Identity, Credential, and Access Management at NASA, from Zachman to Attributes

Corinne Irwin
Dennis Taylor

VISION: Integrated, secure, and efficient information technology and solutions that support NASA
Agenda

- Based upon a paper that Corinne Irwin and I presented at IDtrust 2009 in April 2009 (*Identity, Credential, and Access Management at NASA, from Zachman to Attributes*)
- EA View
- Active Directory consolidation—authentication source to enable smartcard authentication
- LoA Requirements
Introduction

• NASA includes:
  – 20,000 civil servant employees
  – 80,000 on-site contractors
  – Additional partners world-wide

• NASA’s system/application landscape includes:
  – 3,000 applications, most built in-house
  – Mission control, research labs, product fabrication, more
  – Every flavor of every operating system, hardware, software….

• Historically, NASA has been:
  – Highly decentralized
  – Autonomous Centers with a B-to-B network infrastructure
  – Characterized by weak CIO governance

• HSPD-12 helped us:
  – Implement a robust Identity, Credential, and Access Management Architecture
  – Position NASA for use of ABAC and RBAC
Enterprise Architecture

- Enterprise Architecture (EA) frameworks provide structure for developing complex, integrated systems
- Ideally, one:
  - Develops an As-Is architecture
  - Develops a To-Be architecture
  - Performs gap analysis
  - Develops plan to move toward the To-Be architecture
- NASA used Zachman to develop its ICAM architecture starting in 2006
The Really Big Picture

Implemented Objects

- Community
- Asset Group
- Membership
- Position
- Worker
- Credential
- Investigation
- Access Request
- Access Permission
- Clearance
- Access Control
- Access Point
- Asset

Access Permission Rules

Approved!
ICAM Systems Model
Technology Model
Identity Management

- PIV Request Workflow
- Create Identity Workflow
- FNMS: Foreign National Data
- PDW: Civil Servant Data
- IdMAX: Authoritative Identity Information
- IDMS
- NED: Person Lookup NAMS metadata
Identity and Credential
NCAD—Active Directory Forest and Domain Structure

As-Is Structure

To-Be CDR Structure Supports Migration Activities

To-Be Structure: One Forest One Domain

ndc.nasa.gov
AD Consolidation Summary

- Finally top-down versus grass-roots
- Formal project methodology
  - System Engineering Methodology per NASA NPR 7123
  - Project Management Lifecycle per NASA NPR 7120.7
- Detailed large project plan with linked tasks
  - Project plan maintained by an experienced project scheduler
- Formality in test-set development
  - SIR-TP, SATS, ORTS, all with traceability
- Project Manager experienced in large engineering development; experienced program managers for two major contractors leading effort
- Brought in personnel with experience in similar consolidation efforts at Army, AF, and Navy-Marines
- All eggs in one basket argument…SIEM
LoA Introduction: Tokens
Missing—Capture of LoA on Logon

User A

<User ID>

AS-Req

Using Password

NAF DCs

User B

Smartcard + PIN

AS-Req

PKINIT—using Smartcard

NAF DCs

- PAC- SID-UserA
  SG-Password
  SG-LaunchTeam
  SG-Engineering

- PAC- SID-UserB
  SG-Smartcard
  SG-LaunchTeam
  SG-Engineering
Missing—AuthZ based upon LoA
New Developments Since April
Windows 2008 R2

- Windows domain logon on an XP workstation using password
New Developments Since April
Windows 2008 R2

- Windows domain logon on an XP workstation using smartcard (PIV)

LoA Summary

- We are going to be using a mix of primarily passwords and smartcards for a long time.
- We need our authentication service to provide an LoA attribute to our authorization mechanism.
  - Authorization based upon strength of authentication.
- Our eAuth service (based upon Sun Access Manager) can provide this attribute through SAML like structures.
- We need Microsoft Active Directory to provide a similar functionality in their logon (KINIT, PKINIT) and resultant PAC authorization data.
- We need capability to map particular policy OID to security group.
  - id-fpki-common-authentication means PIV card (only real measure).
VISION: Integrated, secure, and efficient information technology and solutions that support NASA
Conclusions

• A well-developed Enterprise Architecture is essential to ICAM implementation
• NASA must implement Position and Community Management modules in order to support robust ABAC
• Integrated data flow means data is only authoritative at the source, and changes can only occur at the source
• Identity federation and LoA require additional maturity in the market
• Technology is sometimes tricky, but politics is harder!
• Single sign-on is a strong motivator for migration
Use Cases

A Worker with
1. a NASA PIV Card
2. a Federal PIV Card
3. a trusted smartcard
4. a usenid/password
5. an RSA token
6. a NASA-issued PKI soft cert
7. a trusted PKI soft cert
8. a trusted 3rd party credential

To Access
10. a resource on the device being used
11. a desktop/console access
20. an integrated AD application
30. an eAuth-enabled application
40. a resource on a remote device (server)
50. Administrative functions
60. a system that restricts access based on attributes
100. a system that restricts access based on assurance level attributes
110. a RADIUS-enabled application/device
120. an RSA-enabled application/device

Where
10. on the Center Institutional Network
20. on a Mission/Specialized Network
21. on an isolated network
22. on a network with limited connectivity
30. on another Center’s network
40. on the Public Internet

Using
10. a NASA-Managed PC
11. a NAF-bound PC
12. a PC that is not NAF-bound
20. a NASA-Managed Mac
21. a NAF-bound Mac
22. a Mac that is not NAF-bound
30. a NASA-Managed Unix Box
40. a trusted PC
50. a trusted Mac
60. a trusted Unix Box
70. an unknown PC
80. an unknown Mac
90. an unknown Unix Box
100. a NASA-managed PDA
110. a trusted PDA
120. an unknown PDA
130. an unknown IP network device
140. a server
150. a NASA-managed IP network device

When
1. during normal operations (24 x 7 x 365)
2. during a COOP event
3. during a DR event
4. when the network service is unavailable
5. when the validation service is unavailable
6. when the authentication service is unavailable
7. during planned mission/specialized events
8. when the authorization service is unavailable
Future LoA Tokens