ADVANCED AUTHENTICATION TECHNOLOGY

Introduction
Computer systems and the information they store and process are
valuable resources which need to be protected. With the current
trend toward networking, compromise of one computer on a network
can often affect a significant number of other machines connected
to the network.

The first step toward securing a computer system is the ability
to verify the identity of users. The process of verifying a
user's identity is typically referred to as user authentication.
Passwords are the method used most often for authenticating
computer users, but this approach has often proven
inadequate in preventing unauthorized access to computer
resources when used as the sole means of authentication. This
bulletin describes advanced authentication technology which can
be used to increase the security of computer systems and
provides guidance in the selection and use of this technology.

User Authentication
Authentication technology provides the basis for access control
in computer systems. If the identity of a user can be correctly
verified, legitimate users can be granted access to system
resources. Conversely, those attempting to gain access without
proper authorization can be denied. As used in this bulletin,
authentication is defined as the act of verifying the identity of
a user. Once a user's identity is verified, access control
techniques may be used to mediate the user's access to data. A
variety of methods are available for performing user
authentication.

The traditional method for authenticating users has been to
provide them with a secret password, which they must use when
requesting access to a particular system. Password systems can
be effective if managed properly (Federal Information Processing
Standard [FIPS] 112), but they seldom are. Authentication which
relies solely on passwords has often failed to provide adequate
protection for computer systems for a number of reasons. If
users are allowed to make up their own passwords, they tend to
choose ones that are easy to remember and therefore easy to
guess. If passwords are generated from a random combination of
characters, users often write them down because they are
difficult to remember.

Where password-only authentication is not adequate for an
application, a number of alternative methods can be used alone or
in combination to increase the security of the authentication
process. The three generally accepted methods for verifying the
identity of a user are based on something the user knows, such as
a password; something the user possesses, such as an
authentication token; and some physical characteristic of the
user, such as a fingerprint or voice pattern.

Token-Based Authentication
Token-based authentication schemes require the system user to
produce a physical token which the system can recognize as
belonging to a legitimate user. These tokens typically contain
information which is physically, magnetically, or electrically
coded in a form which can be recognized by a host system. The
automatic teller machines used by the retail banking industry,
which require the user to carry a magnetic stripe card, are one
example of token-based authentication systems. The most
sophisticated tokens contain one or more integrated circuits
which can store and, in some cases, process information.
Tokens which are manufactured in the form of a credit card with
an onboard microprocessor and memory are commonly referred to as
"smart" cards.

Token-based systems reduce the threat from attackers who attempt
to guess or steal passwords, because the attacker must either
fabricate a counterfeit token or steal a valid token from a user
in addition to knowing the user's password.

Biometric Authentication
Biometric authentication relies on a unique physical
characteristic to verify the identity of system users. Common
biometric identifiers include fingerprints, written signatures,
voice patterns, typing patterns, retinal scans, and hand
geometry. The unique pattern which identifies a user is formed
during an enrollment process, producing a template for that user.

When a user wishes to authenticate to the system, a physical
measurement is made to obtain a current biometric pattern for the
user. This pattern can then be compared against the enrollment
template in order to verify the user's identity. Biometric
authentication devices tend to cost more than password or token-
based systems, because the hardware required to capture and
analyze biometric patterns is more complicated. However,
biometrics provide a very high level of security because the
authentication is directly related to a unique physical
characteristic of the user which is more difficult to
counterfeit. Recent technological advances have also helped to

reduce the cost of biometric authentication systems.

Combination Methods
Passwords, authentication tokens, and biometrics are subject to a
variety of attacks. Passwords can be guessed, tokens can be
stolen, and even biometrics are susceptible to certain attacks.
These threats can be reduced by applying sound design principles
and system management techniques during the development and
operation of an authentication system.

One method which can substantially increase the security of an
authentication system is to use a combination of authentication
techniques. For example, an authentication system might require
users to present an authentication token and also enter a
password. By stealing a user's token, an attacker would still be
unable to gain access to the host system, because the system
would require the user's password in addition to the token.

Implementation Guidelines and Recommendations
An organization must answer numerous questions when it decides to
implement an advanced authentication system. The following
guidelines will assist those responsible for evaluating,
procuring, and integrating these systems.

Risk Analysis - A thorough analysis should be done to
determine what parts of the system in question are vulnerable to
attack, and to prioritize these vulnerabilities in terms of
severity and likelihood.

Product Evaluation and Selection - Once the risks associated with
a host system have been identified, this information can be used
to select an authentication system which provides adequate
protection against these risks. In addition, the authentication
system will have to meet several other requirements in order to
function effectively in a given environment. The organization
responsible for selecting the authentication system should decide
whether sufficient in-house expertise exists to evaluate the
available options. In some cases, it is more cost-effective to
hire a consultant who is familiar with the available technology.

Whether the evaluation is done in-house or by a consultant, the
following items should be considered:

  o Sources of information - A variety of sources should be used
     when evaluating authentication systems. Vendor product
     literature can be very helpful in describing specific
     details of product operation, and in understanding the range
     of products offered. There are several annual conferences

devoted to computer security, network access control, and
authentication technology. In addition to the papers
presented at these conferences, there are usually large
vendor exhibit halls and product forums. Many
organizations, particularly those in the government sector,
have published information on the selection and integration
of advanced authentication technology. These publications
are often the result of practical experience gained during
the implementation of these systems, and so can be
particularly useful.

o Integration into existing environment - This factor is
   discussed further in the next section, but is an important
   consideration when selecting a product. All other features
   of an authentication system may be irrelevant if the product
   cannot be integrated into the customer's computing
   environment.

o Custom design - Sometimes an organization's needs cannot be
   met by a commercially available product. In these cases,
   the organization may decide to do a custom design using
   in-house resources. This alternative is most practical for
   large organizations with experienced system design and
   support groups, or for smaller organizations with a high
   level of expertise in computer access control systems.
   Vendors are often willing to work with customers to modify
   existing products or design new products to meet custom
   requirements. An arrangement which often works well is for
   the customer and vendor to work together on the design of
   the system, and for the vendor to then manufacture the
   product.

o Cost and performance - The relationship between cost and
   performance can be relatively complex for authentication
   technology. Similar products from different vendors may
   vary widely in cost, depending on the vendor's manufacturing
   and development techniques and marketing philosophies. In
   general, devices with a higher performance level will cost
   more, but individual cases should be evaluated carefully.
   The general approach should be to procure the authentication
   system which provides the required level of security and
   other performance factors at a minimum cost.

o Accuracy - The accuracy of an authentication system refers
   to the ability of that system to correctly identify
   authorized system users while rejecting unauthorized users.
   Since this is the primary function of an authentication
   system, accuracy is directly related to the level of

security provided by the system. Vendors may not be
objective about producing and interpreting the results of
tests which quantify the accuracy of the authentication
process with regard to the vendor's particular products.
For these reasons, an organization may wish to run
independent tests to determine the accuracy of an
authentication system in terms which are relevant to the
environment in which the system will be used.

o Reliability - An authentication system should be capable of
   operating in its intended environment for a reasonable
   period of time. During this time, the system is expected to
   perform at or above a level which ensures an appropriate
   amount of protection for the host system. If the
   authentication system fails, the chances for unauthorized
   access during the failure should be minimized.

o Maintainability - All hardware and software systems require
   some form of maintenance. The components of an
   authentication system should be evaluated to determine the
   level of maintenance which the system will require. One
   goal in the design of an authentication system should be to
   minimize the maintenance requirements within the constraints
   of system cost, performance, and available technology.

o Commercial availability - Large-scale networking of computer
   systems and distributed computing are relatively recent
   developments, and are the driving forces behind the need for
   more effective methods for authenticating system users.
   Unfortunately, the market for advanced authentication
   technology is not fully developed and is somewhat unstable.
   Many commercially available authentication systems have not
   yet been sold in quantity. An organization that is
   considering the use of this technology should evaluate the
   vendor's ability to produce systems that meet specific
   quality control standards and in sufficient quantity to meet
   the user's requirements. Contracts written to procure
   authentication systems should provide some form of
   protection for the customer in the event that the vendor is
   unable to produce systems in the quantities required.

o Upgradeability - Because the technology of advanced
   authentication systems is continually developing, any
   authentication system should be able to accommodate the
   replacement of outdated components with new ones. A modular
   approach to the design of an authentication system, with
   clearly defined interfaces between the system components,
   facilitates the process of upgrading to new technology.

o   Interoperability - A wide variety of computing platforms and
    security architectures are in use today. Any authentication
    system should be designed to work with as many of these
    diverse platforms as possible, or at least to require a
    minimum of modifications to work in different environments.

o   Reputation of manufacturer - Obtaining satisfactory service
    during the selection, installation, and long-term operation
    of an authentication system can be difficult if the
    manufacturer is uncooperative. Customers can request a list
    of references from prospective vendors for products and
    services which have been provided to other customers in the
    past. In addition, the resumes of key individuals working
    on the vendor's staff can sometimes be examined to determine
    whether an adequate level of expertise is available.

o   Training programs - Some form of training is usually
    necessary for the people who will be using and maintaining
    an authentication system. An effective training program is
    of critical importance to the success of any new system.
    Vendors should offer training appropriate for everyday users
    of the system, and also for the system administrators who
    will be responsible for managing the system.

System Integration - The integration of an authentication
system into an existing computer environment can be very
difficult. Most operating systems do not contain well-defined
entry points for replacing the default authentication mechanism
supplied with the operating system. This is partly because there
is no widely accepted standard for the interface between an
operating system and an authentication device. Until such a
standard becomes available, there are three general options:

o   In some cases, the vendor who provides the authentication
    system may have already integrated it into certain operating
    systems. If the authentication system meets the
    requirements of the customer and the customer is using the
    specified operating system, then the system integration has
    already been accomplished.

o   Operating system vendors may select certain security
    architectures for incorporation into their systems. If
    these architectures include an authentication technology
    which the customer finds acceptable, then the operating
    system may be purchased with the appropriate authentication
    mechanism as part of the package.

o It may be necessary to customize the authentication system
   and perhaps modify the host operating system so that the two
   can communicate. This will involve cooperation between the
   operating system vendor, the authentication system vendor,
   and the customer, unless the customer has sufficient
   expertise to perform the integration in-house. A
   prototyping approach is strongly recommended, due to the
   complexity of this type of project. Implementing such a
   system on a small scale first can be very helpful in
   determining what problems will be encountered in a
   full-scale implementation.

System Maintenance - After an authentication system has
been selected and installed, it must be maintained. Maintenance
costs can easily exceed the initial acquisition cost if the
system is to be in operation for a reasonable length of time. It
is therefore important that long-term plans for system
maintenance be developed by the customer or provided by the
vendor in the initial stages of the procurement cycle.
Provisions must be made for assigning responsibilities for system
administration so that new users can be enrolled, inactive
accounts deleted, and system malfunctions identified and
corrected.

The majority of network authentication systems employ some form
of cryptography, which means that some form of cryptographic key
management system will be necessary. The key management
component may be provided by the authentication system vendor,
but the process of maintaining and distributing keys usually
requires active participation by the host system. Since the
security of a cryptographic system is directly related to the
level of protection provided for the cryptographic keys, it is
essential for the vendor or customer to develop a system for
managing these keys effectively. Also, the host computer system
will probably evolve over time through the addition of new
software and hardware, and these changes may require
corresponding modifications or upgrades to the authentication
system to maintain compatibility.

Summary
Password-based authentication is the most widely used method for
verifying the identity of persons requesting access to computer
resources. However, authentication based only on passwords often
does not provide adequate protection. The use of authentication
tokens, biometrics, and other alternative methods for verifying
the identity of system users can substantially increase the
security of an authentication system. The proliferation of
networked computer systems and the corresponding increase in the

potential for security violations makes it even more critical
those who design and operate computer systems to understand and
implement effective authentication schemes.

References

    Guideline on User Authentication Techniques for Computer
    Network Access Control, National Institute of Standards and
    Technology (U.S.), Federal Information Processing Standards
    Publication 83, National Technical Information Service,
    Springfield, VA, September 1980.

    Computer Data Authentication, National Institute of Standards
    and Technology (U.S.), Federal Information Processing
    Standards Publication 113, National Technical Information
    Service, Springfield, VA, May 1985.

    Biometric Access Control Device Evaluation Criteria (Draft
    Report), DCI Intelligence Information Handling Committee,
Access Control Subcommittee, Community Headquarters Building,
Washington, DC 20505, February 1991.

    Smart Card Technology: New Methods for Computer Access
    Control, National Institute of Standards and Technology
    (U.S.), NIST Special Publication 500-157, September 1988.

    Financial Institution Sign-On Authentication for Wholesale
    Financial Transactions, American National Standard X9.26,
    American National Standards Committee X9, American Bankers
    Association, May 1990.

    Password Usage, National Institute of Standards and
    Technology (U.S.), Federal Information Processing Standards
    Publication 112, National Technical Information Service,
    Springfield, VA, May 1985.

For More Information
For further information on NIST's ongoing work in advanced
authentication technology, contact Jim Dray, Computer Security
Division, Room A216, Technology Building, National Institute of
Standards and Technology, Gaithersburg, MD 20899, (301) 975-
3356.