4. Information Disclosure

This page has been made public for vendors

Question

What is information disclosure? How does confidentiality mitigate this threat?

Answer

Information disclosure enables an attacker to gain valuable information about a system. Therefore, always consider what information you are revealing and whether it can be used by a malicious user.\(^1\)

An information disclosure attack is a circumstance or event whereby an entity gains access to information for which the entity is not authorized. This type of threat consequence can be caused by the following types of threat actions: exposure, interception, inference, and intrusion. Some methods of protecting against this consequence include access control, flow control, and inference control.\(^2\)

Data confidentiality ensures that information is not made available or disclosed to unauthorized individuals, entities, or processes.\(^2\)

Mitigation techniques to prevent information disclosure include:\(^3\)

- Use strong authorization.
- Use strong encryption.
- Secure communication links with protocols that provide message confidentiality.
- Do not store secrets (for example, passwords) in plaintext.

Mitigations for Specific Threats

What is the threat of data flow sniffing?

Summary: Information disclosure types of threats occur when an attacker can read the private data an application is transmitting or storing. In this case, data being sent over the indicated dataflow may be read (sniffed) by an attacker. Depending on the type of data an attacker can read, it may be used to attack other parts of the system or simply be a disclosure of information leading to compliance violations.

Recommendations: Recommended mitigations include:

- Use strong encryption (FIPS 140-2 approved) to protect sensitive and system data
- At the protocol level, use an appropriate encrypted protocol for the data flow (e.g., use HTTPS for web communications)
- At the message level, just the sensitive data may need to be encrypted
- Store keys and other cryptographic materials in a secure manner
- Implement protections against spoofing since a spoofed endpoint can potentially read encrypted data

What is the threat of weak access control for a resource?

Summary: Information disclosure types of threats occur when an attacker can read the private data an application is transmitting or storing. In this case, improper data protection of the data store can allow an attacker to read information not intended for disclosure. Information from a database, file system, configuration file, or other data store may be exposed due to weak controls on the data store itself.
**Recommendations:** Appropriate mitigations depend on the type of data store indicated. In general, mitigations include:

- Authenticate all users of the data store
- Adhere to the principle of least privilege and limit authorized access to the data store
- Keep systems patched to limit known methods for bypassing authorization checks

What is the threat of Authorization Bypass?

**Summary:** The system's authorization functionality does not prevent one user from gaining access to another user's data or records by modifying the key value identifying the data. It is likely that an attacker would have to be an authenticated user in the system. However, the authorization process would not properly check the data access operation to ensure that the authenticated user performing the operation has sufficient entitlements to perform the requested data access, hence bypassing any other authorization checks present in the system.

**Recommendations:** Recommended mitigations include:

- For each and every data access, ensure that the user has sufficient privilege to access the record that is being requested.
- Make sure that the key that is used in the lookup of a specific user's record is not controllable externally by the user or that any tampering can be detected.
- Use encryption in order to make it more difficult to guess other legitimate values of the key or associate a digital signature with the key so that the server can verify that there has been no tampering.

What is the threat of weak authentication scheme?

**Summary:** Weak authentication schemes allow attackers to assume the identity of legitimate users by stealing or otherwise obtaining login credentials. An attacker may employ any number of strategies to obtain credentials. Custom authentication schemes are susceptible to common weaknesses such as weak credential change management, credential equivalence, easily guessable credentials, null credentials, downgrade authentication or a weak credential change management system.

**Recommendations:** The strongest practical authentication technologies and policies should be implemented. Two-factor authentication (tokens, certificates, biometrics, etc.) are preferable whenever possible. Otherwise, strong username/password policy (minimum length, character diversity, obscurity, etc) should be enforced. For scalability and ease of use, strong authentication mechanisms should be integrated with enterprise directory infrastructure.

**References**

1. MSDN: Information Disclosure
2. Internet Security Glossary, Version 2, IETF RFC 4949
3. OWASP: Application Threat Modeling
4. CWE-639: Authorization Bypass Through User-Controlled Key
5. Imperva: Top Ten Database Security Threats