ITL BULLETIN FOR JANUARY 2013

MANAGING IDENTITY REQUIREMENTS FOR REMOTE USERS OF INFORMATION SYSTEMS TO PROTECT SYSTEM SECURITY AND INFORMATION PRIVACY

Shirley Radack, Editor
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
U.S. Department of Commerce

The electronic authentication of remote users of information systems is a complex technical challenge for organizations because of the different methods used for remote authentication and the different services involved. Electronic authentication (e-authentication) is the process of establishing confidence in user identities that are electronically presented to an information system. Organizations benefit when users have quick and easy access to the online services that they provide, but the organization's system security and privacy must be protected.

Identity Management Issues

Many different Identity Management Systems (IDMSs) are being used worldwide by identity providers to establish and manage the digital identities of an organization's user community. Users present their identities in the form of digital credentials to authenticate themselves to online services. Different digital identity technologies are deployed by different identity providers, and often provider-specific authentication methods are applied in order for the online service to authenticate the user.

Organizations may operate within a federated community, which accommodates two or more identity providers and their specific authentication solutions. There is no uniform approach to dealing with the federation process, nor is there a uniform method for revoking credentials or their associated attributes in a federated community when there are threats to system security and information privacy. The authentication process is subject to many threats and attacks, including eavesdropping and stealing of usernames and identity credentials; redirection of users to fraudulent websites; man-in-the-middle attacks that intercept and alter authentication messages; and takeover of authenticated sessions.

New Study of Identity Management Issues

The Information Technology Laboratory of the National Institute of Standards and Technology (NIST) recently released a new study that analyzes the different types of digital credentials used in the authentication process. NIST Interagency Report (NISTIR) 7817***, A Credential Reliability and Revocation Model for Federated Identities,*** focuses on identifying requirements for assuring credential reliability and for revoking credentials in a federated community to assure the secure operation of e-authentication systems. NISTIR 7817 was written by Hildegard Ferraiolo of NIST, and is available here.

The study proposes a uniform reliability and revocation service (URRS) as a collaborative effort of all parties of the federated community to address some of the risks associated with the different digital credentials and associated authentication processes of the identity provider.

Recommendations for Improving Credential Reliability and Revocation

NISTIR 7817 recommends the following actions to improve the security of the authentication process. These actions are directed toward the different types of digital credentials that are used and the various parties that are involved in the authentication process:

• In the **two-party model**, the user and an organization (service provider) participate in the authentication event. The service provider also acts as the identity provider. The two-party model is the most frequently used scheme today. The user registers with each service separately and receives a digital credential (usually username and password) after completing the registration process. These credentials are used for subsequent logins to the service providers. In this model, users must remember (or carry) credentials for each service to which they subscribe. The two-party model is generally not considered part of a federation, except in Single Sign-On (SSO) applications.

Recommendation 1: In enterprise SSO solutions, service providers receive an assertion concerning a successful prior authentication event by the enterprise's SSO authentication server. In cases where attackers tamper with the session or compromise the credential, a service provider or application may detect the suspicious activities of the attacker. Then the service provider may prevent further malicious activities targeted to other services by reporting the incident to the enterprise's SSO authentication server and suspending the credential. A reporting and revocation procedure could be beneficial in protecting the enterprise SSO environment in a two-party model.

• A **third-party application** can provide auxiliary services by accessing and using a user's primary service. The third-party application usually requires the username and password in order to access, retrieve, and use the data for its application, giving the third-party application uncontrolled access to the user's primary service.

Recommendation 2: In federated communities, delegation technologies should be considered for third-party applications. With delegation technologies, the primary service provider can issue delegation credentials that are tailored for access to data and/or processes limited to the third-party service, but excluding access rights to other information, such as user settings and controls. Should malicious third-party activities occur, the primary service revokes the delegated credential, while the user credential remains valid. Then the user is protected from Denial of Service (DoS) attacks. Delegations of a service should limit the access of a third-party service to the time that is needed to perform the delegated service.

Recommendation 3: A user or service provider in the federation should have the ability to terminate a delegated service through a delegation revocation procedure.

• The **three-party model** involves a user, an independent identity provider, and a service provider. In general, the user authenticates to the identity provider. After successful authentication, the identity

provider issues an assertion to the service provider indicating that the user has successfully authenticated to the identity provider. The service provider in this case outsources authentication to the identity provider and accepts the authentication assertion of the identity provider.

A service provider accepts a user's access requests to its service based on a successful authentication assertion from the identity provider. As is the case with the two-party model, the service provider needs to protect its resources from unauthorized and malicious access.

Evidence of malicious activity at the service provider is not generally shared with the identity provider. The service provider may be unaware of attacks, or may detect unusual or suspicious account activities and block the user. With the feedback from the affected service provider, the identity provider could suspend the user and prevent further attacks that are targeted at other federated services. Service provider feedback is especially useful and indicative in the federation since the feedback is likely reported by several service providers in the federation, thus providing strong evidence of credential compromise. The user as well as the service is saved time, money, and damage because of the service provider's feedback and the identity provider's suspension actions.

Recommendation 4: In a three-party model, a reporting service for credential revocation/suspension is necessary in order for the service provider to provide feedback to the identity provider on the malicious use of credentials.

• Service providers in the three-party model may be part of a **federated Single Sign-on (SSO)** environment where an identity provider authenticates the user once on behalf of the service providers. All service providers accept the authentication assertions and give the user access to their services without the need for the user to re-authenticate for each service individually. The threats from assertion misuse are limited when identity providers issue short-term assertions for the service provider. If the long-term credential that is used to authenticate to the identity provider has been compromised, an attacker could exploit several service providers.

Recommendation 5: Based on the service provider's audit trail and risk mitigation techniques, the service provider may be able to prevent further malicious activities for other service providers by reporting incidents to the identity provider. A reporting service for credential revocation/suspension, therefore, is beneficial to protecting the federated SSO environment in a three-party model.

• **Privacy-enhancing models** seek to minimize the exposure of user attributes and user information, thereby limiting attribute disclosure to service providers based on the "need-to-know" or "least privileged" security limitations. Privacy-enhancing protocols also limit the identity provider and the service provider in collecting and linking the user's login habits. There is no transaction handle and the user can register and use pseudonyms with each service provider or even stay anonymous with a service provider. Most privacy-enhancing authentication protocols are based on selective disclosure schemes where the user has more control to selectively present some attributes, while hiding other irrelevant attributes in the interaction with the service provider. Other schemes do not disclose an attribute value, but provide a predicate/condition for the service provider.

The identity provider is only minimally involved in the authentication process. The provider signs the user's attributes and issues credentials to the user. The user establishes a login account with the service provider with a pseudonym or by establishing an anonymous login account. On subsequent logins, the user presents the credential with the service without further interaction/authentication with the identity provider.

Recommendation 6: Without the identity provider's involvement in the identity event, the status of a user's credential cannot be determined by the service provider. Where the status of a credential or attribute is important to the federation, a service provider may benefit from a blacklist that is part of a federated revocation mechanism. Blacklists are posted by the identity provider and constructed primarily based on feedback received from users or based on individuals reporting a lost, stolen, or compromised credential.

Recommendation 7: The blacklist mechanism is valuable, but may exclude service provider feedback. Service providers are the primary entities that have firsthand information about malicious account activities. With service provider feedback, malicious incidents could be reported by the service provider to the identity provider. As a result, the identity provider could suspend the credential and protect the user from further attacks. To implement this measure, a trusted third party (the revocation service of the federation) would have to perform the task of credential suspension or revocation.

• **In the four-party authentication model,** an attribute provider supplements the identity provider, service provider, and user. The need for attributes, in addition to user identification and authentication, stems from access control models such as Attribute-Based Access Control (ABAC) and Role-Based Access Control (RBAC), where combinations of attributes (authorization attributes) are evaluated at the access decision point of the service to determine authorized access. The four-party model includes single-source and multisource attribute services.

Recommendation 8: The types of attributes accepted by the federation are usually defined by the service providers of the federation. Attributes can be assigned by the identity provider to its users as either self-asserted or verified attributes. Where attributes serve a critical part in the roles or the functions a user is permitted to perform, attributes should be verified and kept up to date. The identity provider should check the sources for attribute updates, such as changes in the attribute qualification, revocation, and suspension.

Recommendation 9: As a benefit of using the same credential, and taking into account service provider feedback mechanisms, the authentication decisions by the attribute provider and identity provider should be based on the same status of the credential.

Uniform Reliability and Revocation Service (URRS)

In federations, service providers relinquish control of maintaining their own population of user credentials by accepting credentials managed by a third-party identity provider. These third-party credentials serve other service providers within the federation as well. To accept third-party credentials, therefore, involves some risks, even if a trust framework is established. There are threats from other service providers, the third-party identity provider, and the users. Because these credentials are

accepted by many service providers, attacks targeting one service and its users are a threat to all other federated services.

NISTIR 7817 proposes a Uniform Reliability and Revocation Service (URRS) to enable all parties of the federated community, including the user and the service provider, to contribute to and participate in improving the identity management process. Involving all parties will enhance acceptance and trust in the credentials by giving the stakeholders with the most risk (e.g., financial loss) the ability to monitor and report credentials. Participation by the user and service provider will lead to closer examination of credentials and to more trusted credentials. Attackers, on the other hand, will have limited success in repeated misuse of a credential because of the monitoring, reporting, and revocation features of the URRS.

The URRS provides revocation status information to and from identity providers, service providers, attribute providers, and users. The URRS also includes credential revocation services that incorporate some of the identified requirements as a federation service. See NISTIR 7817 for details on the roles of the parties of the federated community in the URRS.

For More Information

For information about publications covering identity management and electronic authentication, as well as other security-related publications, see here.

Information about NIST's information security programs is available from the Computer Security Resource Center here.

ITL Bulletin Publisher:
Elizabeth Lennon, Writer/Editor
Information Technology Laboratory
National Institute of Standards and Technology
Email elizabeth.lennon@nist.gov