SAND2007-5490C

UNITED IN DEFENSE: BATTLING THE NEW THREAT FRONTIER

LOCKHEED MARTIN INFORMATION PROTECTION COUNCIL

SEPTEMBER 11-13, 2007 • ALBUQUERQUE, NEW MEXICO

September 12, 2007

Christopher Nebergall

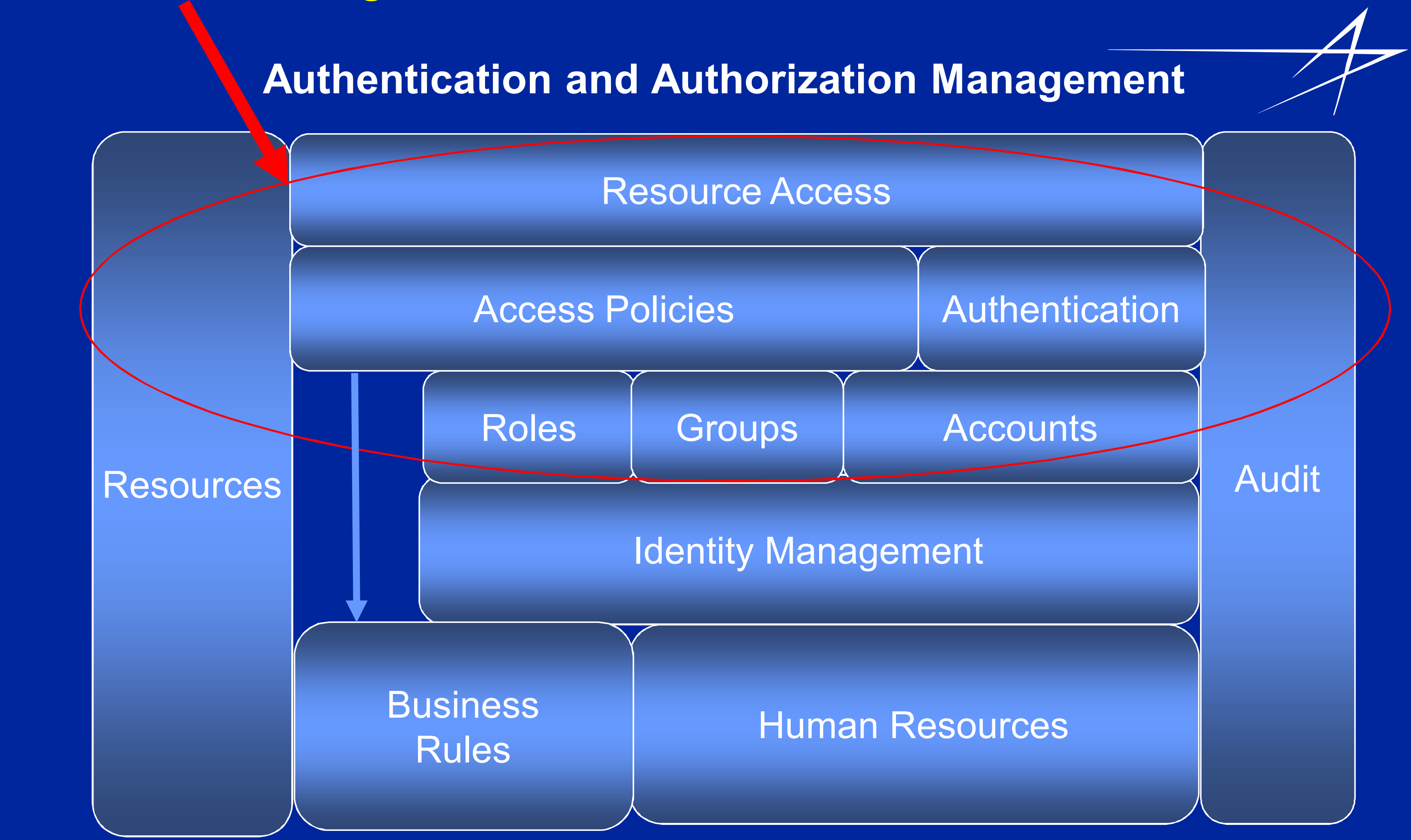
Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company,
for the United States Department of Energy's National Nuclear Security Administration
under contract DE-AC04-94AL85000.

Identity & Access Management
Sandia Experiences

- *Web Access Management and Security*
- *A Look at the Enterprise*
- *Build vs Buy or Both*
- *Why Sun's Access Manager? A History*
- *COTS Solutions - Caveat Emptor*
- *Application Integration - Flexibility Counts*

Web Access Management

Authentication and Authorization Management



A Wide Variety of Web Platforms

- *Sun Web Server 6.1/Sparc Solaris*
- *Weblogic 8.1/9.2 Sparc Solaris*
- *Tomcat 5.5/Sparc Solaris*
- *IIS 6.0/Windows 2003*
- *Apache 1.3 HP-UX Risc*
- *Apache 1.3 - Sparc Solaris*
- *Apache 1.3/2.0 Intel Linux 32/64 bit*
- *Domino 8/Windows 2003*

A Wide Variety of Applications

- ***Oracle Portal***
- ***Oracle - Stellent Content Manager***
- ***MS SharePoint***
- ***MS Outlook Web Access***
- ***Hundreds of in house developed Applications***
- ***Modified Open Source Applications***
- ***Large number of Commercial Off the Shelf (COTS) Applications***

Custom Authentication Everywhere

- ***Windows Integrated Authentication - SPNEGO***
  - ***Browser Compatibility - IE/Firefox/Safari***
- ***Custom Plugin per Web Server***
- ***Very Specific detailed domain knowledge of applications and Web Security Required***

How Well did it Work?

Surprisingly …. Really Well

- *Good Integration with Desktop*
- *Good integration backend File Systems – NTFS, NFS, DFS, etc*
- *Good Security - Kerberos authentication*

What's Missing?

- *Flexible Initial Authentication Methods - 2 Factor Authentication*
- *Browser Independent Single Sign on*
- *SAML Support for Federation with outside Companies*
- *Source Code & API's for updated web service platforms maintained by an outside company and Support Organization*
- *Good Web Service Toolkits*
- *Centralized Authorization*
- *Centralized Logging of Access*

Sun’s Access Manager

- ***Chosen by a competitive selection process of the DOE-NNSA for all of the laboratories and plants in - over a shared private network***
- ***Provides SAML Federated Access and Single Sign on between 12 DOE/NNSA Sites for shared use of web applications***
- ***Central Authentication and Authorization for all web applications at a site***

Build vs Buy or Both
Buy & Customize

- *Heavily customizable COTS Product – more of a toolkit than a complete out of the box solution*
- *Released as the opensso project – for companies and individuals to contribute https://opensso.dev.java.net/*
- *Extensive plugins for different components*
- *Wide variety of Authentication plugins including Windows Integrated authentication/SPNEGO*
- *Open Source Agents – Customize authentication plugins for a Wide Variety of Platforms*

Downside of Sun Access Manager

- *VERY complex to install and maintain*
- *Lack of adequate documentation for customization options*
- *Immaturity in distributed product functionality to support/simplify customization in all the required areas*
- *Complicated products have complicated bugs – slow turn around on fixes*
- *Working on Kerberos Integration for file system support which was lost with move away from SPNEGO*
- *OWA Access, SharePoint Support lacking out of the box*

COTS Product Security – Caveat Emptor

- *Understand web security – Lock down configuration guides not always provided and usually not even standard practice*
- *Domain Cookies - Everything in our network is not trusted at the same level!*
- *Professional Services Installs – Not secure*
- *Test the vendor's security*

Application Integration

- ***Provides security API's which allow developers to integrate SSO into new apps/platforms quickly***
- ***Provides directory information directly to the application through HTTP Headers: email address, phone number, groups, roles, etc***
- ***Future: Provide Fine grained access control using GET/POST Variables***

Flexibility is Important

- *Ability to quickly create plugins for new systems and extend authentication abilities*
- *Do NOT rely solely on professional services for product installs*
- *In house expertise still required for success*
- *Security is still lacking in this market*