
Case Study:

*Using OpenLDAP
for
Physical Access Control*

Terry Neely, PlaSec, Inc.
terry@plasecinc.com

International Conference on LDAP - LDAPCon 2009

Physical access components



Doors & Readers

Weigand
TCP/IP
→



Controllers

TCP/IP
→



Access Control Host

International Conference on LDAP - LDAPCon 2009

Physical Access Control Software



- **Windows/SQL Server based**
- **Proprietary architecture**
- **Interoperability requires coding against vendor specific API**

International Conference on LDAP - LDAPCon 2009

Open Sesame! Network Attack Literally Unlocks Doors

WIRED

LAS VEGAS — Security researchers have spent a lot of time the last couple of years cracking building access systems from the level of the user device — RFID and smartcards, for example.

But a researcher in Texas found that he could crack one electronic access system at the network control level and simply open a door with a spoofed command sent over the network, eliminating the need for an access card. He could do it while bypassing the audit log, so the system wouldn't see that someone opened the door.

The hack is possible because the system uses predictable TCP sequence numbering.

<http://www.wired.com/threatlevel/2009/08/open-sesame/>

International Conference on LDAP - LDAPCon 2009

Contractor indicted for logic bomb

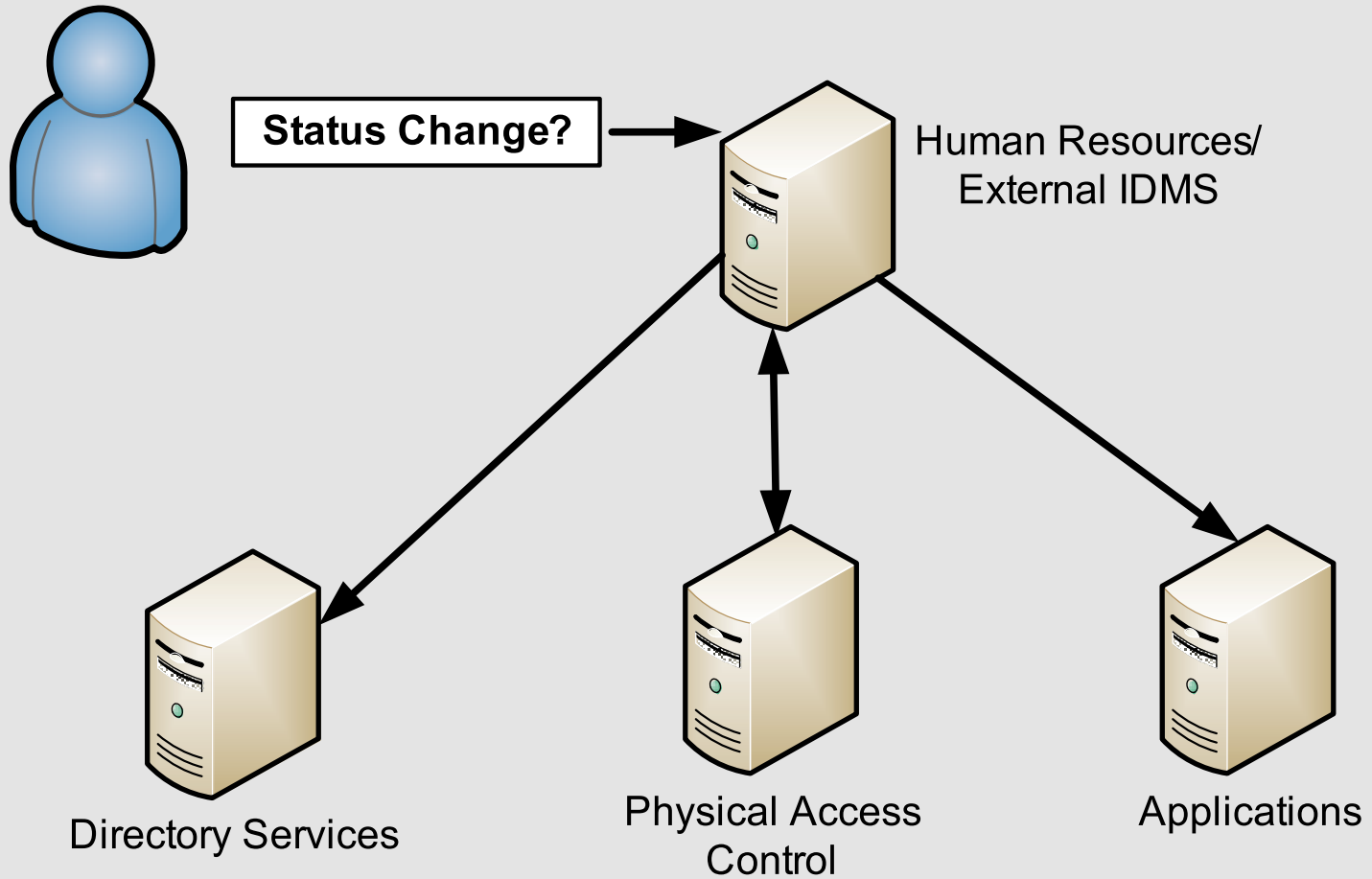


- Rajendrasinh B. Makwana fired Oct 2008
- Planted malicious code after termination
- Badge & laptop returned 3 ½ hours later

<http://finance.yahoo.com/news/Feds-allege-plot-to-destroy-apf-14214374.html>

International Conference on LDAP - LDAPCon 2009

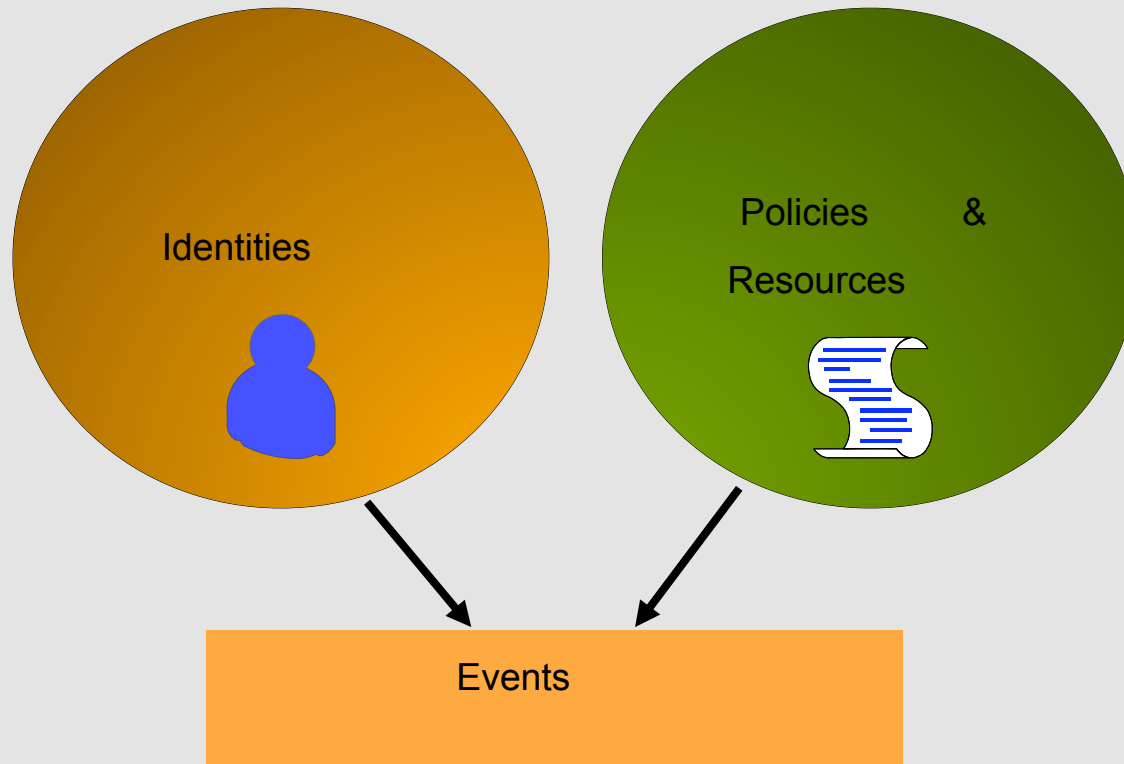
What needed to happen



International Conference on LDAP - LDAPCon 2009

Types of information

Physical Access



International Conference on LDAP - LDAPCon 2009

Data Characteristics



- Traditionally small data set
- Mostly read only with frequent lookups
- Hierarchical data representation
- Multiple geographic sites
- High availability
- Data partitioning

International Conference on LDAP - LDAPCon 2009

Use OpenLDAP as the store

Performance

- Small data set entirely in memory
- ACID properties

Distributed

- Multi-master handles multiple sites
- Mirror mode for high availability

Access

- Natural hierarchy
- Connectors to identity stores
- ACL control data access

International Conference on LDAP - LDAPCon 2009

Provisioning/De-provisioning

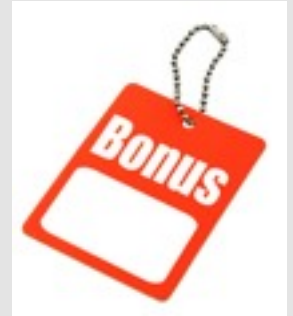
Physical access provisioned with logical

- Leverage existing tools to reach into physical access
- De-provisioning revokes physical access with logical
- Entitlement Management
 - True role based access control
 - Separation of access
 - Temporal and limited roles



International Conference on LDAP - LDAPCon 2009

Benefits using OpenLDAP



- Performance
- ACLs eliminated views and procedures
- Use standard objectclasses
- Schema modifications while running
- Interoperability
- Multi-master replication & mirror mode (no publish/subscribe)

International Conference on LDAP - LDAPCon 2009

Challenges using OpenLDAP

- Learning curve (views, procedures, joins)
- Identities contain photographs
- Badge layouts have graphics and designs
- Biometric templates
- Transactions received from field hardware
- Database transactions

International Conference on LDAP - LDAPCon 2009

Further Info Slide

Terry Neely

11710 Plaza America Drive, Suite 2000, Reston, Va 20190

703-635-7415

terry@plasecinc.com

International Conference on LDAP - LDAPCon 2009