Data Security and Privacy – Access and Use

Table of Contents

Introduction **2**

Key points in this document **2**

Controlling access **3**

User permissions *3*

Air-gapping *3*

Encryption *3*

Sending data over email 3

Accessing logging and auditing **4**

Authorization and authentication **4**

Username and password *5*

Preventing user access with stolen credentials 6

Considerations for passwords and password policies *6*

Resources *9*

INTRODUCTION

Appropriate access and use rules are critical to protecting data privacy. These rules determine whether and how data can be accessed by internal and external parties. This includes regulating which staff members should have access to data, which staff have the authority to grant access to the data to others, and the process through which access is granted.

When it comes to access for external parties, there may be situations where sharing your data externally could be beneficial. You'll need a process for reviewing and approving requests to share data, a data sharing agreement, and a process for how to maintain privacy and security while sharing.

KEY POINTS IN THIS DOCUMENT

- Appropriate access and use rules are critical to protecting data privacy.
- Controlling and securing access to data is done by limiting access through user permissions and through the use of encryption algorithms.
    - Highly sensitive data can be "air-gapped", which means using a separate device (such as an external hard drive or a laptop) that is not directly connected to your government's network to store the sensitive information.
    - Encryption is the protection of data using a digital "lock and key" algorithm. There are two commonly used types of encryption algorithms used in data protection: 1) encryption for data "at rest" (i.e. while it is being stored), and 2) encryption for data "in transit" (i.e. while it is being sent over a network).
    - Organizations should discourage sending confidential data as an unencrypted attachment to email.
- Access to data and system resources can be logged. It is critical that logs are audited and reviewed on a regular basis.
- Authentication is the process of verifying the identity of an individual or resource attempting to gain access to the system. Users must provide an authenticator - like a password or a key - that is recognized by the system as a valid form of verification to gain access to the system.
    - There are three types of authenticators: something you know (ex. a password), something you have (ex. a physical token), and something you are (ex. a physical attribute such as fingerprint). The document outlines weaknesses of each.
    - The most common authenticator is a combination of a username and password. Passwords should never be transmitted over an unencrypted network link as this will allow other systems to eavesdrop on the transmission.
    - User access with stolen credentials often goes unnoticed unless advanced techniques are used to audit user logins and interactions. The document describes two ways to monitor
    - A password policy should be developed to help with the strength and success of password authenticators. The document outlines factors to consider in the policy.

CONTROLLING ACCESS

Data is a valuable asset that needs to be protected. When data is stored in an IT system, safeguards need to be in place to:

- prevent unauthorized access to data,
- prevent unauthorized modification of data,
- provide traceability to show when data has been accessed or modified by authorized users of the system.

Controlling and securing access to data is done by limiting access through user permissions, air-gapping, and through the use of encryption algorithms.

User permissions

Your IT staff can use the operating system to limit access to files and folders on a network. Local users can be restricted to specific folders. Systems can be configured to monitor access and modification of data and create logs that can be audited for security purposes.

Air-gapping

When data is highly sensitive, an organization may decide that the risk that data will be exposed to unauthorized users over the network is too high. To manage this, data can be "air-gapped", which means using a separate device (such as an external hard drive or a laptop) that is not directly connected to the organization's network to store the sensitive information. In these cases, it is critical to have physical access controls (such as using a locked cabinet for storage) as well as digital controls (such as user authentication and data encryption), to monitor access to air-gapped machines and to prevent the unauthorized copying of data.

Encryption

Encryption is the protection of data using a digital "lock and key" algorithm. The goal of encryption is to prevent unwanted access to data. Un-encrypted data can be read by anyone who accesses it. Once encrypted, data is transformed into a form that is not understandable. Only an authorized user will have the encryption key required to unlock the data to make it usable. There are two commonly used types of encryption algorithms used in data protection: 1) encryption for data "at rest" (i.e. while it is being stored), and 2) encryption for data "in transit" (i.e. while it is being sent over a network).

- **Encryption for data "at rest":** With storage level encryption, a key management strategy needs to be developed to manage the storage of and access to encryption keys. The loss of an encryption key may lead to data being exposed or render the data permanently inaccessible. It is vital to keep track of encryption keys and to monitor and control access to them. **Encryption for data "in transit":** For data transport over networks, the data should be protected with encryption. Data going to or from a web server will require an SSL certificate. This is used to verify and check the identity of the server as well as encrypting data between the web browser and server. Files should not be transferred using FTP (File Transfer Protocol) as this is not a secure protocol.

Sending data over email

Organizations should discourage sending confidential data as an unencrypted attachment to email. Email is an insecure protocol where messages can be stored and monitored in various network locations. If data must be sent via email, attachments should be encrypted before being sent. The encryption key will need to be shared between the sender and the recipient but should never be sent via email as this defeats the security mechanism. You can talk to your IT staff about how best to implement email encryption for your organization.

ACCESSING LOGGING AND AUDITING

As part of the IT operational security model for your organization, access to data and system resources can be logged. It is critical that logs are audited and reviewed on a regular basis. Factors to consider with access logging are:

- Determine what actions and operations will be logged, and how long the log files should be retained:
    - Over-logging and/or retaining too much log data can be detrimental to your system, as log files can grow very large and lower system performance.
    - Under-logging and/or deleting log data too quickly may allow a security or data breach to go unnoticed.
- Review and audit logs regularly:
    - If a data or system breach is detected, a response is immediately required to prevent further damage.
    - Some systems can set up rule-based automation to notify administrators in the event of specific events (e.g., if an unauthorized user accesses the system).
    - Logs can also indicate unsuccessful outside attacks on the system which can be used to strengthen firmware and access rules.
    - Review and update logging and audit policies routinely in response to new threats.

AUTHORIZATION AND AUTHENTICATION

One of the most significant challenges with any IT system is managing who is permitted access to the system, what resources they are permitted to access, and verifying that the right user is using the log-in credentials. Users can be individuals, or "resources" which are systems or applications that require access to the IT system (e.g., when one database pulls data from another database).

Authentication is the process of verifying the identity of an individual or resource attempting to gain access to the system. The goal is to be able to verify that the user is who they claim to be. IT systems use a variety of authentication mechanisms to verify users.

Users must provide an **authenticator** - like a password or a key - that is recognized by the system as a valid form of verification to gain access to the system. Authenticators come in three forms:

- something you know
- something you have
- something you are

Table 1 below highlights examples of different types of authenticators that can be considered for use in data management systems.

TABLE 1. TYPES OF AUTHENTICATORS AND THEIR WEAKNESSES.

	Something You Know	Something You Have	Something You Are
Example	A password shared between parties	A physical token that you have in your possession, such as a smart card	A physical attribute of the user. This is known as a biometric authenticator: • Retinal (eye) scan • Fingerprint • Voice pattern • Face scan
Weakness	• Can be lost or forgotten • If too simple, they can be guessed or hacked • Once known, it can be used by others	• The token needs to be registered and verified by the IT system • If the token is lost or damaged, the user will not be able to access system • Lost or stolen tokens can be used by unauthorized individuals	• Can be copied • Demographic biasing of face scan systems limits use[1] • Higher number of false positives with current technology level (i.e., two different users being confused or identified as a single user)

Username and password

The most common authenticator is a combination of a username and password. The username has been established on the system by a trusted entity and a password is established between the user and the system. When the user wants to authenticate to the system (request access to resources), the user will present their username and password. The system will check to ensure that the password is correct for the username presented and if it is, grant access to the system.

The strength of a password authenticator is based on the following assumptions:

- The password is not being shared between users.
- The password is not being used in a way where someone else can see it or hear it.
- The password has not been recorded or duplicated so that user credentials can be copied or stolen.

If any of these items are compromised, the security offered by the password is broken.

[1] https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf

When passwords are being transmitted across a network, the proper security measures need to be in place. Passwords should never be transmitted over an unencrypted network link as this will allow other systems to eavesdrop on the transmission.

Preventing user access with stolen credentials

User access with stolen credentials often goes unnoticed unless advanced techniques are used to audit user logins and interactions. In many cases, stolen credentials can be used for a period of time, because they are completely valid. Ongoing security measures should monitor:

- Requests from the same user using different devices and locations:
    - A single user may have multiple devices. But if a user is logging in or accessing data from different geographic locations, or if the same user appears to be using an unverified device or multiple devices at once, a security concern needs to be raised. It is unlikely that a user will be accessing data from different locations or on multiple devices at the same time, so this represents a security concern.
- Time of day:
    - Auditing of access logs should monitor time of day access for suspicious access during non-business hours.

Considerations for passwords and password policies

A password policy should be developed to help with the strength and success of password authenticators. Table 2 below outlines factors that should be considered in a password policy. The policy should guide users to select a password of suitable strength that will not be compromised. It is recommended that you follow the NIST Digital Identity Guidelines[2] and Special Publication 800-63: Digital Identity Guidelines[3] when developing password policies.

TABLE 2. FACTORS TO CONSIDER IN A PASSWORD POLICY.

Factor	Implications
Password construction	Passwords should be checked against: • Passwords included in previous breach corpuses. This works to prevent a system attack known as 'Credential Stuffing' where attackers will test username/password combinations from published data breaches. • Dictionary words. • Repetitive or sequential characters (e.g. 'aaaaaa', '1234abcd'). • Context-specific words, such as the name of the service, the username, and derivatives thereof.
Password length	As the number of characters of a password increases, so does the strength of a password. However, too long of a password can also cause security issues as users

[2] https://pages.nist.gov/800-63-3/

[3] https://pages.nist.gov/800-63-FAQ/

	may be inclined to write the password down in a physical location which introduces a significant security risk. A balance in length needs to be struck between having a password that is strong enough but can be remembered by users. Password strength meters can be incorporated into user applications so that users understand the strength of their chosen password.
Life-time of passwords	Some organizations may choose to have a user change their password on a given time interval. The basis of this is that if the password has been stolen, it can be used to impersonate a user often without their knowledge. If password lifetimes are enforced, then the periodic changing of passwords, will eventually eliminate any access by unauthorized users using stolen credentials. Counter to this, if a password lifetime policy is used, users may cycle through a set of passwords or may result in writing the password down. NIST[4] no longer recommends enforcing password lifetime, as users who know that they will have to change a password at some point in the future tend to choose weaker passwords[5].
Password reuse	Users should be encouraged to use a unique password and not reuse an existing password. Reused passwords are susceptible to credential stuffing attacks (see "password construction" above).

When developing a password policy for the organization, the actions outlined in table 3 should be considered for use and storage of passwords.

TABLE 3. POTENTIAL ACTIONS RELATED TO USE AND STORAGE OF PASSWORDS.

Action	Consideration
Password Input Timeouts	To deter unwanted access attempts, password timeouts should be considered. This will limit the number of times a user can enter a password incorrectly in a given time period. If the number of attempts exceeds a determined threshold, the account will be temporarily locked. All bad attempts will be logged for audit review. By limiting the number of password input attempts coupled with a lock-out period, a system can better withstand an automated attack where an attacker attempts to gain access using a list of known passwords against a specific username. With auditing and notification in place, this provides an opportunity for the IT system administrators to apply remedial actions. Additionally, the true account holder can be notified in the event of repeated failed access attempts.

[4] https://pages.nist.gov/800-63-3/sp800-63b.html#memsecretver

[5] https://pages.nist.gov/800-63-FAQ/#q-b05

Password Storage	Passwords should not be directly stored on a system in a raw form. This creates significant risk in the event of a system compromise as an attacker may have the ability to gain access to an entire password list. Some systems will store passwords using reversible encryption with a master password that allows the password file to be unlocked. The preferred form of security for password storage is called **hashing**. With hashing, a fixed length signature is generated from the password that is being stored. If the signature is compromised, it is not generally possible to determine what the password was that generated the hash. It is not possible to recover a password from a hash secured password store.
Password Managers	The use of a password manager should be encouraged. A password manager is a piece of software that users use to access all of their strong passwords from a single password vault, which is protected with encryption. The vault is controlled by a single strong password known only to the user. While NIST does not explicitly recommend the use of a password manager, it recommends that software systems be compatible with the use of a password manager[6]. When evaluating password managers, products that allow the master password to be recovered should be avoided as this increases the attack surface and can allow the password vault to be compromised potentially through the use of password recovery.
Multi-Factor Authentication	Multi-factor authentication (MFA) is a layered security approach that requires users to present two or more authenticators to verify their identity to the system. Unlike with single authentication systems, if one MFA authenticator is compromised or lost, the security of the system remains intact. While biometrics can form part of a MFA, NIST has identified limitations[7]. A commonly used form of MFA is an ATM bank card + PIN where you need both the PIN code and card to access a bank account. Other options now exist for the use of MFA and are numerous in the marketplace. Many solutions will link with a user's mobile phone to present a one-time use pin code that can be used in combination with a user's password.
Password Recovery	In the event of a lost or forgotten password, the organization will need a password recovery or reset policy to ensure proper authentication of the user requesting the password recovery.

[6] https://pages.nist.gov/800-63-FAQ/#q-b12
[7] https://pages.nist.gov/800-63-FAQ/#q-b13

	For web based applications, an online password recovery system can be linked to a user's verified email account. A user can be sent a time-limited password recovery link that will direct them to a temporary, single-use, secure web-portal for changing their password. Password recovery requests and changes will be logged and reviewed. Any password change to a user account will notify the user via their verified email to confirm the change and advise them to contact their organization's IT department if the user recovery request is not genuine. A recovery password in any form must not be sent via email as this is an insecure communication channel and susceptible to eavesdropping.

Resources

Back to Basics: What's multi-factor authentication - and why should I care?