SAND2010-6819C

Detecting Insider Activity Using Enhanced Directory Virtualization

October 8, 2010

William R. Claycomb
Member of Technical Staff
Sandia National Laboratories

Dongwan Shin
Associate Professor
New Mexico Tech

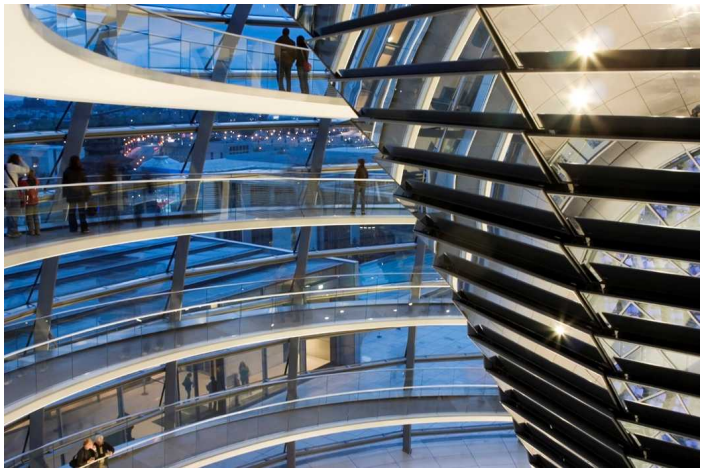
Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

Agenda

- Background on Insider Threats
- Background on Directory Services
  - Directory Virtualization
- Enhancing Directory Virtualization
- Implementation Examples
- Primary Contributions
- Future Work

Insider Threats

- "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:



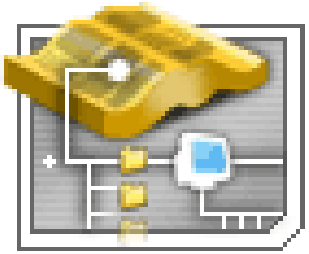
- The ability of an insider to use technical methods to override access controls without detection
- System vulnerabilities that allowed technical insiders to use their specialized skills to override access controls without detection

Sandia National Laboratories

Agenda

- Background on Insider Threats
- **Background on Directory Services**
  - **Directory Virtualization**
- Enhancing Directory Virtualization
- Implementation Examples
- Primary Contributions
- Future Work

Sandia National Laboratories

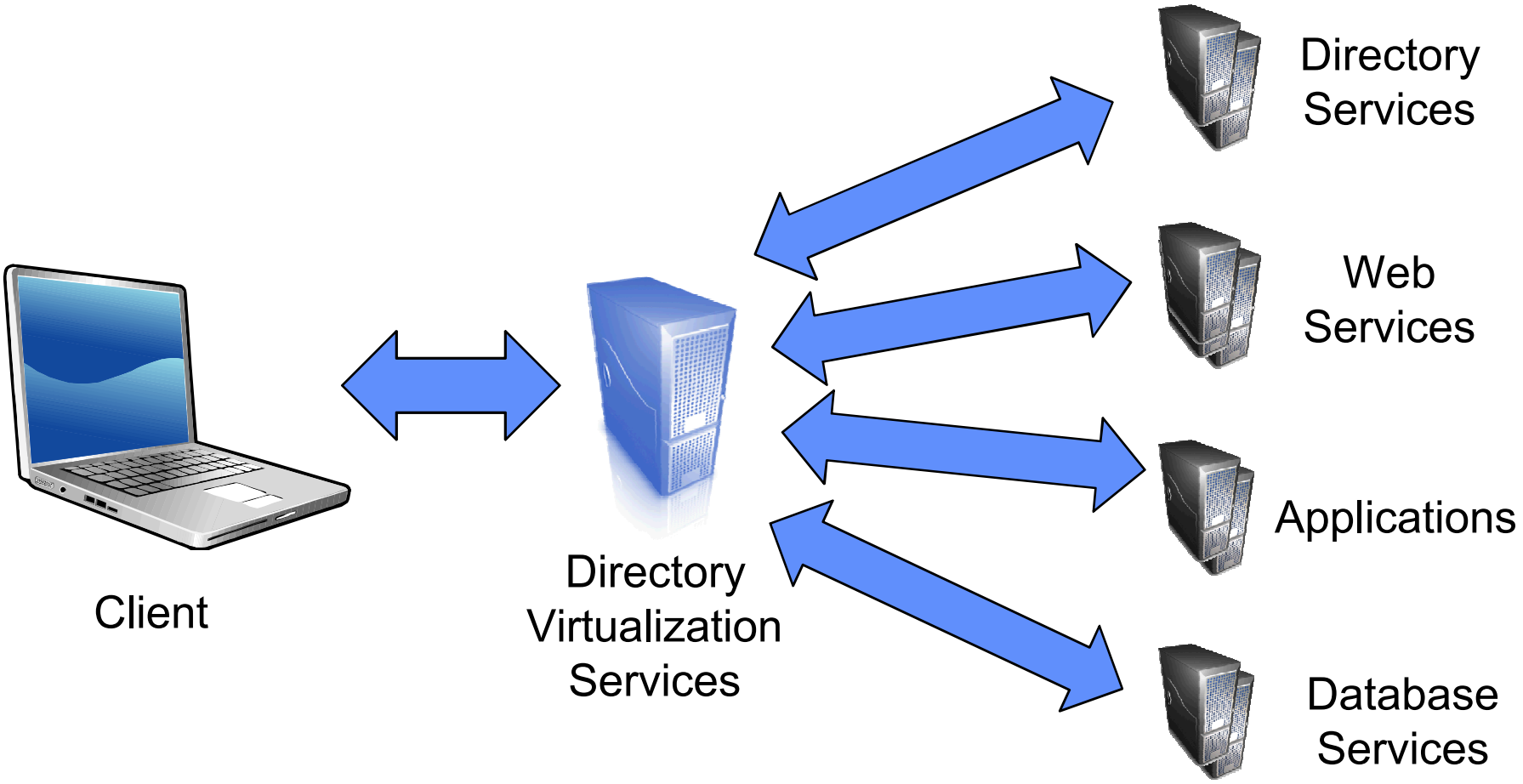


Directory Services

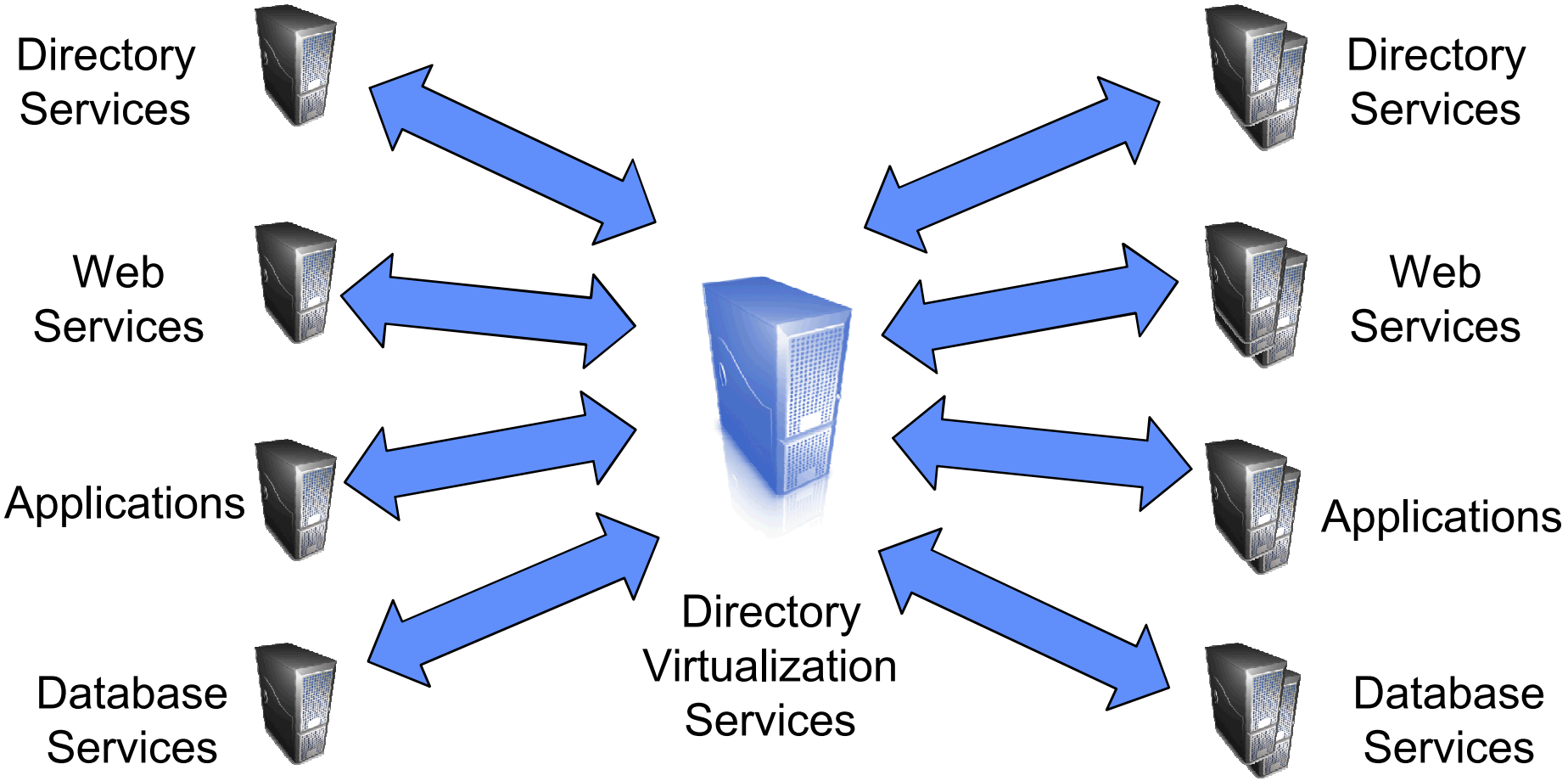
- Localized data store containing information about objects (Users, Computers, Contacts, etc.)
- Provide information to applications
  - Authentication and access control
  - Contact information
  - Group membership
- Popular Directory Services Implementations
  - Windows Server *Active Directory*
  - IBM *Tivoli*
  - *OpenLDAP*
  - Fedora *Directory Server*
  - Sun JAVA System *Directory Server*

Sandia National Laboratories

Directory Virtualization



Directory Virtualization and Synchronization



Attacks on Directory Services

- Create a new user
  - Allows insider to impersonate another account, rather than using her own
- Change group membership
  - Modify ACL to gain unauthorized access to protected resources
- Reset user password
  - Allows insider to masquerade as an existing user
  - Used to circumvent processes that monitor for unauthorized account creation

Sandia National Laboratories

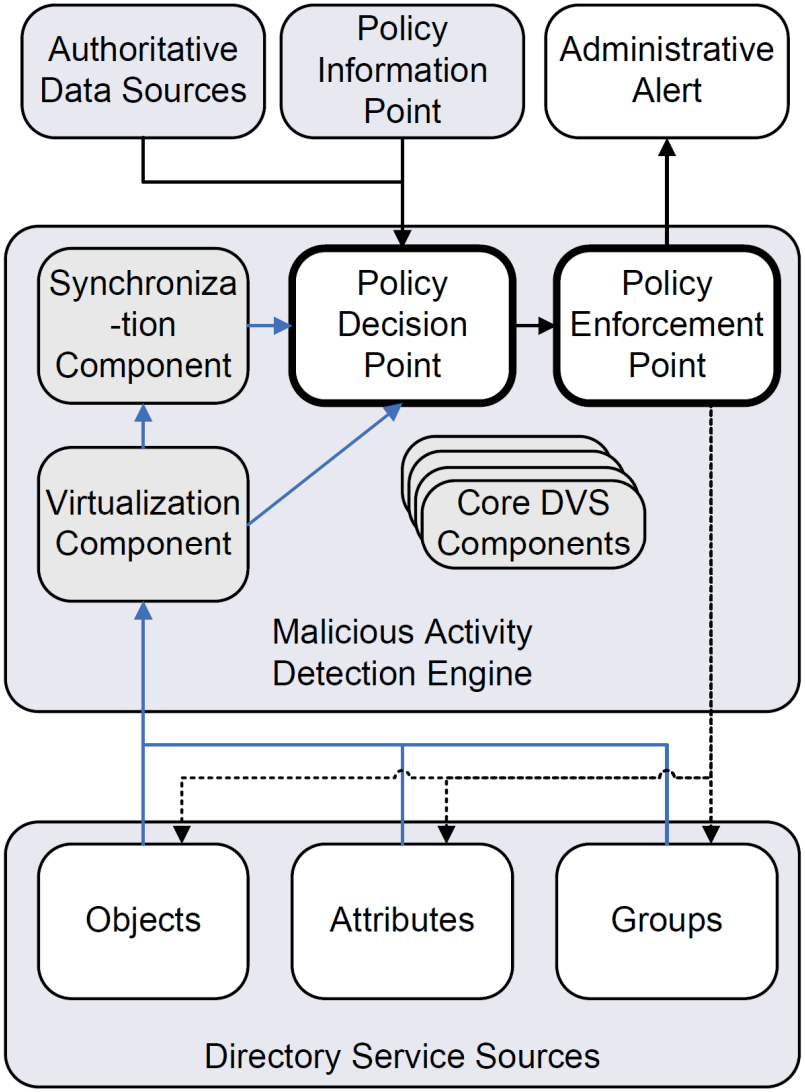
Agenda

- Background on Insider Threats
- Background on Directory Services
  - Directory Virtualization
- **Enhancing Directory Virtualization**
- Implementation Examples
- Primary Contributions
- Future Work

Enhancing Directory Virtualization

- Malicious Activity Detection Engine (MADE)
  - Builds on core components
    - Virtualization
    - Synchronization
  - Adds Policy Components
    - Policy Decision Point (PDP)
    - Policy Information Point (PIP)
    - Policy Enforcement Point (PEP)

Architecture



Sandia National Laboratories

Policy Decision Point

- Detects events
- Obtains policy information from PIP
- Makes determination on activity detected
- Coordinates response using PEP

Modeling the Problem

- **Boolean function describing an account and its relationships with other data sources**

$$s_i \equiv s_j\left(a_1, a_2, \ldots, a_j\right)$$

- $s_j\left(a_1, a_2, \ldots, a_j\right) = 1$ **implies** $a_1 = 1, a_2 = 1, \ldots, a_j = 1$
- **Disjunctive conditions can be included in separate conjunctive states**

Function Conditions

- Variety of possibilities
  - Value (or presence) of a specific attribute on an account
  - Membership of an account in a particular group
  - Relationship between two objects and their attributes
  - Etc.

Example

- **Unauthorized account creation**
  - **Policy:** $s_{new\_acct}(a_X, a_Y, a_Z)$
  - a_X : **presence of account in data source X**
  - a_Y : **"active" status of the account in data source Y**
  - a_Z : **presence of specific training records for the account owner in data source Z**

Agenda

- Background on Insider Threats
- Background on Directory Services
  - Directory Virtualization
- Enhancing Directory Virtualization
- **Implementation Examples**
- Primary Contributions
- Future Work

Implementation: Hypothetical Organization

- DVS implemented with Microsoft Visual Studio
- Directory Services
  - Microsoft Active Directory
  - Sun Java System Directory Server
- Database Services
  - Microsoft SQL
- PIP integrated into DVS
  - Could have been Windows Server Group Policy, etc.
- Tests
  - 15000 user objects
  - 4 domain controllers, 1 SQL database

Implementation: Creating Unauthorized User Accounts

- Insider creates new user to access unauthorized resource
- Policy to prevent such action:

$$s_{auth\_acct}\left(a_{auth\_acct}\right)$$

- Virtualization service monitors directory service for changes, passes events to synchronization service
- Sync service reports new account to PDP
- PDP requests information from auth_acct,
- Applies information to policy retrieved from PIP
- Because $s_{auth\_acct}\left(a_{auth\_acct}\right)=0$, PDP notifies PEP of actions to take, based on information from PIP
- PEP takes appropriate action
  - disable account
  - notify admin

Implementation: Creating Unauthorized User Accounts

- **Test**
  - Use administrative controls to create a new account in directory service
- **Performance**
  - Unauthorized account disabled by MADE within 1 sec of detection

Implementation: Changing Group Membership

- Object attributes often used to make access control decisions
  - Group membership, clearance level, citizenship, organizational status, management level, etc.

Implementation: Changing Group Membership

- **Policy:**

$$s_{group\_membership}\left(a_{auth\_admn}, a_{mbr\_org}, a_{grp\_size}\right)$$

- a_{auth_admn} : **Account is listed as valid domain administrator in** *auth_admin*
- a_{mbr_org} : **Account owner is part of specified organization in a separate data source**
- a_{grp_size} : **Three or less accounts can exist in domain administrators group at any one time**

Sandia National Laboratories

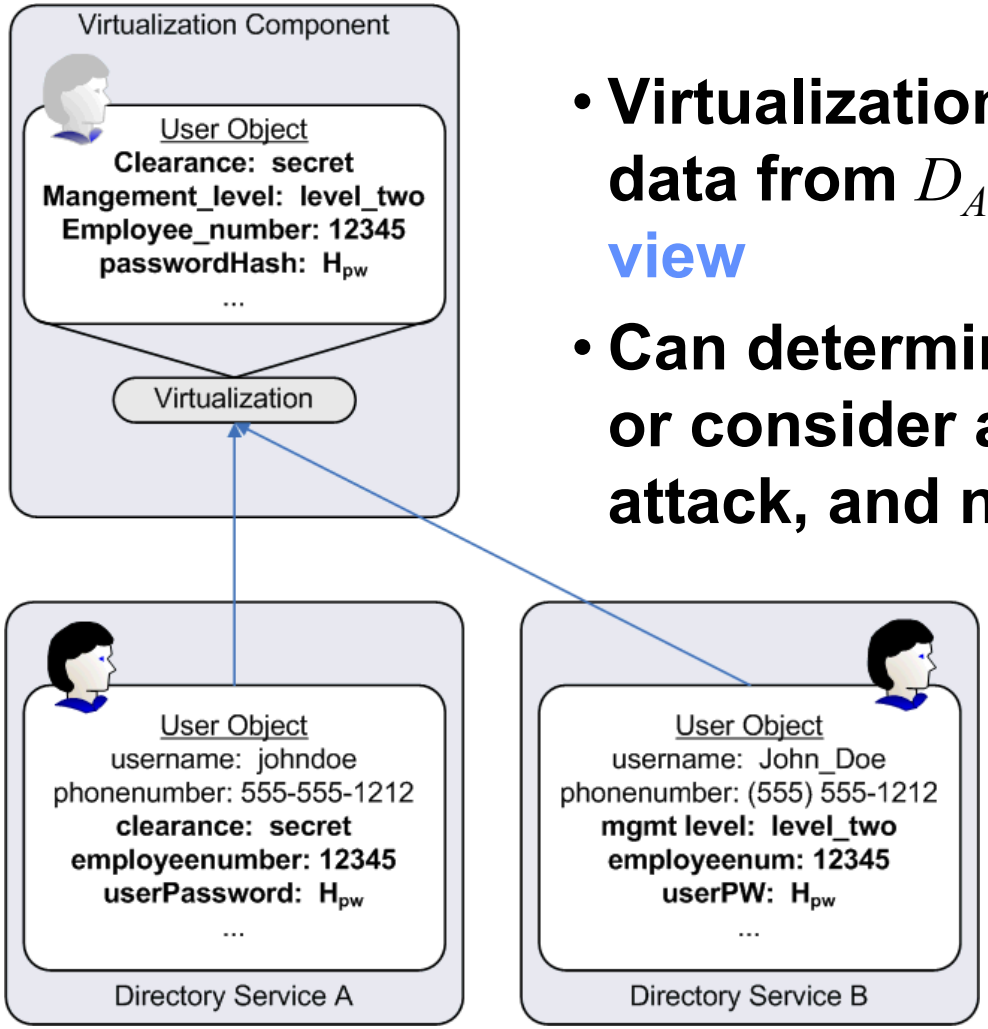
Implementation: Changing Group Membership

- **Attack: Adding an unauthorized account to *Domain Administrators* group**
- **Detection similar to previous example**
- a_{auth_admin} **and** a_{mbr_org} **are determined to be false**
- a_{grp_size} **may also be exceeded**
- **PEP notified to take appropriate action**
- **Interesting to note that policy decision used information from the directory service itself**
  - **Group size**
- **Performance and results similar to previous case**

Implementation: Using Cross-Directory Relationships

- Two different directory services
- Users required to have matching accounts in both directories
  - Directory D_A contains mandatory clearance level information
  - Directory D_B contains mandatory management level information
- Administrators are not allowed to administer both directories simultaneously

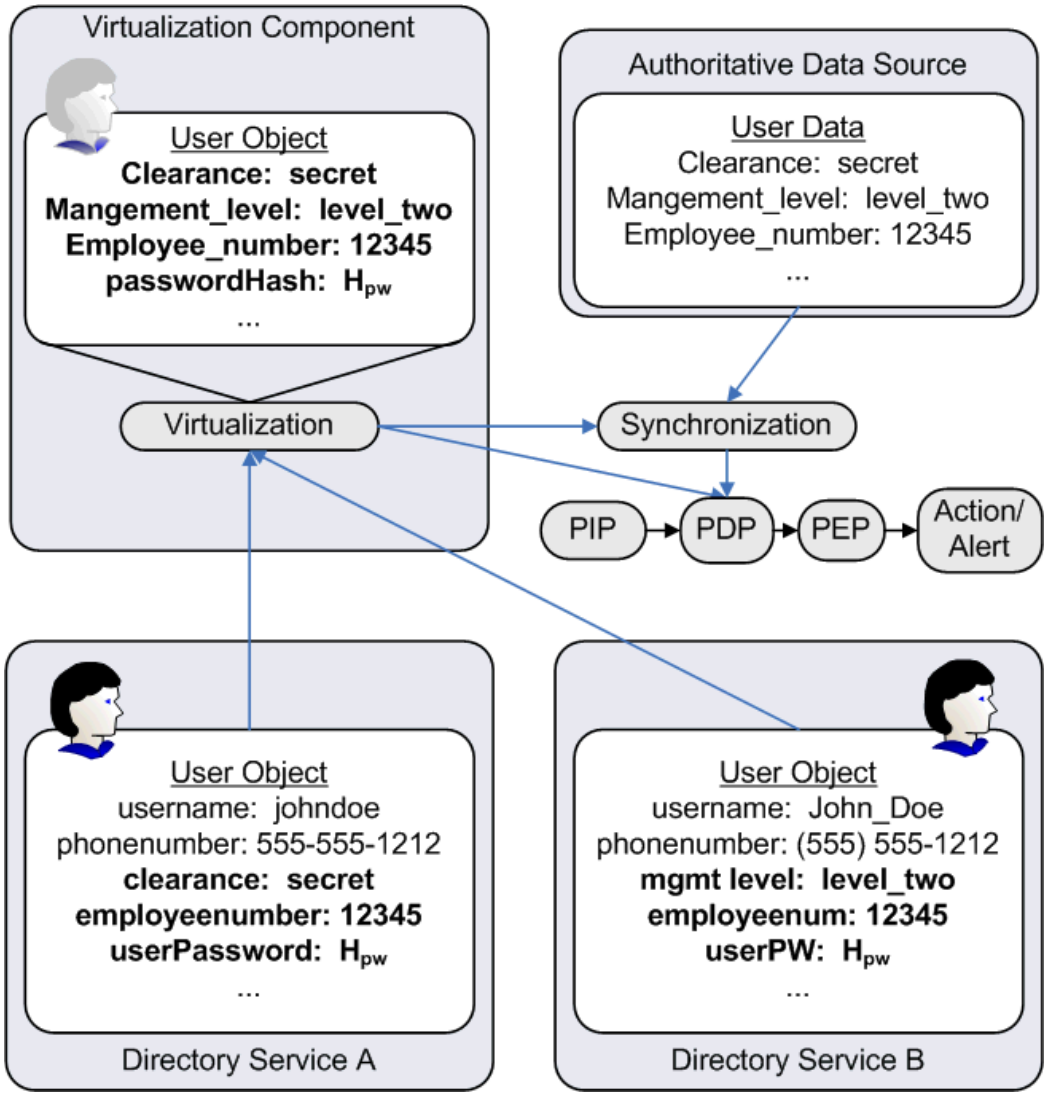
Implementation: Using Cross-Directory Relationships



- **Virtualization component combines data from D_A and D_B to form a single view**
- **Can determine authoritative source, or consider a discrepancy a potential attack, and notify PDP**

Sandia National Laboratories

Implementation:
Using Cross-Directory Relationships



Sandia National Laboratories

Implementation: Using Cross-Directory Relationships

- **Policy:**

$$s_{auth\_acct}\left(a_{clearance}, a_{mgmt\_level}, a_{pwd\_match}\right)$$

- $a_{clearance}$: **presence of correct clearance level**
- a_{mgmt_level} : **presence of correct management level**
- a_{pwd_match} : **synchronization of passwords between domains**

Sandia National Laboratories

Implementation: Using Cross-Directory Relationships

- **Attack: Insider changes a user password in D_A in order to impersonate that account**

- **Performance similar to previous examples**
  - **Detection and enforcement within one second of detection**

Agenda

- Background on Insider Threats
- Background on Directory Services
  - Directory Virtualization
- Enhancing Directory Virtualization
- Implementation Examples
- **Primary Contributions**
- Future Work

Primary Contributions

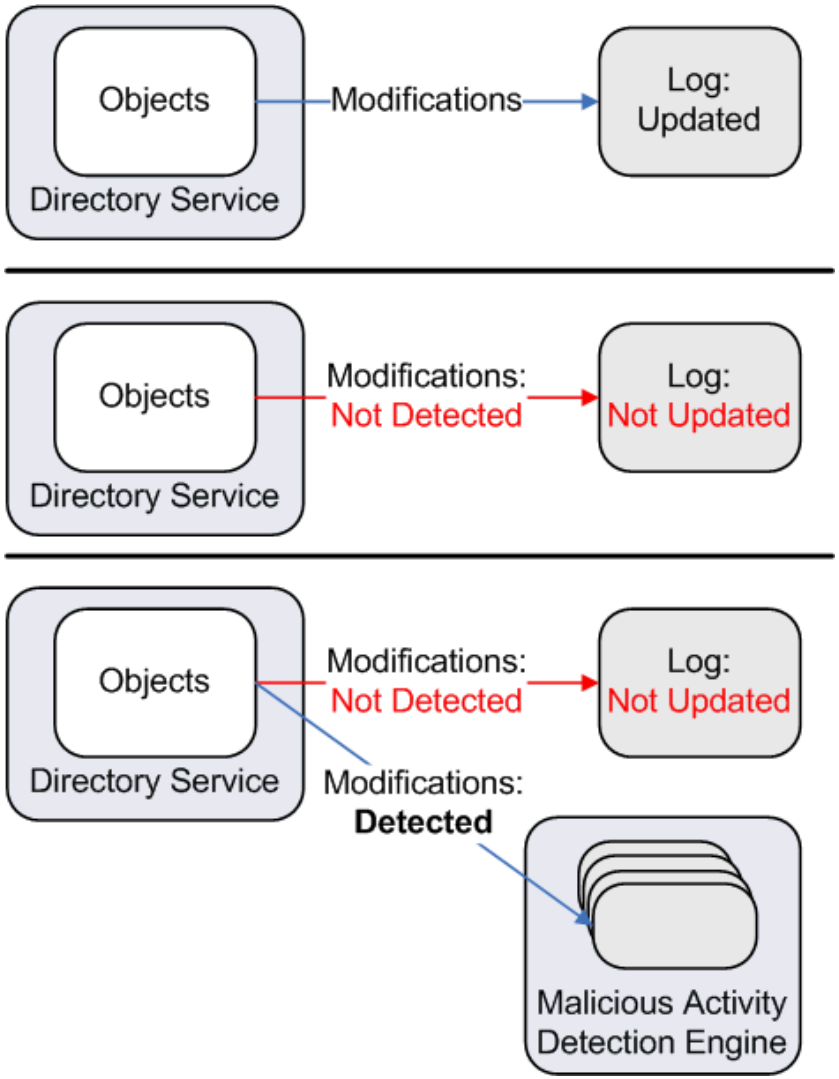
- Monitoring for unauthorized changes is not new
- Adding policy engine in this form is somewhat novel
- Real contribution is the ability to monitor multiple systems simultaneously, and present a consolidated systems view of key data and relationships.
- Insider may be able to modify individual components, but is less likely to be able to modify all monitored components simultaneously

Primary Contributions

- DVS present a lightweight footprint
  - Many DVS may be distributed across the network
  - Makes disabling or defeating them more difficult
- DVS exist outside normal directory services
  - Enhances the chances of detecting a savvy insider
  - Basically a covert channel for directory services

Sandia National Laboratories

Covert Channel



Sandia National Laboratories

Attacks on MADE

- Administrator with control of authoritative data sources
  - Separation of duties
  - Careful monitoring and auditing
- Administrator access to DVS
  - Disable monitoring
  - Makes key changes to specific repositories simultaneously
- Administrator access to administrative applications
  - Makes unauthorized changes appear legitimate
- Administrative access or attacks on PIP or PEP

Future Work

- Additional performance testing under real-world scenarios and in production environments
- Apply MADE to other access control models
- Deployment of many lightweight DVS
- Enhanced interaction with PIP
  - What other systems can be used as PIP
  - How to prevent PIP compromise

Sandia National Laboratories

Questions

http://www.sandia.gov

http://scl.cs.nmt.edu

wrclayc@sandia.gov

doshin@nmt.edu

This work was partially supported at the Secure Computing Laboratory at New Mexico Tech by the grant from the National Science Foundation (NSF-IIS-0916875)

Sandia National Laboratories