USING PERSONAL IDENTITY VERIFICATION (PIV) CREDENTIALS IN PHYSICAL ACCESS CONTROL SYSTEMS (PACS)

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

The security of the federal government's operations is dependent upon the use of secure, reliable methods for identifying the people who access federal facilities and information systems. Homeland Security Presidential Directive 12 (HSPD-12), *Policy for a Common Standard for Federal Employees and Contractors*, issued in August 2004, charged the Information Technology Laboratory of the National Institute of Standards and Technology (NIST) with developing a mandatory standard for secure and reliable forms of identification for use throughout the federal government. NIST has developed Federal Information Processing Standard (FIPS) 201, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, and supporting specifications, reference implementations, and conformance tests to help federal agencies use the PIV standard.

In November 2008, NIST issued a new publication recommending best practices for implementing PIV technologies in physical access control systems (PACS). The publication addresses current weaknesses in the PACS used in many federal buildings, which were often developed for a specific site. If they employ vendor-specific architectures, employees and contractor identification (ID) cards issued for one facility may not be accepted at another facility. Also, many systems do not assure the identity of the cardholder, and the ID cards that have been issued can be easily cloned or counterfeited.

NIST Special Publication (SP) 800-116, *A Recommendation for the Use of PIV Credentials in PACS*

NIST SP 800-116, *A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS)*, was written by William MacGregor of NIST, Ketan Mehta of Mehta, Inc., and David Cooper and Karen Scarfone of NIST. The publication describes a strategy that agencies can apply in using PIV Cards for access to federal buildings, and in moving toward the goal of governmentwide interoperability of PIV credentials.

NIST SP 800-116 recommends a risk-based approach for selecting appropriate PIV authentication mechanisms to manage physical access to federal government facilities and assets. One section deals with known technical threats to PIV authentication mechanisms. Another section provides guidance on implementing FIPS 201 and its supporting special publications, which specify requirements for PACS interfaces with the PIV Card and PIV System.

Other subjects covered include the benefits of electronic verification and direct integration of a PIV Card with the electronic PACS; a discussion of available authentication mechanisms and their application in PACS environments; and the selection of a level of security for each application. FIPS 201 requires that PIV credentials include graduated criteria - from least secure to most secure - for authentication to ensure flexibility in selecting the appropriate level of security for each application. The final sections of the publication help agencies prepare a migration plan for enabling the use of PIV credentials in their PACS environments in order to achieve improved operations, enhanced security, trust and interoperability with other federal agencies, and cost efficiencies. A discussion of the issues that need to be studied in the future is included.

The appendices of NIST SP 800-116 provide summaries of PIV information for easy reference. All of the recommendations presented throughout the publication are summarized in Appendix A. Appendix B provides information on how to achieve unique identifiers for individual PIV Cardholders. Appendix C provides a complete list of possible PIV authentication mechanism combinations that are available for application to federal facilities. A reference list of NIST and other sources of information about PIV, both in-print and online, and a glossary of the abbreviations and acronyms used in the publication complete the appendices.

NIST SP 800-116 is available from the NIST Web site:
http://csrc.nist.gov/publications/PubsSPs.html.

Background Information on HSPD-12 and FIPS 201

HSPD-12 stated that the wide variations in the quality and security of forms of identification used to gain access to secure federal and other facilities where there is potential for terrorist attacks should be eliminated. The directive called for the development of a mandatory, governmentwide standard for secure and reliable forms of identification issued by the federal government to its employees and contractors. HSPD-12 stated that the secure and reliable forms of identification should be:

- Based on sound criteria for verifying an individual's identity;
- Strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation;
- Rapidly authenticated electronically; and
- Issued only by providers whose reliability has been established by an official accreditation process.

FIPS 201, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, which was developed to satisfy the requirements of HSPD-12, was approved by the Secretary of Commerce and issued in 2005. FIPS 201 specifies technical and operational requirements for interoperable PIV Systems that issue PIV Cards as identification credentials and that use the cards to authenticate an individual's identity. PIV Cards are smart cards that incorporate an individual's identity credentials. PIV components and subsystems use the electronically stored data on the cards to carry out automated identity verification of the individual. Authentication of an individual's identity is an essential component of secure access control to facilities and to information systems. FIPS 201 describes the minimum requirements for a federal personal identity verification system, including personal identity proofing, registration, and issuance. The standard also provides detailed specifications that will support technical interoperability among PIV Systems of federal departments and agencies.

NIST has developed supplementary specifications and recommendations that assist agencies in implementing the technical and administrative requirements of FIPS 201. See the More Information section at the end of this bulletin for references to PIV-related publications. To help agencies acquire PIV Systems that correctly implement FIPS 201 and that are interoperable, NIST developed a validation and testing program for the standard.

Information about NIST's activities to support Personal Identity Verification (PIV) of federal employees and contractors is available at the NIST Web site: http://csrc.nist.gov/groups/SNS/piv/index.html.

Challenges to Use of PIV in PACS

Currently, many federal government PACS lack interoperability and authentication assurance for the ID cards that have been issued. In addition, PACS also present other challenges:

- Scalability. Some deployed systems are limited in their capability to process the longer credential numbers necessary for governmentwide interoperability.

- Security. PACS readers in operation can read an identifying number from a card, but in most cases, they do not perform a cryptographic challenge/response exchange. Most bar code, magnetic stripe, and proximity cards can be copied easily. The technologies used in these systems may offer little or no authentication assurance.

- Validity. Many PACS control expiration of credentials through an expiration date stored in a site database. There is no simple way to synchronize the expiration or revocation of credentials for a federal employee or contractor across multiple sites.

- Efficiency. The personal identification numbers (PINs), public key infrastructure, and biometrics with deployed PACS are managed on a site-specific basis. Individuals must enroll PINs, keys, and biometrics at each site. Since PINs, keys, and biometrics are often stored in a site database, they may not be technically interoperable with PACS at other sites.

Security Concerns and Authentication Methods

The technical threats to PIV Systems are often carried out by attackers who exploit overlooked or newly introduced vulnerabilities in operational systems. The PIV System protects the trustworthiness of the PIV Card data objects through PIV Card access rules and digital signatures. Overall trust in the execution of a PIV authentication mechanism is also dependent on correct operation of the PIV Card, the PACS, and the PIV Card validation infrastructure, and, to a degree, on protecting the confidentiality, integrity, and availability of the communication channels among them. Attacks may be directed against any of these components, with varying difficulty and potential impact. Threats to be considered in developing a risk-based approach to PIV Systems include:

Identifier collisions: If information is lost from the unique identifier on a card before it is compared against Access Control List (ACL) entries, multiple cards may generate the same reduced identifier, resulting in multiple cardholders being granted the same access privileges.

Terminated PIV Cards: PIV Cards may be terminated for a number of reasons, including a lost or stolen card. A terminated PIV Card could continue to provide access unless checks for termination are performed.

Visual counterfeiting: Counterfeit cards that mimic the appearance of a PIV Card could be used when PIV Cards are only visually inspected by a security guard. Guards can be trained to recognize the security features of a valid card, but electronic verification is recommended.

Skimming: A contactless PIV Card reader with a sensitive antenna could be concealed in a briefcase and could read data from a PIV Card in close proximity. This threat can be countered by the use of access rules that prevent the release of biometric and other data over the contactless interface, and by the use of other shielding techniques.

Sniffing: Sniffers are receivers that can pick up signals when a PIV Card is presented to a contactless reader at an access point. A sniffer could potentially capture the entire message transaction between the reader and the card.

Social engineering: An attacker who persuades the cardholder to give up possession of a PIV Card could quickly insert the card into a contact reader and copy all of the information available for free reading. An attacker could also create a Web page that asks the subject to insert the PIV Card into the computer and enter the PIN for an apparently legitimate purpose. The cardholder’s PIN and all of the readable PIV data could be captured.

Electronic cloning: Data collected through successful skimming, sniffing, or social engineering attacks could be used to create a partial clone of a PIV Card. Additional authentication mechanisms such as public and secret keys used for cryptographic authentication methods would prevent the success of cloning attacks.

Electronic counterfeiting: An attacker could construct a battery-powered, microprocessor-based device that emulates a PIV Card, and program it to try many instances of fabricated cardholder identity information with the reader.

FIPS 201 defines the mechanisms for authenticating the holders of PIV Cards. Cards that undergo Visual (VIS) inspection methods should include information such as name, photograph, agency identification, and expiration date on the card. Cards using the Cardholder Unique Identifier (CHUID) contain the Federal Agency Smart Credential Number (FASC-N), which uniquely identifies the holder of each card. Cards implementing Biometric (BIO) and Attended Biometric (BIO-A) methods include the fingerprints and facial image of the cardholder. PIV Authentication Key (PKI) is a PIV authentication mechanism that is implemented by an asymmetric PIV authentication key challenge/response protocol. Another authentication mechanism is Card Identification Key (CAK), which uses an optional key to authenticate the cardholder.

VIS, CHUID, and CAK authentication mechanisms provide one-factor authentication. VIS provides weak one-factor authentication since the card verification is subjective. CHUID also provides weak one-factor authentication since the card could be cloned or counterfeited. The BIO mechanism provides one-factor authentication since the reference biometric template is compared against the sample biometric template. The PKI authentication mechanism provides two-factor authentication since it requires possession of the PIV Card and knowledge of the PIN. The BIO-A mechanism provides two-factor authentication since the reference biometric template is compared with the sample biometric template in the presence of an attendant. The knowledge of a PIN, the third factor of authentication, can only be trusted by combining PKI + BIO(-A) or CAK + BIO(-A) authentication mechanisms.

FIPS 201 defines authentication mechanisms at three E-Authentication assurance levels: SOME, HIGH, and VERY HIGH. FIPS 201 also standardizes optional credential elements that extend trust in the PIV System to functions beyond authentication. A gap remains, however, between the concepts of authentication assurance levels and their application in a PACS environment. NIST SP 800-116 introduces the concept of “Controlled, Limited, Exclusion” areas to employ risk-based PIV authentication mechanisms for different areas within a facility. See the Recommendations section below.

Future Needs

NIST has identified issues that need further study to improve the implementation and use of PIV Systems and to protect the personal privacy of the users. Some issues for future investigation include:

- development of an enhancement or replacement for the FASC-N to achieve both credential identification and binding of the information about the cardholder, and to support an extensible framework for subject identification; and

- use of Secure Biometric Match-On-Card (SBMOC) techniques, which employ the communication of sensitive biometric data in encrypted form that can be decrypted only by the PIV Card. SBMOC does not require the use of the cardholder’s PIN and can be performed safely and quickly over a contactless interface.

NIST’s Recommendations for Using PIV Credentials in PACS

Recommendations to federal agencies are presented throughout NIST SP 800-116 and are summarized in Appendix A of the publication. NIST recommends that agencies develop a PIV Implementation Maturity Model (PIMM) to measure the progress of facility and agency implementations.

Since the areas accessible via different access points within a facility do not all have the same security requirement, the PIV authentication mechanisms should be selected to be consistent with, and integral to, the overall security requirements of the protected area. A facility may need to employ multiple authentication mechanisms. NIST SP 800-116 defines the protected areas as Controlled, Limited, and Exclusion areas. Proof of affiliation, such as an agency badge, is often sufficient to gain access to a Controlled area. Access to Limited areas is often based on functional subgroups or roles, as established by authentication of the cardholder. Access to Exclusion areas may be gained by individual authorization only. These areas correspond generally to the definitions in FIPS 201 for LOW (Controlled), MODERATE (Limited), and HIGH (Exclusion) impacts on assets or resources.

NIST recommends the use of one authorization factor for Controlled areas, two authorization factors for Limited areas, and three authorization factors for Exclusion areas. A list of possible uses of PIV authentication mechanisms against protected areas is provided in Appendix C.

A risk-based migration strategy should be planned and implemented to achieve the effective use of PIV credentials. NIST SP 800-116 recommends a model that allows agencies to incrementally enable their use of PIV access points. The model is defined in terms of maturity levels:

Maturity Level 1—Ad hoc PIV verification. The facility is able to authenticate PIV Cards by performing required authentication mechanisms on an ad hoc, on-demand basis.

Maturity Level 2—Systematic PIV verification to Controlled areas. PIV Cards and currently deployed non-PIV PACS cards are accepted for access to the Controlled areas at this level.

Maturity Level 3—Access to Exclusion areas by PIV or exception only. Non-PIV PACS cards are not accepted for access to the Exclusion areas at this level.

Maturity Level 4—Access to Limited areas by PIV or exception only. Non-PIV PACS cards are not accepted for access to the Limited or Exclusion areas at this level.

Maturity Level 5—Access to Controlled areas by PIV or exception only. Non-PIV PACS cards are not accepted for access to any areas at this level.

More Information

For information about NIST standards, guidelines, and other security-related publications that help organizations plan and implement a comprehensive approach to IT security, see NIST's Web page: http://csrc.nist.gov/publications/index.html.

These publications provide information and specifications for the implementation of PIV credentials:

FIPS 201-1, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, specifies technical and operational requirements for interoperable PIV Systems that issue PIV Cards as identification credentials and that use the cards to authenticate an individual's identity.

NIST SP 800-73-2, *Interfaces for Personal Identity Verification*, consists of four parts:

1- End-Point PIV Card Application Namespace, Data Model and Representation
2- End-Point PIV Card Application Interface
3- End-Point PIV Client Application Programming Interface
4- The PIV Transitional Data Model and Interfaces

NIST SP 800-76-1, *Biometric Data Specification for Personal Identity Verification*, specifies the technical acquisition and formatting requirements for biometric data of the PIV System.

NIST SP 800-78-1, *Cryptographic Algorithms and Key Sizes for Personal Identity Verification*, specifies the acceptable cryptographic algorithms and key sizes to be implemented and used for the PIV System.

NIST SP 800-104, *A Scheme for PIV Visual Card Topography*
NIST Interagency/Internal Report (NISTIR) 7284, *Personal Identity Verification Card Management Report*

The following publications provide information about specifications for PIV validation, PIV readers, and PIV accreditation:

NIST SP 800-85A, *PIV Card Application and Middleware Interface Test Guidelines*
This publication is being updated. The revised document, Draft SP 800-85A-1, *PIV Card Application and Middleware Interface Test Guidelines (SP 800-73-2 compliance)*, is posted on the Computer Security Resource Center Web site: http://csrc.nist.gov.

NIST SP 800-85B, *PIV Data Model Test Guidelines*
NIST SP 800-96, *PIV Card to Reader Interoperability Guidelines*
NIST SP 800-79-1, *Guidelines for the Accreditation of Personal Identity Verification (PIV) Card Issuers (PCI's)*

NIST SP 800-87-1, *Codes for Identification of Federal and Federally-Assisted Organizations*
NIST IR 7337, *Personal Identity Verification Demonstration Summary*
NISTIR 7452, *Secure Biometric Match-on-Card Feasibility Report*

Disclaimer

Any mention of commercial products or reference to commercial organizations is for information only; it does not imply recommendation or endorsement by NIST nor does it imply that the products mentioned are necessarily the best available for the purpose.