Information Security Thought Paper - Passwords

Introduction

A password is a secret word or phrase that must be used to gain access to something. In the IT environment, it is usually a string of characters that allows a person access to a computer system or service. In 2006, the National Institute of Science and Technology (NIST) published the NIST 800-63 guidelines to provide a standard framework for digital identity and authentication to ensure secure access to a computer system or service. The password policies, standards and guidelines that are widely in use today are based on those guidelines - the Government of BC's security policies and standards, the Open Web Application Security Project (OWASP) and Payment Card Industry Data Security Standard (PCI-DSS) password guidelines.

Password Concerns

Password policies, standards and guidelines based on the NIST 800-63 2006 guidelines, required complex passwords to be created and changed on a regular frequent basis. Given that a user has an average of 90 accounts with passwords to be managed today, NIST found that over time, strict adherence to these requirements invariably led to the following issues:

- Creation of weak passwords due to the difficulty in creating unique complex passwords and the frequent forced password change intervals; and
- Poor password practices.

Research has shown that users predictably tend to use special characters like '@' for 'a' to satisfy the requirement for complexity, and append a numeral at the end of the password to satisfy the requirement for uniqueness and typically increase that numeral at each forced change. Users also tend to use the same password for all accounts or write down passwords on a note that is stuck/placed close to the logon device due to the difficulty in remembering the complex password and the sheer number of passwords to be remembered.

These issues and the increase in successful phishing attacks on users and password data breaches today allow systems/services that are secured by use of passwords alone to be easily compromised.

Recommendations

In recognition of the burden placed on users inadvertantly by those requirements, NIST published an updated version in 2016. The new guidelines are more user-centric and forgo the mandated regular frequent forced password changes and complex passwords. Based on the new guidelines, it is recommended that:

1. The following technical controls and methods be implemented to mitigate all attacks against passwords since tinkering with the password policy alone is not effective:
    - Increase end user device protection;
    - Apply user behaviour analytics;
    - Use robust authentication methods including multi-factor authentication
    - Ensure authentication methods are accessible for users with visual or cognitive challenges;
    - Avoid knowledge-based authentication e.g. use of security questions that are easily discoverable;
    - Use strong user IDs that are secured – use of email addresses as user IDs is not recommended as this information is usually publicly available for attackers to use;

- Make the creation and use complex passwords non-mandatory, and encourage the use of passphrases or long passwords where possible;
- Incorporate a password strength meter in the password creation/change mechanism to help users create strong passwords;
- Check passwords for commonly used passwords, dictionary words, context-based words (e.g. business name, given names, etc.) and repetitive use of characters in sequence (e.g. '11111');
- Exclude hints and reminders for forgotten password during the logon process;
- Remove forced scheduled password expiry – require users to change passwords only when there is suspicion of a compromise, when logging on for the 1st time after account creation, after a password reset by a system administrator/help desk (not including Personal Identification Numbers (PINS) for devices that only the user has access to) or when a device/service comes with a default password; and
- Implement Privilege Account Management (PAM) technologies for monitoring and managing privileged accounts and access.

2. Increase awareness and training on information security techniques for users and system administrators such as:
   - Creation of strong passwords;
   - Never using the corporate account passwords in personal accounts;
   - Not using the same password for several/all accounts;
   - Use of password managers to manage passwords; and
   - Detecting social engineering threats/attacks.

Conclusion:

Password policies, standards and guidelines should be updated to reflect the new NIST 800-63 guidelines published in 2016. Implementation of multi-factor authentication and requiring passwords to be changed only when one of the following situation occurs should alleviate much of the password concerns that exist today:

- When there is suspicion of a compromise;
- When a new account is being logged in for the 1st time;
- After a password reset by a system administrator/help desk; and
- Devices/services come with default passwords.

Resources:

GitHub: https://github.com/OWASP/CheatSheetSeries/blob/master/cheatsheets/Authentication_Cheat_Sheet.md
OWASP ASVS: https://www.owasp.org/index.php/Category:OWASP_Application_Security_Verification_Standard_Project
PCI-DSS: http://pcidsscompliance.net/pci-dss-requirements/how-to-comply-to-requirement-8-of-pci-dss/
NIST 800-63-3: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf
https://spycloud.com/new-nist-guidelines/
https://cdn2.hubspot.net/hubfs/3791228/SpyCloud_Understanding_Latest_NIST_Guidelines.pdf
https://www.ftc.gov/news-events/blogs/techftc/2016/03/time-rethink-mandatory-password-changes
https://www.schneier.com/blog/archives/2014/03/choosing_secure_1.html
https://docs.microsoft.com/en-us/microsoft-365/admin/misc/password-policy-recommendations?view=o365-worldwide
https://rawgit.com/w3c/coga/master/issue-papers/privacy-security.html

Gartner articles:

1. Best Practices for Managing PINS and Passwords (2001) – Article 95546
2. Best Practices for Managing Passwords: Overview (2003) – Article 119076
3. Best Practices for Managing Passwords: Usage Guidelines (2003) – Article 119117
4. Best Practices for Managing Passwords: System Security (2003) – Article 119130
5. Best Practices for Managing Passwords: User Policies Must Balance Risk, Compliance and Usability Needs (2015) – Article G00263956
6. Don't Waste Time and Energy Tinkering with Password Policies; Invest in More Robust Authentication Methods or Other Compensating Controls (2019) – Article G00326733
7. Best Practices and Success Stories for User Behaviour Analytics (2016) – Article G00270142
8. Four Kinds of Password Management (2015) – Article G00292189