NABA Recommendations on Authentication

Authentication

Authentication is the process of verifying that an individual, entity, or website is whom it claims to be. In the context of web applications, authentication is commonly performed by submitting a username or user ID and one or more items of private information, i.e., password, that only a given user should know.

Specific Recommendation

Alignment with NIST Special Publication's (SP's) – 800-63-3 and 800-63-3b Digital Identity Guidelines

NABA recommends that its members' authentication provisions be in line with NIST SP-800-63-3and SP-800-63-3b. As such, the authentication mechanism employed should be aligned with the criticality of the IT or broadcast system requiring protection.

Additional Considerations

The following are some additional considerations:

- **User ID Provisions**
  All usernames/user IDs should be case-sensitive and they should also be unique. For high-security applications, usernames/user IDs could be assigned instead of being user-defined.

- **Implement Proper Password or Passphrase Strength Controls**
  Password and passphrase "strength" is a key issue associated with best practices in authentication. A "strong" password may be defined as one with a minimum of eight and preferably sixteen characters of length, as enforced by the application. All keyboard characters should be permitted in defining a password. It would be preferable if pass-phrases, versus passwords, were used.

- **Implement a Secure Password Recovery Mechanism**
  Applications should be designed so that a user can gain access to their account in the event they forget their password. In addition, it is important that an application stores passwords using a hardened encryption and that passwords are only transmitted over TLS (Transport Layer Security).

- **Implement Stronger Application Authentication Approaches**
  An authentication factor is a category of evidence that an individual must present to prove they are who they say they are. The three authentication factors are:

  Knowledge Factor – something you know, e.g., password
  Possession Factor – something you have, e.g., mobile phone, tablet, laptop
  Inherence Factor – something you are, e.g., fingerprint, voice print

- **Protect Against Automated Attacks**

  Login throttling is an approach used to prevent an attacker from making too many attempts at guessing a password. It shuts down access to the application after a predetermined maximum number of attempts.

Locking out an account is another effective response to an attacker making multiple access attempts. The number of failed logins should be associated with the account itself.

- **Logging and Monitoring**

  The comprehensive logging and monitoring of all authentication attempts in order to detect attacks and failures on a real-time basis is critically important. Specifically, ensure that all password failures and all account lockouts are logged and thoroughly reviewed.

- **Authentication with No Passwords**

  This situation can occur with third-party applications that wish to connect to a web application, from a mobile device, another website, etc. In such cases. OAuth (Open Authorization) protocol can be used. It uses a token generated by the server and defines how the authorization flow must occur, so that a client, such as a mobile application, can tell the server what user is authorized to use the service.

  OpenID is an HTTP-based protocol that uses identity providers to validate that a user is who they say they are. For non-enterprise environments, like Facebook, etc. OpenID is considered a secure option as well.

  Security Assertion Markup Language (SAML) is XML-based and isn't only initiated by a service provider; it can also be initiated from the identity provider. While OpenID has used predominantly in the consumer market, SAML is intended for enterprise applications.

- **Multi-Factor Authentication (MFA)**

  Employ MFA (multi-factor authentication) for all services, particularly for web services, VPN's (virtual private networks), and especially for privileged accounts and accounts that access critical systems.

Recommendations

NABA recommends that broadcasters evaluate the criticality of the broadcast or IT system under review and align the authentication methodology accordingly.

In addition, it also recommends that its members' authentication provisions be in line with the provisions of both NIST SP-800-63-3 and SP-800-63-3b.

March 2024