Scientific Access to the National Laboratories and the Personal Identification Verification Standard

Potentially Broad Detrimental Impact to Scientific Activities involving Non-Employees and Non-Contractors

A DOE Laboratory Directors' System of Labs' Computing Coordinating Committee (SLCCC) White Paper[1]

23 December 2004

The Personal Identify Verification (PIV) standard being developed by NIST is an effort to create a common identification system for federal employees and contractors to be used for access to federally controlled facilities and computing systems. While highly supportive of appropriate and effective security, members of the research and engineering community have serious concerns about how PIV may be applied and implemented.

The concerns with the proposed standard fall into these general categories:

- The usage scenarios and requirements for non-federal employees and non-contractors, including many collaborators and users of national scientific facilities, have not been taken into account in the standard, leading to ambiguities in interpretation.
- It is not clear how the proposed system will relate to and interoperate with existing security standards and security systems.
- The proposed system has not been tested and may have security vulnerabilities.

Under some interpretations of the standard, the system could halt many of the unclassified scientific missions underway at the National Laboratories; under other interpretations, this may not be an issue.

This white paper attempts to gather the issues raised by security experts and scientific leads across the Laboratories in order to foster discussion on how best to improve the security of our national resources while supporting our national research capabilities and mission.

Background

In August of 2004, President Bush issued Homeland Security Presidential Directive 12 (HSPD-12), creating a policy for a common identification standard for federal employees and contractors. The directive requires that a standard for secure and reliable identification be published by the Department of Commerce by February 2005, and that executive departments and agencies implement the standard by October 2005. In regards to access, the directive states only that the departments and agencies shall "require the use of identification by Federal employees and contractors that meets the Standard in gaining physical access to Federally controlled facilities and logical access to Federally controlled information systems."

The National Institute of Standard and Technology is responsible for the creation of the standard called for in HSPD-12. They have formed the Personal Identity Verification (PIV) project to respond to the directive. Information on the project is available on the web at http://www.csrc.nist.gov/piv-project/. The proposed standard, Federal Information Processing

---

[1] SLCCC is a coordinating committee that includes each CIO of the National Laboratories. Comments on this paper should be directed to Remy Evard, remy.evard@anl.gov, Argonne National Laboratory (Chair, PIV Task group); Becky Verastegui, verasteguirj@ornl.gov, Oak Ridge National Laboratory (Chair, SLCCC Executive Committee); Sandy Merola, merola@lbl.gov, Lawrence Berkeley National Laboratory (SLCCC Executive Committee); Roy Whitney, whitney@jlab.org, Jefferson Lab (SLCCC Executive Committee).

Standards Publication 201 (FIPS PUB 201), as well as supporting documentation and presentations, are available at this web site.

FIPS PUB 201 describes an identity-card system. The publication describes the cards themselves, a system for issuing and managing cards securely, and some aspects of the ways in which cards would be used to securely authenticate for access to federal facilities and systems. In addition to standard attributes of identification cards such as name and image, the cards will have an imbedded chip containing a unique ID, cryptographic keys, and biometric (fingerprint) data of the card bearer.

Concerns Related to Unclassified Science and Engineering

It is not clear whether or not the system as described in FIPS PUB 201 will be applied rigorously to all facility and computer access at the Department of Energy's National Laboratories. If it is applied in the strictest reading of the publications, the following issues will become serious problems.

Non-Employee and Non-Contractor Access

As directed by HSPD-12, the approach in FIPS PUB 201 addresses the identification requirements of an environment in which federal employees and contractors access federally controlled resources. However, in order to fulfill their research and facility missions, the Department of Energy laboratories operate scientific user facilities for use by non-federal and non-contractor employees and participate in collaborations that include researchers outside of the federal government. Many of the labs have as many non-employee and non-contractor visitors, collaborators and users conducting work on-site and on the computing systems along side employees. In addition, a sizable fraction of the collaborators and users accessing the data and computational resources never physically come on-site to the labs.

The proposed PIV system describes how employees and contractors of the federal government would attain PIV cards, but has no mechanism for non-employees and non-contractors to acquire cards, especially those who do not physically appear at the laboratory. Standard users of laboratory facilities are university researchers, foreign collaborators, and industry partners, none of whom would meet the criteria for a card, not even the "low assurance" option of the standard. The planned processes require physical presence at a specific registrar and presentation of a valid state or federal ID, some of which would be impossible for foreign scientists to provide.

If the system were to be applied to all laboratory facilities and computing systems and the process for card acquisition was not extensively modified to enable access by non-employees, non-contractors and foreign scientists, then thousands of unclassified research projects will halt or be seriously impacted.

Integration With and Key Capabilities of Existing Security Systems

The model described in FIPS PUB 201 is a public key infrastructure (PKI). The entire system is not completely described, such as the provisions for key management, delegation, and assignment of identity to systems. The usage scenarios in the documents describe a fairly simple client/server model that is appropriate when authenticating a federal user to a federal web page, but does not meet the requirements for complex system simulation on a multi-node supercomputer. If the proposed standard is meant to replace or interoperate with existing credential systems the following issues require resolution:

- No method of using the PIV card for access to computers beyond the directly attached machine is described. A researcher may need to delegate the right to authenticate to a service so that some essential step can be completed without direct intervention, such as the ability to run a parallel simulation across a thousand processors without typing a PIN a thousand times.

- In common networking and collaboration interactions, users are only one of the concerns. Devices, hosts, and services also need to be identified securely for mutual authentications. This does not appear to be addressed.
- Many laboratories have significant deployments of credential and directory systems supporting the day-to-day use of the entire Laboratory workforce and collaborative community. There is no information on how the PIV standard will interoperate with or replace these.

Technical and Security Concerns

The FIPS PUB 201 standard states clearly and appropriately that the use of the standard does not guarantee the security of the overall system. It is clear that this is meant to be a step towards an overall improvement of security, not a completely secure system. Nonetheless, there are two security-related aspects of the standard that should be considered in the deployment of this system.

First, the use of the proposed PIV system will not stop a hacking technique known as "session hijacking". Session hijacking, which is a growing threat, occurs after the authentication step.

Second, and perhaps most importantly, history has shown repeatedly that security systems take time to mature. It is common for a system to be considered strong on paper to be rendered highly vulnerable in practice. The aggressive timeframe for the rollout of the PIV increases the odds that essential design flaws will not be detected in advance of widespread deployment. For example, from the specification, it appears that a PIV card may be vulnerable to a compromised PIV card reader. Exactly whether or not this is true is an open question, dependent on detailed analysis of a system that does not yet exist and is not fully specified – but the implications, if true, could be very costly to all agencies involved in the deployment of the system.

Issues to Address

The President's directive, HSPD-12, is clear that PIV is meant to apply to federal employees and contractors accessing federally controlled resources. The FIPS PUB 201 draft standard focuses precisely on that scenario, and the proposed plan will likely result in major improvements in security for resources that fit well into that model.

The concern of the scientific community is that if this same plan is applied broadly, such as to access by non-federal employees and non-contractors to scientific user facilities at the National Laboratories, then the majority of work at the science labs will be stopped or reduced significantly. The concern is that with the ambiguities in the FIPS PUB 201 draft, it may be applied beyond the environment for which it was apparently intended.

In order to make progress on the PIV while supporting our national science mission, the following issues should be carefully considered:

- If HSPD-12 will be applied to physical facilities and computing systems at the National Laboratories, then there must be a reasonable mechanism for people who are not federal employees, not federal contractors, not citizens, or not physically present at the facility to continue their legitimate use of these facilities and systems.
- If these resources will be available via the PIV system, the interaction between the PIV and other authentication mechanisms must be clarified.
- If the PIV system is intended to replace other authentication systems at some point in time, it must have their degree of sophistication in order to support modern multi-system interactions.
- If the PIV system will be deployed on the planned schedule, there must be mechanisms to fully test the system and mechanisms to quickly and economically recover from potentially major system design flaws.