Using PIV Smart Cards on Linux for Authentication to Windows Active Directory

Douglas E. Engert

Computing and Information Systems

April 26, 2006

DOE Cyber Security Group Training Conference

Dayton, Ohio

Updated for:

AFS & Kerberos Best Practices Workshop

SLAC

May 10, 2007

Argonne National Laboratory is managed by
The University of Chicago for the U.S. Department of Energy

Driving Force

- Homeland Security Presidential Directive/Hspd-12
    - *August 2004*
  - "and logical access to Federally controlled information systems."
- FIPS-201 "Personal Identity Verification (PIV) of Federal Employees and Contractors."
    - *February 2005*
  - Response to HSPD-12
- NIST 800-73 "Interfaces for Personal Identity Verification"
    - *February 2005*
  - Defines the PIV card
- NIST 800-73-1
    - *April 2006*
  - Updated version

Logical Access

- “NIST believes PIV smartcard login is essential to protecting logical access to Federally controlled information systems. … promote compatibility of PIV cards with COTS smart card login mechanisms and common applications with minimal negative impact on privacy. ”
  NIST 800-73-1 Appendix F-Errata
- Login
  - To local workstation
    - *Standalone*
    - *Part of a domain*
  - To network applications
    - *Part of a domain*
- Web authentication
  - Another login to network application

The Project Goal

Add PIV support for logical access to some open source smart card package such that it can be used by other common applications. Get the modifications added to the open source distribution so it will be generally available when PIV cards are generally available.

- OpenSC was chosen
  - Open source libraries for accessing smartcards
  - Many different smart cards
  - ISO 7816-4 routines
  - Can use PC/SC
  - Provides a PKCS #11 interface to applications
  - Was easy to add PIV
  - Modifications accepted and expected to be in 0.11.0 release
  - Can run on Windows and Mac too!

Update for AFS & Kerberos Best Practices Workshop

- http://www.opensc-project.org
  - OpenSC 0.11.1 has basic PIV code
  - OpenSC 0.11.2 has gzip'ed cert support thanks to Identity Alliance
  - SCA – Mac OS X Installer - 0.11.2
  - SCB – Windows Smart Card Bundle - still 0.11.1
    - *PKCS#11 for Fire Fox, needs ID Ally CSP for login*
  - http://www.opensc-project.org/opensc/wiki/UnitedStatesPIV
- http://packages.debian.org/unstable/utils/opensc

NIST 800-73-1

- Part 1 - PIV data model, and objects on card
- Part 2.1 – PIV Application Programming Interface
- Part 2.3 – Card Edge Commands

- We chose to implement at the card edge command level as this is a natural separation between the card and the software. Thus any PIV card can be used, without any vendor drivers or middleware.

Smartcard Applications

- Web browsers
  - Netscape, Mozilla, Firefox – Security plug-in is a PKCS #11 shared library or DLL.
- OpenSSH
  - Modifications available on mailing list to use PKCS #11
  - Could just use keys, without the certificates
- Kerberos
  - Use PKINIT to get initial Kerberos Ticket
  - Can be done at login using pam_krb5
- Globus
  - Needs a way to call PKCS #11 – it had one in 2000.

Our Test Environment

- Ubuntu/Debian Linux
- OpenSC daily snapshots and libp11 and engine_pkcs11
  - http://www.opensc-project.org
- Pcsc-lite-1.3.0 and ccid-1.0.0 or newer
  - http://pcsclite.alioth.debian.org
- Heimdal Kerberos 0.8.1 or snapshots
  - http://www.pdc.kth.se/heimdal
- MIT & University of Michigan PKINIT changes
- Pam_krb5-3.5
  - http://www.eyrie.org/~eagle/software/pam-krb5/readme.html
- Windows 2003 Active Directory with Enterprise CA
- Other test environments
  - Mac OS 10.4
  - Solaris 9 and 10

PIV Test Cards

- Beta cards from Obethur, Mobile Mind and GemPlus
- Some protect the certificate with the PIN
  - NIST 800-73-1 has lifted this restriction
- OpenSC used to initialize the test cards
  - Every vendor’s cards are a little different
  - Piv-tool used to generate key pair and save public key
  - OpenSSL used to create certificate request
  - Windows enterprise CA to issue enterprise certificate
    - *Cut-and-paste request on Web form*
    - *Save certificate as file*
  - Piv-tool used to load certificate on card
  - Piv-tool used to change PIN

What can you do with existing environments

- Use Windows AD with enterprise certificates
  - Argonne has a site wide Windows Active Directory with all employees
  - We have a smart card project with people around the site using cards
- Use Windows AD with cross-realm to existing Kerberos infrastructure
- Use the Heimdal KDC, but it is still under development
- Wait for MIT and Apple to add KDC support for PKINIT

- In any case, the full PKI infrastructure is not available today
- So start testing so you are ready

Conclusion

- Commercial vendors will take care of 95% of the market
  - Both client and server side
- Open source operating systems can use PIV cards
- Code has been developed that will be widely distributed
  - OpenSC is packaged for Debian and Red Hat
- Open source clients can use commercial servers
  - Standards
- For web users, that’s all that is needed
- For Kerberos authentication, PKINIT client code is still under development
- You can state testing today

Questions

- deengert@anl.gov