SAND2009-2975C

An Enhanced Approach to Using Virtual Directories for Protecting Sensitive Information

May 6th, 2009

Bill Claycomb
Systems Analyst
Sandia National Laboratories
Albuquerque, New Mexico, USA

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.

Agenda

- Directory services and virtual directories
- Threats to directory services
- Protecting information in directory services
- Previous approaches
- A new approach
- Analysis
- Testing/implementation and discussion

Sandia National Laboratories

Directory Services

- Localized data store containing information about objects
  - Users
  - Computers
  - Contacts, etc.
- Provide information to applications
  - Authentication and access control
  - Contact information
  - Group membership
- Use LDAP Communication Protocol
  - *Lightweight Directory Access Protocol*

Directory Services Data

Object

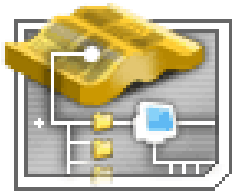
Attribute

dn: cn=Joe User,dc=somedomain,dc=com
cn: Joe User
givenName: Joe
sn: User
telephoneNumber: 1 505 555 1212
postalAddress: 123 Main St.
mail: juser@somedomain.com
objectClass: inetOrgPerson
objectClass: organizationalPerson
objectClass: person
objectClass: top

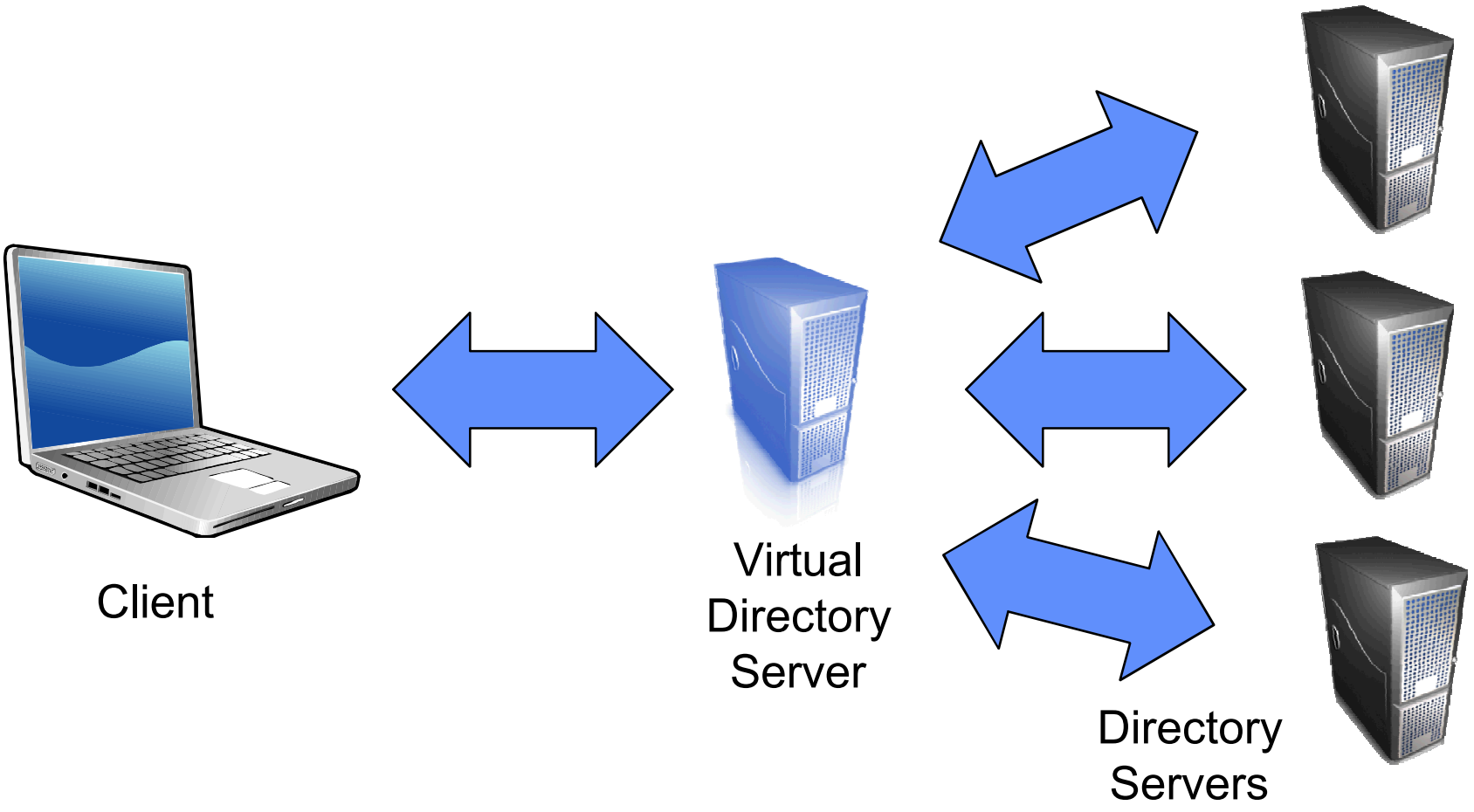
Sandia National Laboratories

Directory Services

- **Popular Directory Services Implementations**
  - **Windows Server *Active Directory***
  - **IBM *Tivoli***
  - **Apple *Open Directory***
  - ***OpenLDAP***
  - **Fedora *Directory Server***
  - **Sun JAVA System *Directory Server***



Virtual Directories



Sensitive Directory Information

Sensitive information in a *directory*?

- **Needed for certain applications**
- **Needed to meet security guidelines such as "*need-to-know*"**

- **What is "*sensitive information*," anyway?**

Sandia National Laboratories

Threats to Sensitive Directory Information

- Data Theft
  - Ordinary users who may have access
    - Insider Threat
  - Administrative users who can grant themselves access
    - Administrator Threat
- Data Manipulation
  - Administrative users carrying out certain types of attacks
- How does an attack happen?

Threats to Sensitive Directory Information

- "Insider Threat Study: Illicit Cyber Activity in the Government Sector", a study conducted by U.S. Secret Service and CERT (2008) found:
  - Most of the insiders had authorized access at the time of their malicious activities
  - Access control gaps facilitated most of the insider incidents, including:
    - The ability of an insider to use technical methods to override access controls without detection
    - System vulnerabilities that allowed technical insiders to use their specialized skills to override access controls without detection

Protecting Sensitive Directory Information

Solutions

- Expose only limited information to external users
- Provide custom virtual directories
  - Relies on user authentication
- Limit access to the existing directory
  - Authentication
  - Access Control Lists
  - Encryption

Sandia National Laboratories

Previous Approach

- Use a modified virtual directory to manage data requests
- Protect sensitive directory information through encryption
- Allow data owner to manage and protect the key
- Provide a method of delegating access to others
- Provide an easy to use interface for users to manage data protection and delegation

Sandia National Laboratories

Previous Approach - Authentication String

$$ID_c \mid \{K_{cv} \mid H(pwd_c)\}_{K_v}$$

- ID_c – **Client username**
- K_{cv} – **Symmetric key between client and virtual directory server**
- pwd_c – **Client password**
- K_v – **Virtual directory key**

Previous Approach - Data in the Directory

$$\{data \mid H(pwd_o) \mid ACL\}_{K_{cv}}$$

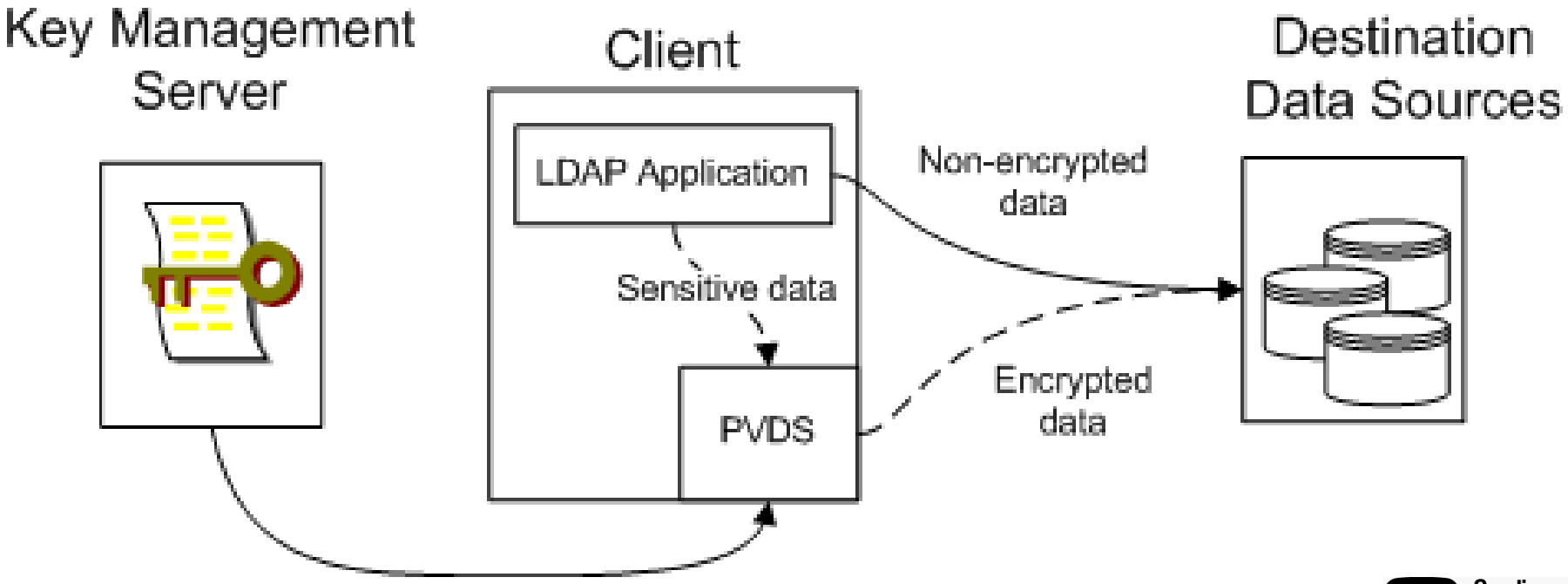
- $data$ – **Plaintext data to store**
- pwd_o – **Data owner password**
- ACL – **Data access control list**
- K_{cv} – **Symmetric key between client and virtual directory server**

A New Approach

- Personal Virtual Directory Service
- Move from centralized role to distributed role for data protection

Modifying the Enterprise

- **Add interaction with existing architecture**
  - **Key Management Services (KMS)**



Sandia National Laboratories

Components of PVDS

- Key Management Infrastructure
- Client Modifications
- Delegating Access
- Protecting the Data

Sandia National Laboratories

Client Modification - Authentication String

- **Previous approach**

$$ID_c \mid \{K_{cv} \mid H(pwd_c)\}_{K_v}$$

- **New approach**

$$ID_c \mid dest_{LDAP}$$

Delegating Access - Data in the Directory

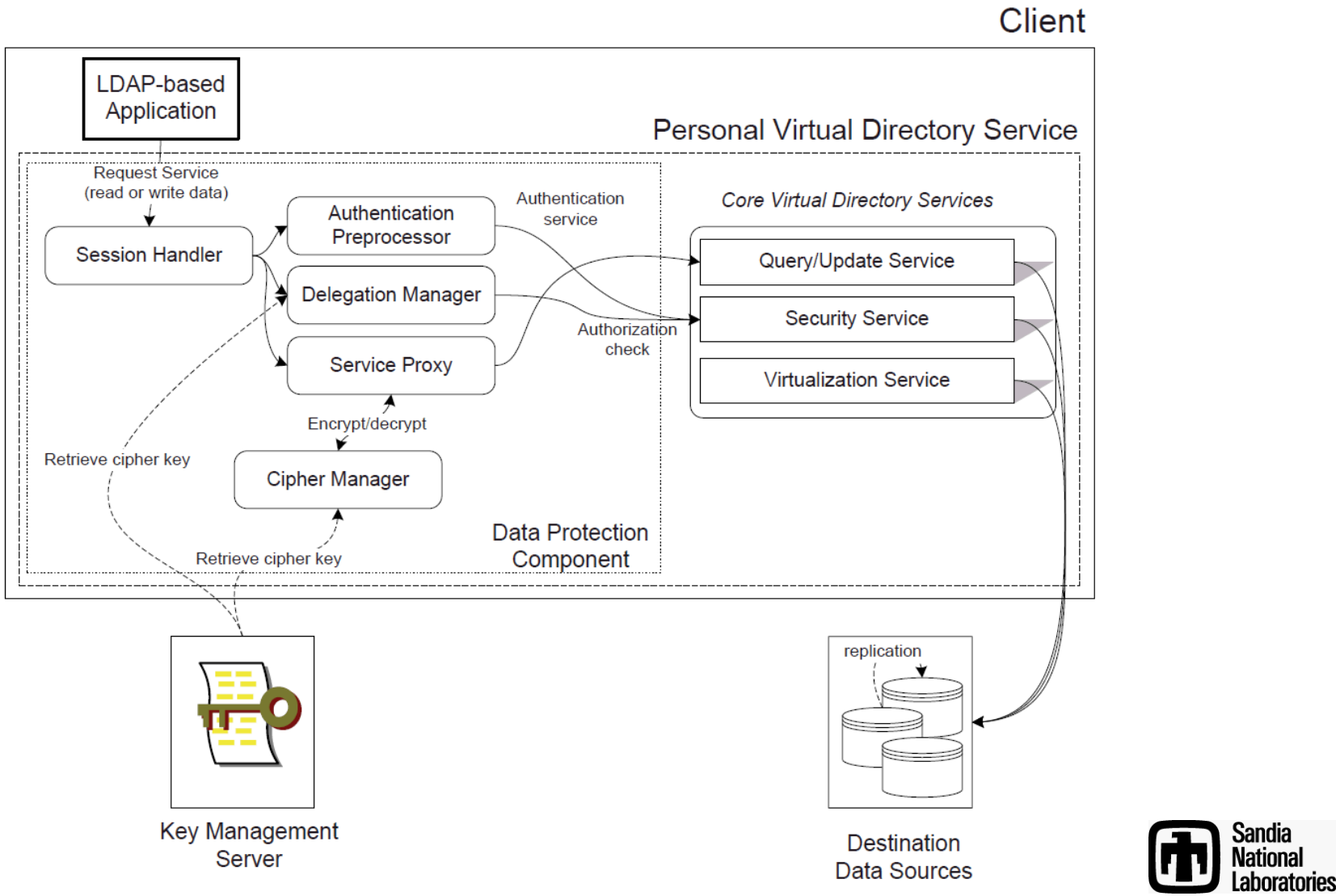
- **Previous Approach**

$$\{data \mid H(pwd_o) \mid ACL\}_{K_{cv}}$$

- **New Approach**

$$\{\{data\}_S\}_{K'_{rw}} \| \{K_{rw}\}_{K'_o} \| ID_o \| \{S, K'_{rw}\}_{K_o} \| \{S, K'_{rw}\}_{K_{u1}} \| \{S, \phi\}_{K_{u2}} \| \ldots$$

Personal Virtual Directory Service Components



Sandia National Laboratories

Advantages of PVDS

- Uses existing key management infrastructure
- Little client modification
- No user-based key protection
- Directory independent
  - Can be extended to protect databases as well

Sandia National Laboratories

Attack Models

- Compromising a client machine
- Impersonation
  - Requires attack on KMS

Testing Results

- **Average attribute access time**

Configuration	Time (ms)
No PVDS – no encryption	5.5
PVDS – not encrypting	8.0
PVDS – 4% of attributes protected	12.6

Testing Results

- **Directory Size on disk**

Configuration	Beginning size (MB)	Final size (MB)
PVDS – no encryption	6.3	56.6
PVDS – 4% of attributes encrypted	6.3	89.9

Future Directions

- Reduce the impact of working with encrypted attributes
  - Time
  - Disk space
- Analyze impact to different types of data sources
- Consider how security policies may conflict with using a virtual directory to manage security
- Analyze attacks on KMS
- Usability studies

Questions

http://www.sandia.gov

wrclayc@sandia.gov

Sandia National Laboratories