Information Security Updates

Password Management

Issue 13

Recent Incident

Gamer sentenced for stealing Steam passwords

A former University of Salford student has been given a suspended sentence for stealing online gaming credentials, in a rare conviction under anti-hacking laws.

The University of Salford contacted the police after it received a complaint from a US resident regarding the theft of personal information. The police worked with the academic institution and with the security company McAfee to gather evidence.

(http://www.zdnet.co.uk/news/security-management/2011/05/18/gamer-sentenced-for-stealing-steam-passwords-40092802/)

Industry Practice

Password Requirements of Taylor University

The password requirements of Taylor University are listed out on its website. For instance, new passwords must be at least 8 characters long. New passwords must be different from the previous 24 passwords. New passwords must not contain the username or any part of your full name. New passwords must contain characters from three of the following four categories including lower-case letters (a-z), upper-case letters (A-Z) and numeric digits (0-9), non-alphanumeric characters.

(https://passwords.taylor.edu/pwmanager.aspx)

I. Background

Industry Story

Sony Hack Reveals Password Security is Even Worse than Feared

A million Sony users' password / username IDs and 250,000 Gawker login credentials, each stored in plain text, were exposed via separate hacks.

An analysis by security researcher Troy Hunt revealed that two-thirds of users with accounts at both Sony and Gawker used the same password on both sites. Half the password sample from the Sony hack used only one character type and only one in a hundred passwords used a non-alphanumeric character, much the same as revealed by the earlier Gawker hack. Only 4 per cent of these passwords had three or more character types. In addition, around 36 per cent of the passwords used appeared in a password dictionary, a factor that would leave them wide open to brute-forcing attacks

The data gleaned by Hunt from the Sony hack shows that this is unlikely to be some sort of statistical quirk. On the contrary, by any metric, consumer password security revealed via the Sony hack is dire.

See the article:
(http://www.theregister.co.uk/2011/06/08/password_re_use_survey/)

Password Management Overview

Passwords are secret strings of characters that are used for authenticating users and gaining access to information resources. As the authentication method used by most of the universities' information systems today, an appropriate management framework of passwords plays a significant role in sustaining information security within universities.

The objective of password management solutions is to reduce the risks of passwords being compromised due to inappropriate user behaviours or security threats caused by malicious activities. Typical components encompass processes and technologies that regulate the provision and storage of user account IDs and passwords across the information systems within organisations such as universities.

Reference:
http://csrc.nist.gov/publications/drafts/800-118/draft-sp800-118.pdf
http://www.ogcio.gov.hk/eng/prodev/download/s17.pdf

II. Management

In general, management should ensure that formal policies and procedures have been established to govern the allocation of passwords to authorised personnel and the strong password requirements in accordance with industry standards. Such policies and procedures should be consistently implemented, either through manual processes or automated controls, across all academic / administrative divisions and information systems to enforce general users' compliance with the common practices (please refer to Section III General Users for recommended password requirements). In addition, the implementation can be further enhanced through implementing various password management technologies.

Three common practices are employed by most of the password management solutions today: 1) single sign-on technology; 2) password synchronisation; and 3) local password management.

These practices are designed to minimise the risk of password compromise because of human factors, such as passwords being written down in clear text, passwords being logged when typed at keyboards, or weak passwords created for the ease of use.

Nevertheless, these practices may also cause other security risks to which the management should pay attention during implementation.

Single Sign-On Technology

- **Implementation**

  Single sign-on ("SSO") technology allows a user to be authenticated once and gain access to all information resources that he or she is authorised to use. The user is only required to enter the user account and password to SSO software, which performs authentication to individual resource using unique and strong passwords, and meanwhile keeps this process transparent to the user. The benefit of using SSO is that users are not required to remember multiple strong passwords for individual resources. Instead, the SSO software will enforce it automatically for them.

  There are different possible architectures for SSO technologies. One common example is to have a Kerberos-based authentication service for user authentication and a centralised database or directory service (e.g. Lightweight Directory Access Protocol Server) for the storage of authentication information for individual resources.

- **Security Concern**

  The nature of SSO brings a single point of failure to users at the centralised servers hosting users' authentication credentials of individual resources. The availability of the centralised server affects the availability of all the resources which rely on the SSO services for authentication.

  The security of the centralised server is particularly important since any compromise of the server will lead to the compromise of credentials for many resources. Management should harden the centralised server and encrypt the transmission of authentication credentials to prevent this single point of failure from exploitation.

Related Article

Top Five Most Common Password Management Mistakes that Administrators Make

Management must ensure that their IT security is at the highest level possible, at all times. Privileged passwords that guard the logical access to an organisation's critical information resources are vulnerable items and enterprise password management software has proven to protect these passwords effectively. However, even with this software in place, administrators continue to make common information security mistakes continuously. Some of the most frequent mistakes include allowing weak passwords, connecting to unknown WiFi HotSpots, not performing vulnerability scans or audits on a regular basis and so on.

(http://it.tmcnet.com/enterprise-password-management/articles/181179-top-five-most-common-enterprise-password-management-mistakes.htm)

Related Article

Tougher Passwords Are Easier to Forget and Lead to Productivity Loss, Occasional Misery

In the last year, how many hours have you spent trying to remember a password or a user name? How many minutes did you wait for unconcerned servers to spit out a "reminder" email message? How many times could you not access something because your search for a reminder did not succeed? Have you created new and duplicate accounts because it was easier than getting reminded, or remembering?

(http://campustechnology.com/articles/2006/04/tougher-passwords-are-easier-to-forget-and-lead-to-productivity-loss-occasional-misery.aspx?sc_lang=en)

References:
http://csrc.nist.gov/publications/drafts/800-118/draft-sp800-118.pdf

II. Management (Cont'd)

Password Synchronisation

- **Implementation**

  Password synchronisation is similar to SSO from users' perspective. The user is only required to remember one password to gain access to all the authorised resources.

  However, no centralised directory or authentication server is required for using password synchronisation to perform authentication to individual information resources. Instead, their passwords are automatically synchronised to the same password as the one typed in and remembered by the user.

  Although using password synchronisation does not reduce the number of authentications required to gain access to individual resources, its implementation is easier and less expensive than SSO technologies since no centralised server is required to store authentication credentials.

- **Security Concern**

  There is a major security disadvantage of password synchronisation. Since the passwords to all resources are the same, the compromise of any instance of the password, especially the low-security resource, will lead to the compromise of the entire resources under the same password synchronisation solution. Prior to implementing password synchronisation solutions, management should establish additional controls that enforce users to choose strong passwords.

Local Password Management

- **Implementation**

  Local password management utility allows users to remember only one master password to gain access to the usernames, passwords and account numbers of other information resources. Users usually select an account from a list, giving command to the utility to copy the corresponding password. The password can then be pasted by users onto the authentication field of the target information systems or applications.

  Local password management software can be installed on users' computers. Some software also supports the storage of passwords on a removable media instead of local storage, which introduces an extra layer of protection enforced by the ad-hoc connection of the password storage and the computers. For example, Kaspersky password manager can be installed on mobile device. Once the device is removed, the password database is automatically locked and any trace of the password data is removed from the host machine.

Relevant Guideline

Password Management Guideline from OGCIO

Bureaux/departments shall define a strict password policy that details at least, minimum password length, initial assignment, restricted words and format, password life cycle, and include guidelines on suitable system and user password selection.

Passwords shall not be shared or divulged unless necessary (e.g., helpdesk assistance, shared PC and shared files). The risk of sharing passwords is that it increases the probability of security being compromised. If passwords must be shared, explicit approval from the Departmental IT Security Officer must be obtained. Besides, the shared passwords should be changed promptly when the need no longer exists and should be changed frequently if sharing is required on a regular basis.

(http://www.ogcio.gov.hk/eng/prodev/download/s17.pdf)

Related Article

Six Biggest Rising Threats from Cybercriminals

Many of us use Facebook, LinkedIn and other social networks to connect with friends, family and colleagues, which leaves us vulnerable to a new technique called social network account spoofing. The idea is that a scammer poses as either someone you know or a friend of a friend to get close to you and fool you into revealing personal information. He then uses that information to gain access to your other accounts and eventually steal your identity.

(http://www.pcworld.com/article/228206/six_biggest_rising_threats_from_cybercriminals.html)

References:
http://csrc.nist.gov/publications/drafts/800-118/draft-sp800-118.pdf
http://www.kaspersky.com/kaspersky-password-manager

Related Article

Mobile phone users more vulnerable to phishing

Computer users seem to be getting better at spotting fake websites that are trying to steal their passwords, but when it comes to mobile phones, the deck is most definitely stacked against users.

Researchers at the University of California recently took a look at 100 mobile applications, written for Android and the iPhone, and then considered 15 techniques that scammers could use to write malicious programs that steal the victim's user name and password on websites such as Facebook or Twitter.

(http://news.techworld.com/security/3282953/mobile-phone-users-more-vulnerable-to-phishing/)

Related Article

Making computers hacker-proof

Hackers can now be discouraged from hacking into user accounts despite having access to passwords, which is revealed by a new research from Lebanon. According to the Key-Pattern Analysis ("KPA"), a new approach developed by the American University of Beirut, the password stolen by hackers can become ineffective. K PA is an attempt to scrutinise the speed with which a user taps the keys as well as measuring the gaps between keystrokes, the beat of their typing.

The result can be a biometric profile to record the way individual users type in their password.

(http://www.hindustantimes.com/Making-computers-hacker-proof/Article1-699255.aspx)

II. Management (Cont'd)

- **Security Concern**

  The security of the passwords stored within local password management utility is highly dependent on the security enforced on users' computers or devices because they are installed locally.

  Management is recommended to choose local password management software that have timeout feature to automatically lock the stored passwords from being copied after certain period, such as five minutes. The buffer (used for copy and paste passwords) should also be cleared automatically by the software after the password is pasted onto the authentication fields by users.

III. General Users

Common Practices to be Followed by General Users

- **Use Strong Passwords**

  From the users' perspective, it is essentially important to develop the awareness on the use of strong and complex passwords. The following is an example of password strength recommended by the Centre of Internet Security ("CIS") for a Windows XP desktop computer:

Password Parameter	Password Strength Requirement
Minimum Password Length	Create a password of minimum 8 characters
Maximum Password Age	Change the password every 90 days in maximum
Password Complexity	Create a password with an uppercase character, a lowercase character, digits and non-alphanumeric characters
Password History	Do not reuse the previous 24 passwords
Force first time password change	Change temporary passwords at the first log-on;

- **Never Write Down Your Passwords**

  Despite the implementation of SSO or password synchronisation, there are still plenty of passwords required to be remembered by the user. However, users should never write down their passwords for the ease of use. This will increase the risk of passwords being compromised, which may result in sensitive information being accessed by unauthorised personnel or even the information systems / networks of universities being attacked.

References:
http://benchmarks.cisecurity.org/tools2/windows/CIS_WindowsXP_Benchmark_v2.01.pdf

III. General Users (Cont'd)

- **Do Not Disclose Your Passwords to Any Third Party**

  Users should be aware that their individual passwords must not be shared with other users to gain access to resources or applications. This is because the original use of password is to facilitate identification and authentication so that relevant resources can only be accessed by authorised individual users based on their identity. Disclosure to third parties not only compromises the confidentiality of passwords but also imposes serious security risks on the information resources affected. Users should change their passwords immediately if there is any evidence

  Nevertheless, there are also industrial best practices and users are advised to:

  - avoid keeping a record (e.g. paper, software file or hand-held device) of passwords, unless this can be stored securely and the method of storing has been approved;
  - not include passwords in any automated log-on process, e.g. stored in a macro or function key;
  - not share individual user passwords;
  - not use the same password for business and non-business purposes; and
  - change passwords whenever there is any indication of possible system or password compromise;

Conclusion

The protection of password-based authentication system requires the commitment of both the management and the general users in universities. Password management solutions are available for centralising the management of passwords to minimise the risk of compromise. Nonetheless, users should also be responsible for the security of their passwords and raise their awareness to password protection on top of operational convenience.