recently used passwords.

13. Do not use the same password for everything; have one password for non-critical activities and another for sensitive or critical activities.

DOs

1. Use a password with a mix of at least six mixed-case alphabetic characters, numerals and special characters.

2. Use a password that is difficult to guess but easy for you to remember, so you do not have to write it down.

3. Use a password that you can type quickly, without having to look at the keyboard, thereby preventing passers-by seeing what you are typing.

THINGS TO NOTE WHEN HANDLING PASSWORDS

DON'Ts

1. Do not write down your password, particularly anywhere near your computer or file it in a box file with the word 'password' written on it.

2. Do not tell or give out your passwords to other people, even for a very good reason.

3. Do not display your password on the monitor.

4. Do not send your password unencrypted, especially via email.

5. Avoid using the "remember your password" feature associated with some websites, and disable this feature in your browser software.

6. Do not store your password on any media unless it is protected from unauthorised access (e.g. encrypted with an approved encryption method).

DOs

1. Change your password frequently, at least every 90 days.

2. Change the default or initial password the first time you login.

3. Change your password immediately if you believe that it has been compromised. Once done, notify the system/security administrator for follow up action.

THINGS TO NOTE FOR SYSTEM / SECURITY ADMINISTRATORS

DON'Ts

1. Do not send passwords to users unencrypted especially via email.

2. Do not disclose or reset a password on a user's behalf unless his or her identity can be verified.

3. Do not allow the password file to be readable publicly.

DOs

1. Choose good passwords as initial passwords for accounts.

2. Use different passwords as initial passwords for different accounts.

3. Request users change the initial password immediately upon receiving the new password.

4. Change all system default passwords, including service accounts after installing a new system.

5. Ask users to change their passwords periodically, at least once every 90 days.

System Security Features

The following are desirable security features available in some operating and application systems that can assist in enforcing some of the recommended password selection criteria. It is recommended that such features should be enabled whenever possible.

1. Automatically suspend a user account after a pre-defined number of invalid logon attempts.

2. Restrict a suspended account to only allow reactivation by manual action controlled by the system/security administrator.

3. Prevent users from using passwords shorter than a pre-defined length, or re-using previously used or old passwords.

V. CONCLUSION

While password is the most commonly used method of authenticating users entering computer systems, passwords are frequently targeted by attackers wanting to break into systems. It is critical that this first line of defence against unauthorised access is effective by rigorously practicing good password management policies. Different passwords should be used for different systems with respect to the security requirements and the value of information assets the need to be protected. Make use of other access control mechanisms to facilitate password management and reduce the effort required by users in memorising a large number of passwords. This should be enforced with good security policies and guidelines, supported by user awareness training and education on the best practices in choosing and handling passwords.

In addition, for effective information security management, consideration should also be given in areas including but not limited to physical security, data and application security, network security, and technologies for strengthening security protection, such as firewalls, VPN and SSL.