August 2004

ITL Bulletin

ADVISING USERS ON INFORMATION TECHNOLOGY

ELECTRONIC AUTHENTICATION: GUIDANCE FOR SELECTING SECURE TECHNIQUES

Shirley Radack, Editor
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology

Our citizens and businesses benefit when they can easily access convenient electronic services provided by federal agencies via the Internet. To assure the security of these electronic services, agencies often need a process for verifying the identity of the remote users of their information systems. The process of electronic authentication (e-authentication) can be securely implemented using currently available techniques that give the information system provider a level of assurance about the user's identity.

In December 2003, the Office of Management and Budget (OMB) issued Memorandum M-04-04, *E-Authentication Guidance for Federal Agencies*, to help federal agencies provide secure electronic services that protect individual privacy. The memorandum advises agencies to review their electronic transactions, determine which transactions require e-authentication, and provide an appropriate level of assurance for those transactions that require authentication. M-04-04 describes four levels of identity assurance and calls on the National Institute of Standards and Technology (NIST) to develop technical guidance for agencies to use for identifying the appropriate authentication technologies that meet their requirements.

Electronic Authentication Guideline

NIST's Information Technology Laboratory recently issued NIST Special Publication (SP) 800-63, *Electronic Authentication Guideline*, by William E. Burr, Donna F. Dodson, and W. Timothy Polk, which provides technical guidance on existing and widely implemented methods for remote authentication. The methods described in the new guideline are based on the application of secret information that is known by the individual to be authenticated and that is used to create identity credentials. This *ITL Bulletin* summarizes the new guideline.

NIST SP 800-63 identifies minimum technical requirements for remotely authenticating the identity of users and provides guidance for each of the four levels of authentication that OMB defines in M-04-04. Topics covered in the guideline include discussion of the e-authentication process, the use of tokens, identity proofing, authentication protocols, and assertion mechanisms. Definitions of technical terms, references to general and NIST publications, and specific information about the use of passwords are also included in the publication.

The e-authentication guide is available in electronic format from the NIST Computer Security Resource Center at http://csrc.nist.gov/publications. When used with other government guidance, recommendations, and publications available on the website, the guide will help organizations to develop a comprehensive approach for determining the appropriate level of e-authentication assurance that they need and to select the best available technical solutions.

The Authentication Process

A user wishing to perform an electronic transaction with an agency should be authenticated through a process that starts with the individual proving identity to a trusted authority and registering a secret for later use. The user, as an *applicant*, registers

Continued on page 2

ITL Bulletins are published by the Information Technology Laboratory (ITL) of the National Institute of Standards and Technology (NIST). Each bulletin presents an in-depth discussion of a single topic of significant interest to the information systems community. **Bulletins are issued on an as-needed basis** and are available from ITL Publications, National Institute of Standards and Technology, 100 Bureau Drive, Stop 8900, Gaithersburg, MD 20899-8900, telephone (301) 975-2832. To be placed on a mailing list to receive future bulletins, send your name, organization, and business address to this office. You will be placed on this mailing list only.

Bulletins issued since June 2003

- ❐ *ASSET: Security Assessment Tool for Federal Agencies*, June 2003
- ❐ *Testing Intrusion Detection Systems*, July 2003
- ❐ *IT Security Metrics*, August 2003
- ❐ *Information Technology Security Awareness, Training, Education, and Certification*, October 2003
- ❐ *Network Security Testing,* November 2003
- ❐ *Security Considerations in the Information System Development Life Cycle*, December 2003
- ❐ *Computer Security Incidents: Assessing, Managing, and Controlling the Risks*, January 2004
- ❐ *Federal Information Processing Standard (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems*, March 2004
- ❐ *Selecting Information Technology Security Products*, April 2004
- ❐ *Guide for the Security Certification and Accreditation of Federal Information Systems*, May 2004
- ❐ *Information Technology Security Services: How to Select, Implement, and Manage*, June 2004
- ❐ *Guide for Mapping Types of Information and Information Systems to Security Categories*, July 2004

with a *Registration Authority (RA).* The applicant undergoes *identity proofing* by the RA and, if the applicant's identity is verified, the RA requests that a *Credentials Service Provider (CSP)* issue *digital credentials,* binding a *token* (a secret) to the identity. The applicant becomes a *subscriber* of the CSP and is a *claimant* to a *verifier* when authenticating. Authentication that the claimant is a subscriber is accomplished by proving to the verifier that the claimant controls the token registered to the subscriber. The verifier may be a *relying party* (typically a government website), or the verifier may be a separate entity that provides *assertions* to the relying party about the identity or other attributes of the subscriber. Authentication of the agency server or the verifier to the user is accomplished by proving that the server also controls its own token.

In electronic commerce, these functions may be consolidated and partitioned in different ways. For example, a bank might perform the RA, CSP, and Verifier functions for its customers (subscribers). A bank customer authenticating to an agency information system may be referred to the bank for authentication, using the password created for financial transactions. The institution then may issue assertions about the subscriber's identity to the agency.

Who we are

The Information Technology Laboratory (ITL) is a major research component of the National Institute of Standards and Technology (NIST) of the Technology Administration, U.S. Department of Commerce. We develop tests and measurement methods, reference data, proof-of-concept implementations, and technical analyses that help to advance the development and use of new information technology. We seek to overcome barriers to the efficient use of information technology, and to make systems more interoperable, easily usable, scalable, and secure than they are today. Our website is http://www.itl.nist.gov/.

In some cases, an employer might register its employees with an independent public key Certification Authority (CA) that issues credentials (public key certificates) directly to the employee-subscribers. Or an employer might operate as both the RA and CA. NIST SP 800-63 covers these examples, as well as additional alternatives, in which the basic elements of authentication may be combined in different ways to respond to specific needs.

Authentication Factors

Authentication systems are frequently described by the authentication factors that they incorporate. The three factors often considered as the cornerstone of authentication are:

❑ Something you know (for example, a password);

❑ Something you have (for example, an ID badge or a cryptographic key); and

❑ Something you are (for example, a voice print or other biometric measurement).

Authentication systems that incorporate all three factors are stronger than systems that incorporate only one or two of the factors. The system may be implemented so that multiple factors are presented to the verifier, or some factors may be used to protect a secret that will be presented to the verifier. For example, a hardware device that holds a cryptographic key might be activated by a password or the hardware device might use a biometric representation to activate the key. This type of device provides two-factor authentication, although the actual authentication protocol between the verifier and the claimant only proves possession of the key.

Determining Assurance Levels

OMB advises that agencies follow a five-step process in determining the appropriate assurance level for their applications:

❑ Conduct a risk assessment for e-authentication of the system. The risk analysis measures the severity of potential harm and the likelihood of occurrence of adverse impacts to the system if there is an error in identity authentication. Guidance for conducting a risk analysis is available in OBM Circular A-130 and in NIST SP 800-30, *Risk Management Guide for Information Technology Systems*.

❑ Map identified risks to the applicable assurance level. After all of the risks have been identified, agencies should tie the potential impact of the risks to the proper level of authentication to be used.

❑ Select technology based on e-authentication technical guidance. OMB advises that agencies refer to the technical guidance issued by NIST.

❑ Validate that the implemented system has achieved the required assurance level. A final validation is needed to confirm that the system achieves the required level of assurance, and that the selected authentication process satisfies requirements.

❑ Periodically reassess the system to determine technology refresh requirements. Reassessments ensure that the authentication requirements continue to be valid as technology and requirements change.

The required level of authentication assurance should be determined, based on the potential impacts of an authentication error on:

❑ Inconvenience, distress, or damage to standing or reputation;

❑ Financial loss or agency liability;

❑ Harm to agency programs or public interests;

❑ Unauthorized release of sensitive information;

❑ Personal safety; and/or

❑ Civil or criminal violations.

OMB defines four levels of authentication assurance for electronic transactions requiring assurance and identifies the criteria for determining the level of e-authentication assurance required for specific applications and transactions, based on the risks and their likelihood of occurrence. As the consequences of an authentication error and misuse of credentials become more serious, the required level of assurance increases.

Level 1 is the lowest assurance, and Level 4 is the highest. The levels are based on the degree of confidence needed in the process used to establish identity and in the proper use of the established credentials.

- Level 1 - Little or no confidence in the asserted identity's validity.
- Level 2 - Some confidence in the asserted identity's validity.
- Level 3 - High confidence in the asserted identity's validity.
- Level 4 - Very high confidence in the asserted identity's validity.

Determining Technical Requirements

After determining the assurance level needed for each of the areas of potential impact, agencies should determine the required overall assurance level. The NIST guidance defines technical requirements for each of the four levels of assurance in the following areas:

- Tokens (typically a cryptographic key or password) for proving identity. Passwords and symmetric cryptographic keys are shared secrets, which both the claimant and the verifier must protect. Asymmetric cryptographic keys have a private key (which only the subscriber knows) and a related public key, which can be made publicly available through a public key certificate issued by a Public Key Infrastructure (PKI).
- Identity proofing, registration, and the delivery of credentials that bind an identity to a token. This process may be done remotely or in person, depending upon the level of assurance required for the system.
- Remote authentication mechanisms, that is the combination of credentials, tokens, and authentication protocols used to establish that a claimant is in fact the claimed subscriber.
- Assertion mechanisms used to communicate the results of a remote authentication to other parties. Assertions issued by verifiers about claimants as a result of a successful authentication are either digitally signed by their issuers or are obtained directly by relying parties from a trusted party via a secure authentication protocol. Authentication protocols provide a way for a claimant to prove control of a token to a verifier without being compromised by eavesdroppers or other attackers. Eavesdroppers can compromise otherwise secure protocols used with symmetric keys if the tokens are passwords.

ITL Bulletins Via E-Mail
We now offer the option of delivering your ITL Bulletins in ASCII format directly to your e-mail address. To subscribe to this service, send an e-mail message from your business e-mail account to listproc@nist.gov with the message **subscribe itl-bulletin**, and your name, e.g., John Doe. For instructions on using listproc, send a message to listproc@nist.gov with the message **HELP**. To have the bulletin sent to an e-mail address other than the From address, contact the ITL editor at 301-975-2832 or elizabeth.lennon@nist.gov.

Summary of Requirements for Levels 1 Through 4

Following is a summary of the technical requirements specified in NIST SP 800-63 for the four levels of assurance defined by OMB:

Level 1 requires little or no confidence in the asserted identity. No identity proofing is required at this level, but the authentication mechanism should provide some assurance that the same claimant is accessing the protected transaction or data. A wide range of available authentication technologies can be employed and any of the token methods of Levels 2, 3, or 4, including Personal Identification Numbers (PINs), may be used. To be authenticated, the claimant must prove control of the token through a secure authentication protocol.

Plaintext passwords or secrets are not transmitted across a network at Level 1. However, this level does not require cryptographic methods that block offline attacks by an eavesdropper. For example, simple password challenge-response protocols are allowed. In many cases, an eavesdropper, having intercepted such a protocol exchange, will be able to find the password with a straightforward dictionary attack.

At Level 1, long-term shared authentication secrets may be revealed to verifiers. Assertions issued about claimants as a result of a successful authentication are either cryptographically authenticated by relying parties (using approved methods) or are obtained directly from a trusted party via a secure authentication protocol.

Level 2 requires confidence that the asserted identity is accurate. Level 2 provides for single-factor remote network authentication, including identity-proofing requirements for presentation of identifying materials or information. A wide range of available authentication technologies can be employed, including any of the token methods of Levels 3 or 4, as well as passwords. Successful authentication requires that the claimant prove through a secure authentication protocol that the claimant controls the token. Eavesdropper, replay, and online guessing attacks are prevented.

Long-term shared authentication secrets, if used, are never revealed to any party except the claimant and verifiers operated by the CSP; however, session (temporary) shared secrets may be provided to independent verifiers by the CSP. Approved cryptographic techniques are required. Assertions issued about claimants as a result of a successful authentication are either cryptographically authenticated by relying parties (using approved methods) or are obtained directly from a trusted party via a secure authentication protocol.

Level 3 is appropriate for transactions that need high confidence in the accuracy of the asserted identity. Level 3 provides multifactor remote network authentication. At this level, identity-proofing procedures require verification of identifying materials and information. Authentication is based on proof of possession of a key or password through a cryptographic protocol. Cryptographic strength mechanisms should protect the primary authentication token (a cryptographic key) against compromise by the protocol threats, including eavesdropper, replay, online guessing, verifier impersonation, and man-in-the-middle attacks. A minimum of two authentication factors is required. Three kinds of tokens may be used:

- ❑ “soft” cryptographic token, which has the key stored on a general-purpose computer,
- ❑ “hard” cryptographic token, which has the key stored on a special hardware device, and
- ❑ “one-time password” device token, which has symmetric key stored on a personal hardware device that is a cryptographic module validated at FIPS 140-2 Level 1 or higher. Validation testing of cryptographic modules and algorithms for conformance to Federal Information Processing Standard (FIPS) 140-2, *Security Requirements for Cryptographic Modules*, is managed by NIST.

Authentication requires that the claimant prove control of the token through a secure authentication protocol. The token must be unlocked with a password or biometric representation, or a password must be used in a secure authentication protocol, to establish two-factor authentication. Long-term shared authentication secrets, if used, are never revealed to any party except the claimant and verifiers operated directly by the CSP; however, session (temporary) shared secrets may be provided to independent verifiers by the CSP. Approved cryptographic techniques are used for all operations. Assertions issued about claimants as a result of a successful authentication are either cryptographically authenticated by relying parties (using approved methods) or are obtained directly from a trusted party via a secure authentication protocol.

Level 4 is for transactions that need very high confidence in the accuracy of the asserted identity. Level 4 provides the highest practical assurance of remote network authentication. Authentication is based on proof of possession of a key through a cryptographic protocol. This level is similar to Level 3 except that only “hard” cryptographic tokens are allowed, cryptographic module validation requirements are strengthened, and subsequent critical data transfers must be authenticated via a key that is bound to the authentication process. The token should be a hardware cryptographic module validated at FIPS 140-2 Level 2 or higher overall with at least FIPS 140-2 Level 3 physical security. This level requires a physical token, which cannot readily be copied, and operator authentication at Level 2 and higher, and ensures good, two-factor remote authentication.

Level 4 requires strong cryptographic authentication of all parties and all sensitive data transfers between the parties. Either public key or symmetric key technology may be used. Authentication requires that the claimant prove through a secure authentication protocol that the claimant controls the token. Eavesdropper, replay, online guessing, verifier impersonation, and man-in-the-middle attacks are prevented. Long-term shared authentication secrets, if used, are never revealed to any party except the claimant and verifiers operated directly by the CSP; however, session (temporary) shared secrets may be provided to independent verifiers by the CSP. Strong approved cryptographic techniques are used for all operations. All sensitive data transfers are cryptographically authenticated using keys bound to the authentication process.

Electronic identity credentials bind an identity (name) to a token. In some cases, they may be public documents, such as a public key certificate that binds a name to a public key, and that are published for anyone to use. In other cases, credentials that bind a shared secret to an identity are kept in protected CSP databases. Some protocols provide that CSPs issue one-time credentials to verifiers consisting of a name, challenge, and a reply, but not the long-term shared secret.

Passwords

Appendix A of the guide provides advice about how to estimate the strength of passwords. Attackers may be able to guess the passwords that are chosen by users, and systems should constrain the ability of attackers to test many password guesses. The guideline does not set minimum password length and does not establish a requirement to change passwords frequently. Instead, a method is described for estimating the “guessing entropy” of passwords, based on the password rules (minimum length, types of characters required, randomly chosen or user chosen, and the use of dictionaries to rule out commonly chosen passwords). The method limits the maximum allowed probability (one chance in 2^{14}) that an attacker with no other knowledge of the password could guess the password over its entire life. This calculation must account for methods used to limit the rate at which attacks can be carried out (e.g., three bad guesses in a row will lock the account for 24 hours) as well as rules for changing passwords.

Passwords can be retained for years if they are fairly complex and if the system limits the rate at which attacks can operate. Requiring frequent change of very complex passwords may result in high costs for the agencies in providing help to users, usability problems, and insecure user practices, such as keeping lists of passwords under keyboards. Moreover, even complex passwords may be vulnerable to "shoulder surfing" attacks and keyboard loggers, while verifier impersonation (e.g., decoy websites) and "social engineering" attacks may trick subscribers into revealing their passwords.

Looking Ahead

Electronic government is becoming increasingly important to agencies. OMB M-04-04 establishes a framework for determining the level of authentication assurance needed for e-government transactions, and NIST SP 800-63 provides specific technical guidance on how to achieve that level of assurance. M-04-04 and SP 800-63 assist agencies in providing a consistent level of authentication assurance to deliver services and perform their missions while protecting their systems and the privacy of users. NIST continues to investigate other methods for remote authentication, including the use of biometric data and the use of private and personal, but not secret, information. Future guidance will be issued as needed to cover additional authentication techniques and changing technical requirements.

***Disclaimer**: Any mention of commercial products or reference to commercial organizations is for information only; it does not imply recommendation or endorsement by the National Institute of Standards and Technology nor does it imply that the products mentioned are necessarily the best available for the purpose.*

U.S. DEPARTMENT OF COMMERCE
National Institute of Standards and Technology
100 Bureau Drive, Stop 8900
Gaithersburg, MD 20899-8900