Kerberos at Penn

Shumon Huque
University of Pennsylvania

Kerberos Conference, October 27th 2010
Massachusetts Institute of Technology
Cambridge, Massachusetts, USA

University *of* Pennsylvania

- Founded 1740, Philadelphia, PA
- 24,000 students, 4,000 faculty, 12,000 staff
- 50,000 IP addresses in use
- Some central and many decentralized IT units

Kerberos Deployment

- Initial deployment: 2000 through 2002
  - Replaced legacy homegrown system
- Campus-wide KDCs: MIT Kerberos 1.5.x
- Many departmental windows servers do (1-way) cross realm authentication
- Custom IDM/account management tools

Penn
UNIVERSITY *of* PENNSYLVANIA

Native Kerberos vs. Password Verification

- We’ve spent a significant amount of time and energy trying to influence large scale use of native Kerberos authentication.
- Some successes but numerous failures. It’s difficult to do this in an environment of **heteregenous**, **unmanaged** computers.
- A number of application protocols (and their popular implementations) still don’t have good support for Kerberos.

Intermediate systems

- RADIUS
  - primarily to support 802.1x EAP-TTLS-PAP
- Web Single-SignOn: CoSign (UMich)
- Federation: Shibboleth (via CoSign)
- Authenticated LDAP
  - This is for authenticated access to our online directory. We strongly discourage using this for application authentication.

Kerberos for the Web

- Made several attempts in this area over the years, but has still not gained (much) traction
- SPNEGO/HTTP Negotiate (+ SSL for channel protection)
- KX.509 (from Univ of Michigan) - Kerberos to short term X.509 credentials
- Need: widespread support and adoption; official IETF standards

Multi-factor

- Investigated and piloted (no production):
  - CRYPTOcard
  - RSA SecurID
- Integration options:
  - Kerberos pre-authentication step
  - 2nd input to web SSO systems

Authorization systems

- Kerberos: authentication only
- Applications need to consult separate authz infrastructure (ours is based on the Internet2 Grouper system)
- Many windows systems also use their usual methods (Authz data/PAC etc) for additional local policies

Near term enhancements

- Upgrade to recent version of MIT code
- Adapt local changes to plug-in framework
- Test FAST (protect AS exch from offline dict attack)
- Incremental propagation
- LDAP back-end & multi-master (investigation)
- Migration -> stronger encryption types

Wants, hopes, desires?

- (Better) Native Kerberos for HTTP
- EAP method (wireless/802.1x authn)
- IPsec (does anyone use/implement KINK, GSS-IKE etc?)
- VoIP (SIP etc)
- Kerberos on mobile devices
- Multi-factor

Questions?

Shumon Huque

shuque@upenn.edu

National Aeronautics and Space Administration

NASA ICAM

Office of the Chief Information Officer

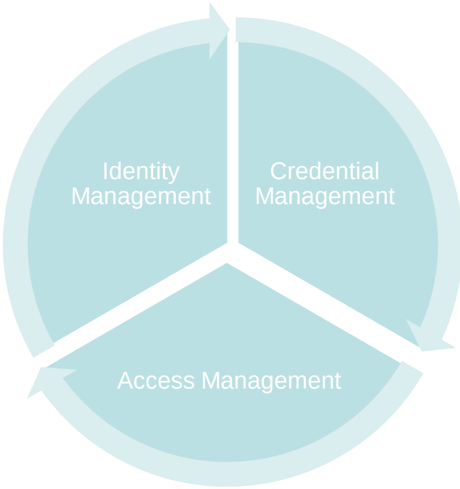
NASA IT Vision: *The NASA IT Organization is the* ***very best*** *in government*

Dennis Taylor

What is ICAM?

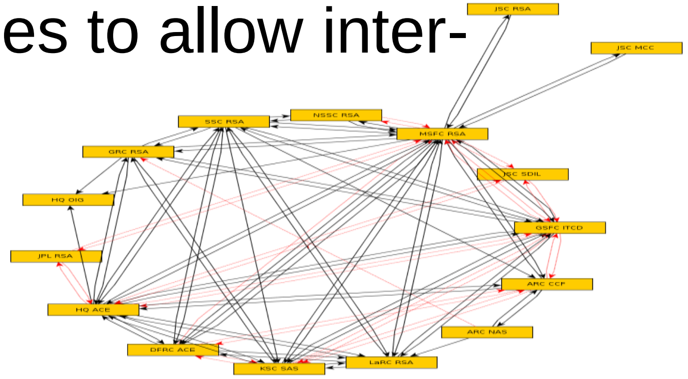
Identity, Credential, and Access Management provide Agency tools to answer these key questions:

- Who are you?
- How do you prove it?
- What can you use?



Before ICAM

- Ten or more implementations each for:
  - » Identity Management
  - » Badge Issuance
  - » RSA Token accounts
  - » Directory Services
  - » More….
- Isolated stovepipes or complex meshes
- Need for paper processes to allow inter-Center collaboration
  - » Slow, laborious



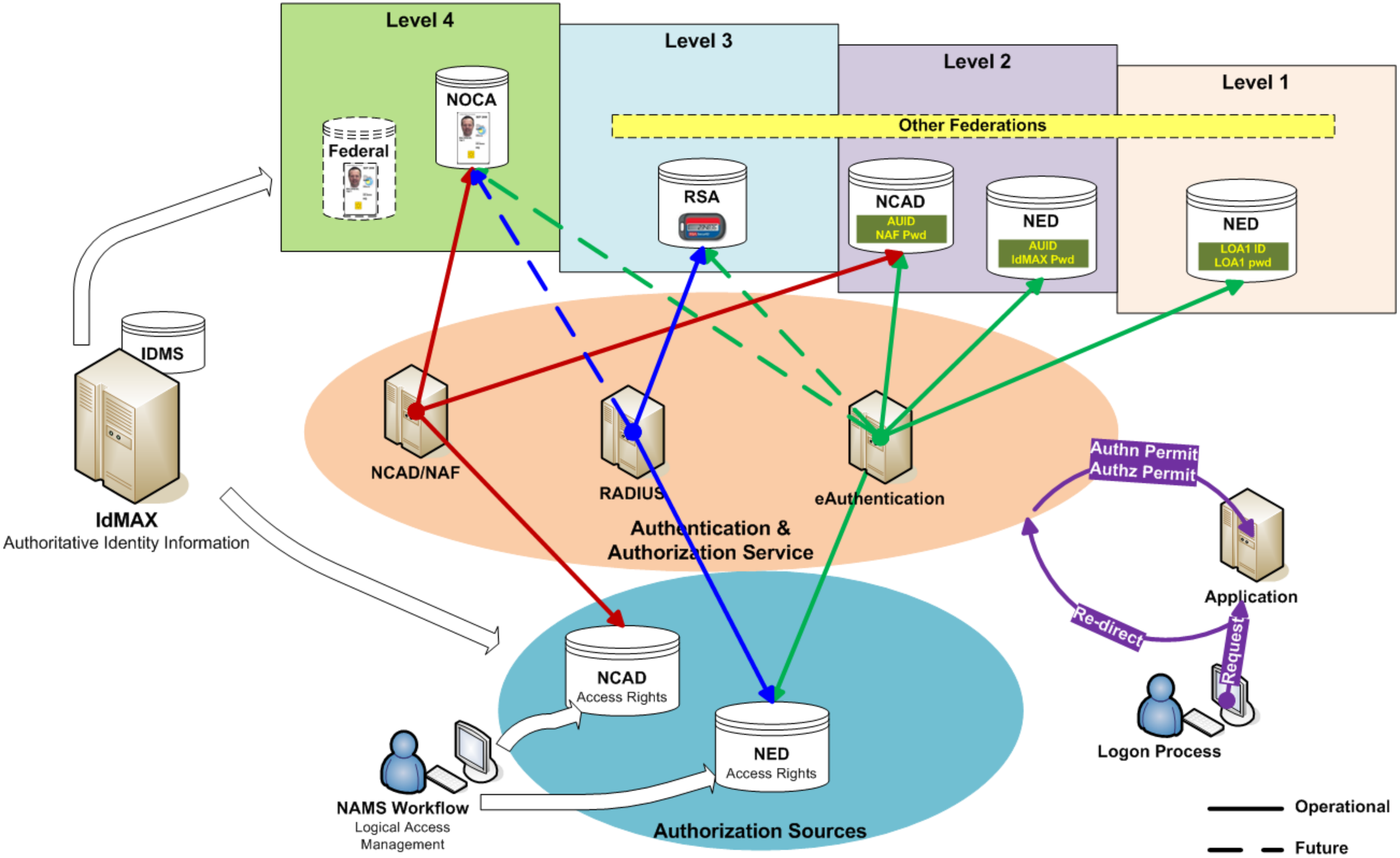
The Consolidation

- **Identity:** A single, authoritative identity store for everyone that does business with NASA
  - » Decommissioned Center x.500s and local identity systems
- **Credential:** A few Agency credentials to access most facilities and systems
  - » We have already retired hundreds of application-unique passwords
- **Physical Access:** An Agency-wide system for all physical access to buildings and rooms
- **Logical Access:**
  - » NASA Account Management System (NAMS) allows access to over 1,000 applications
  - » A single Active Directory forest/domain
  - » The Access Launchpad for access to web applications
  - » Consolidated RSA infrastructure for two-factor access where smartcards cannot be used

The Active Directory Consolidation NCAD

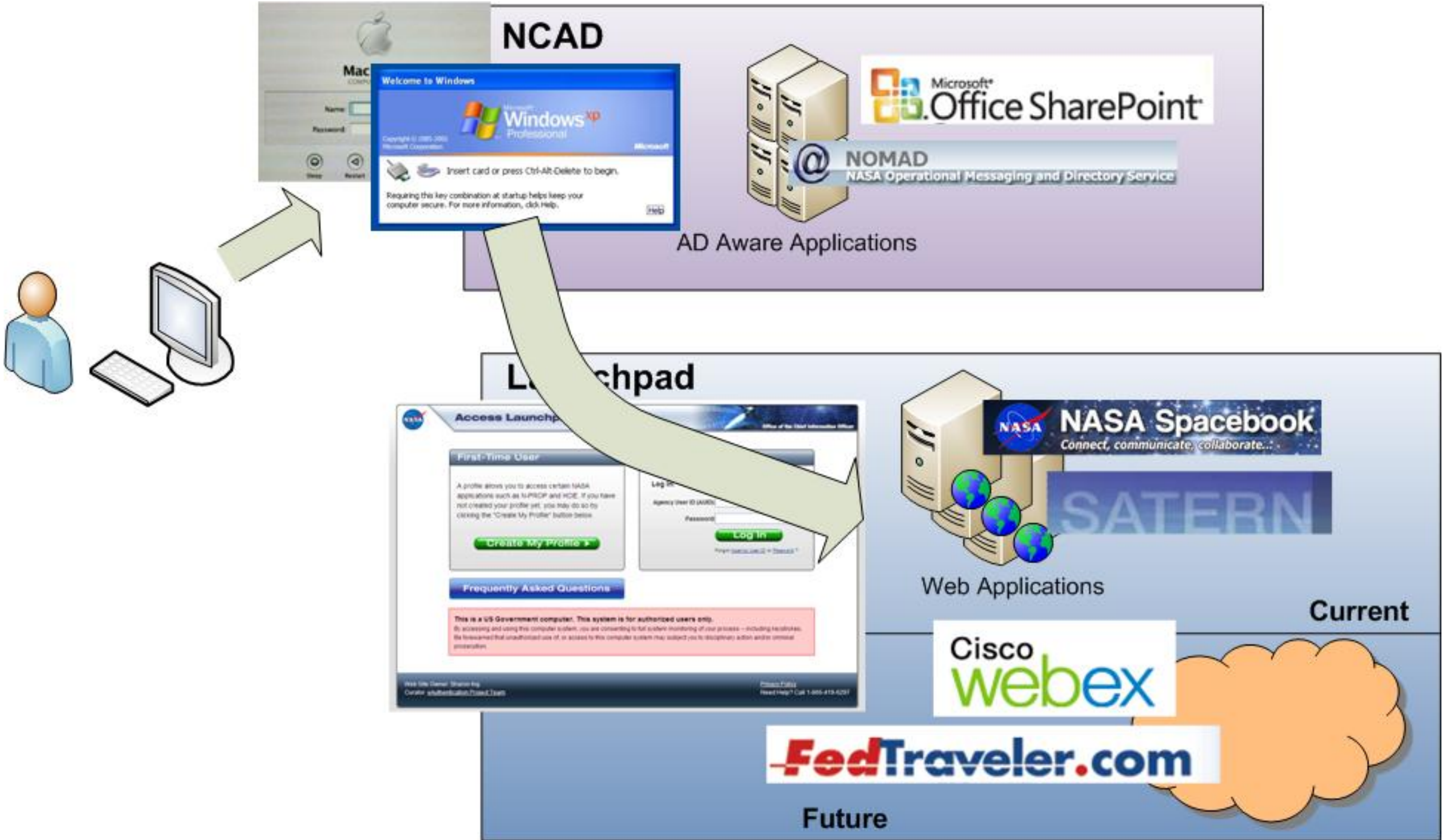
- Single Forest/Single Domain (Single Realm)
- Began in 2006, completed in Summer 2010
- Migrated 57,000 desktops; 66,000 users; 3,700 servers
- Reduced to a single forest, single domain
- Eliminated all 35 two way trusts
  - » Allowing eleven one way trusts (they trust us, we do NOT trust them)
- Replaced hundreds of domain controllers with 69 for the entire Agency
- Reduced an unknown number of AD domain administrators (>100) to eight

ICAM Logical Access Service Description



Integration of NCAD and Launchpad

User’s desktop (Kerberos) login allows pass-through access to any Launchpad application.


NCAD
Mac
Welcome to Windows
Microsoft Windows XP Professional
Copyright © 1985-2001 Microsoft Corporation
Microsoft
Help
Microsoft Office SharePoint
NOMAD
NASA Operational Messaging and Directory Service
AD Aware Applications
Launchpad
Access Launchpad
Office of the Chief Information Officer
First-Time User
Create My Profile ▸
Log In
Agency User ID (AUID)
Password
Log In
Frequently Asked Questions
NASA Spacebook
Connect, communicate, collaborate...
SATERN
Web Applications
Current
Cisco webex
FedTraveler.com
Future

Insert card or press Ctrl-Alt-Delete to begin.

Requiring this key combination at startup helps keep your computer secure. For more information, click Help.

A profile allows you to access certain NASA applications such as N-PROP and HCIE. If you have not created your profile yet, you may do so by clicking the "Create My Profile" button below.

This is a US Government computer. This system is for authorized users only.
By accessing and using this computer system, you are consenting to full system monitoring of your process – including keystrokes. Be forewarned that unauthorized use of, or access to this computer system may subject you to disciplinary action and/or criminal prosecution.

Demo

- Webex demo

Kerberos @ Columbia University

Matt Selsky <selsky@columbia.edu>

10/27/2010

COLUMBIA UNIVERSITY
INFORMATION TECHNOLOGY

History of Kerberos at Columbia

- Kerberos v4 deployed in 1992?
- Kerberos v5 deployed in 1999
- In 2005 ban placed on “insecure protocols”
  - No more telnet/ftp
  - Everything needs SSL or GSSAPI
  - All users required to change their passwords

Basic facts

- 341K principals (was 550K)
  - 80K from current students, faculty & staff
  - Alumni
  - 1400 host/service principals (central IT mostly)
  - Other
- 4 x 1-way trusts from various AD domains
- Many AD domains across campuses
  - No forest
- Running MIT krb5 1.8 on KDCs
  - 7yr old SPARC
  - New x86

Basic facts

- User principals provisioned based on data-feeds from HR, Registrar & departments
- All users have central "UNI" & possibly various AD passwords (might have different usernames)
- Most users use plaintext passwords, not GSSAPI
  - Easy to roll out
- GSSAPI used heavily for server-to-server authn/encryption
  - Cyrus Murder internal communication instead of SSL
- GSSAPI used by a small group of power-users for IMAP, SMTP, SSH, SPNEGO to Subversion

Database Propagation Challenges

- 550K principals + 7 year old hardware -> trouble
- Passwords are only sync'd once/day (in the middle of the night)
- Database dump would be noticeable during the day
- Web authentication process uses kadmind directly to check password age
  - Auditors want 90-day password expiration for Enterprise Applications only
- When the primary KDC is overloaded users notice their password reverting

Database Propagation Mitigation

- Delete 210K principals so dump doesn't take so long
  - Just don't delete that many principals during the day
- Dump/Load is much faster on Linux and newer hardware
- Still kprop'ing once/day
- Will switch to iprop as soon as the KDC migration to Linux is finished

Web Authentication

- Currently
  - Wind (CAS derivative)
    - Allows principal and demographic ACLs
  - Pamacea
    - Allows above + anything supported by .htaccess/.htpasswd
  - Shibboleth
- Next
  - Looking at CAS, Cosign, etc
  - Want to consolidate on single, unified authentication system
  - Must support guests

Other Authentication

- RADIUS
  - Router/switch logins by Network Engineers
  - Dial-up modems
  - VPN concentrators
  - Wireless authentication

AD Interop

- AD supports 4K users of Exchange, filesharing, etc
- CTO declared that passwords must be sync'd between AD and MIT KDC
- MIT fixed realm referral bug for non-member Windows workstations
  - CIFS now works
- Exchange 2010 still doesn't work from non-member workstations for RPC-over-HTTP
  - Might require VPN for all remote Outlook usage. Probably not.
- Looking at krb5-sync instead of having trusts

Recent Improvements

- Upgrade KDCs from MIT krb5 1.6 -> 1.7 -> 1.8
- KDC Master-key rolled and converted from DES to AES-256
- Strong enc-types enabled, but not required
  - Will take affect as users change their passwords
  - Hosts need to be re-keyed

Upcoming

- Campus-wide password change coming in December (maybe)
  - Still deciding if InCommon-Silver strength rules will be required
  - Users will get AES keys
  - Need a backup plan for getting AES keys to users
    - Trojan the Web Authentication stack to re-encrypt their password to AES?
- Need to finish re-keying host/service principals
- Enable preauth for user principals
  - Need to test legacy applications (or just retire them already)
- Upgrade clients to krb5 1.8
- Use RSA tokens for preauth?
- Rekey krbtgt/CC.COLUMBIA.EDU
- Upgrade master KDC to Linux
- Deploy iprop

Kerberos at Oxford

Dominic Hargreaves

MIT Kerberos Conference 2010

Kerberos at Oxford

Overview of the Oxford environment

Where Kerberos fits in

Initial deployment

Where we are now

Challenges and opportunities

Thoughts for the future

Photo http://www.flickr.com/photos/etmeyer/2580402810

The Oxford environment

- 20,000 students, 10,000 staff
- 70 research-active departments
- 38 independent colleges
- 250 administrative units
- … all with their own IT support structures and services
- … and multiple central IT service providers

Our setup

- Migration from accounts and passwords in LDAP
- New webmail software
- Now: 1.8 master, 1.6 slaves
- krb5-sync
- Account provisioning
- End-user principal management
- Service provider service principal management
- WebAuth and Shibboleth
- LDAP authorization/directory

Challenges

- krb5-sync
- Propagation and database locking
- Novell desktop login
- Political: educate and inform IT staff and vendors

Opportunities

- Reduce/eliminate bad old password silos
- Student self-registration

Future

- More cross-realm trusts
- Hardware tokens, multi-factor auth
- New user populations
- Seamless desktop and web SSO
- Identity management
- Central group store