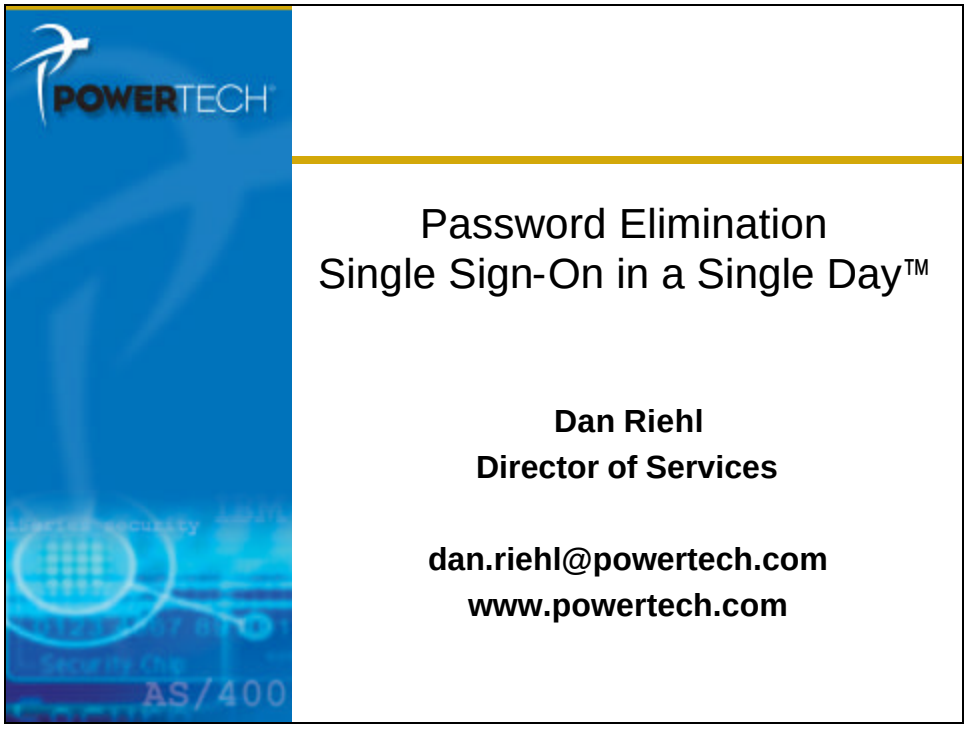


Password Elimination
Single Sign-On in a Single Day™

Dan Riehl
Director of Services

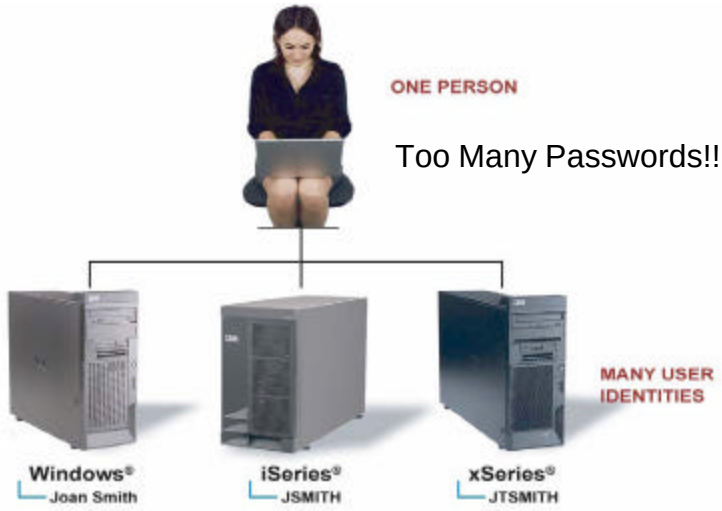
dan.riehl@powertech.com
www.powertech.com

Agenda

- The Password Problem
- Case Study for SSO
- Traditional SSO Approaches
- The Password Elimination approach
  - Kerberos NAS (Network Authentication Service)
  - Enterprise Identity Mapping (EIM)
  - Web Applications with Identity Tokens
- Implementation Overview

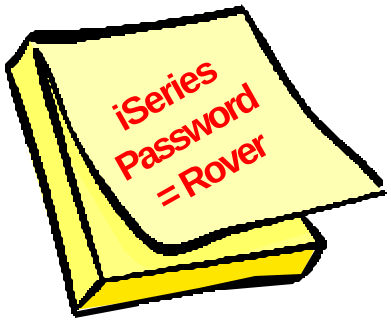
2006 Copyright The PowerTech Group, Inc. All rights reserved

The Problem Defined



2006 Copyright The PowerTech Group, Inc. All rights reserved

The Problem Defined



- Insecure passwords
  - Trivial passwords
  - Users write them down on sticky notes
  - Same password on all systems
  - Passwords expire on different systems at different times

Just how many User IDs and Passwords do YOU have?

2006 Copyright The PowerTech Group, Inc. All rights reserved

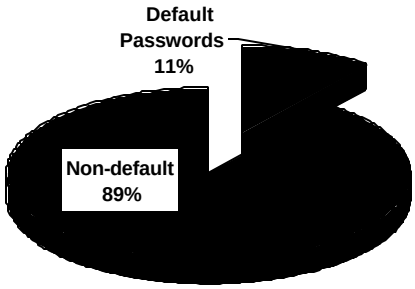
iSeries Password Policy

- No default passwords
  - Password = username
- Enforce strong passwords
  - Minimum password length
    - ✓ QPWDMINLEN = 6
  - Passwords should expire in 60 days
    - ✓ QPWDEXPINTV = 60
  - Password must be different from previous passwords
    - ✓ QPWDRQDDIF = 5 *(last 10)*
  - Require a digit in the password
    - ✓ QPWDRQDDGT = 1

2006 Copyright The PowerTech Group, Inc. All rights reserved

Weak Passwords

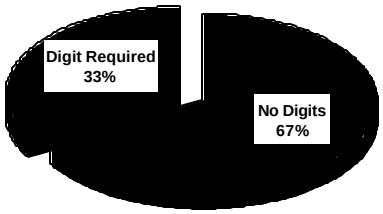
- Most iSeries have weak password rules
  - Average of **90** default passwords per system!
  - 67% of systems don't require a digit in passwords.
  - 64% of systems allow passwords to be the same as previous passwords



2006 Copyright The PowerTech Group, Inc. All rights reserved

Weak Passwords

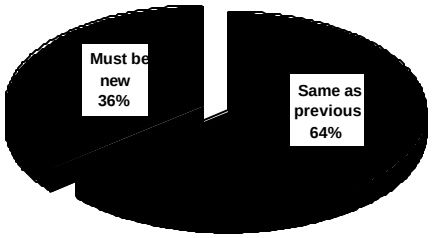
- Most iSeries have weak password rules
  - Average of 90 default passwords per system!
  - **67% of systems don't require a digit in passwords**
  - 64% of systems allow passwords to be the same as previous passwords



2006 Copyright The PowerTech Group, Inc. All rights reserved

Weak Passwords

- Most iSeries have weak password rules
  - Average of 90 default passwords per system!
  - 67% of systems don't require a digit in passwords.
  - **64% of systems allow passwords to be the same as previous passwords**



2006 Copyright The PowerTech Group, Inc. All rights reserved
PowerTech Confidential www.powertech.com info@powertech.com

What is Single Sign-On?

Windows®

Authenticate at first server
No additional sign-on to connect to other trusted systems

2006 Copyright The PowerTech Group, Inc. All rights reserved

Success Story
Conn-Selmer, Inc.

- (NYSE: LVB) The largest U.S. manufacturer and distributor of band and orchestral instruments
- Plants are located worldwide
- Over 1,100 employees
- Environment
  - One iSeries with 400 end users
  - Windows Domain, running Active Directory
  - Using iSeries Access and iSeries Netserver

2006 Copyright The PowerTech Group, Inc. All rights reserved

The Problem

- External SOX Audit
- Needed to enforce regular expiration of passwords
- Had to eliminate the need to maintain passwords on 2 systems the iSeries and Windows Network
  - PC files were stored in the iSeries IFS
  - For Netserver to work without SSO, the iSeries and Windows passwords had to be the same

2006 Copyright The PowerTech Group, Inc. All rights reserved

The Solution

SSO and PowerLock EasyPass

- Up and running with SSO in 5 hours
- Eliminated iSeries passwords from almost all user profiles
  - PASSWORD(*NONE)
- You don't need to expire passwords that don't exist. Problem Solved !!

"Having single sign-on allows us to set Windows password controls to auto-expire, thus forcing the user to change passwords on a regular basis without worrying about keeping both passwords in-sync."

Joseph Shore, Conn -Selmer

2006 Copyright The PowerTech Group, Inc. All rights reserved

SSO Benefits

- **Increase productivity**
  - End users
  - Administrators
  - Programmers
- **Remember ONE strong password**
- **Meet audit requirements**
- **Save money**
  - Less calls to the help desk to reset a password

Gartner Group studies have shown that password reset calls represent 15-35% of all help desk calls at a cost of up to $31 per call

2006 Copyright The PowerTech Group, Inc. All rights reserved

What is Single Sign-On?

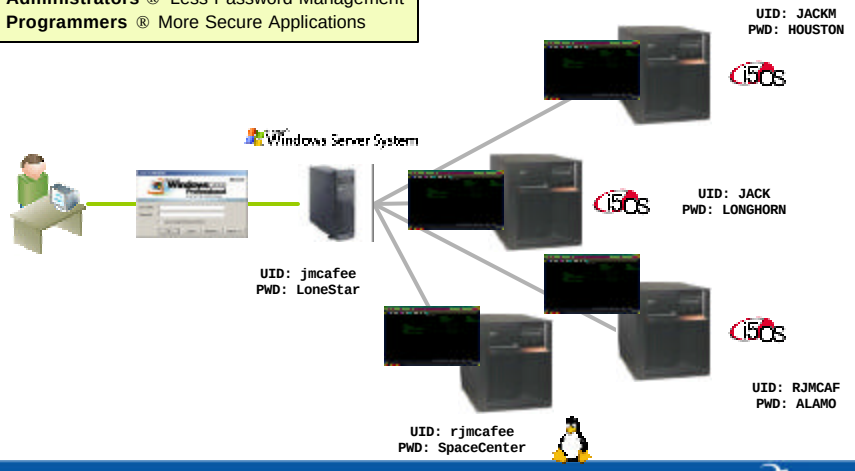
- SSO requires only one password
  - First server you connect to each morning
  - Typically a Windows 2000/2003 domain
- Users require less help desk assistance
  - Password formation rules can be more rigid
  - Easier and faster to reset a password on a single system
  - OS/400 password can be set to *NONE
- SSO simplifies disabling a user
  - Again, there is just one profile to maintain

2006 Copyright The PowerTech Group, Inc. All rights reserved

A "Typical" Configuration

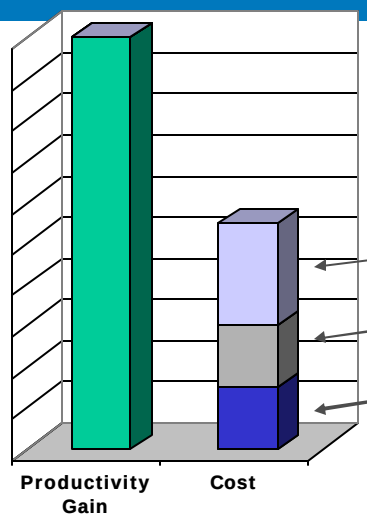
Who Benefits from SSO?

1. **End Users** ® Higher Productivity
2. **Administrators** ® Less Password Management
3. **Programmers** ® More Secure Applications



2006 Copyright The PowerTech Group, Inc. All rights reserved

Measuring SSO ROI



> Productivity Gain > Cost?

> Cost Components:

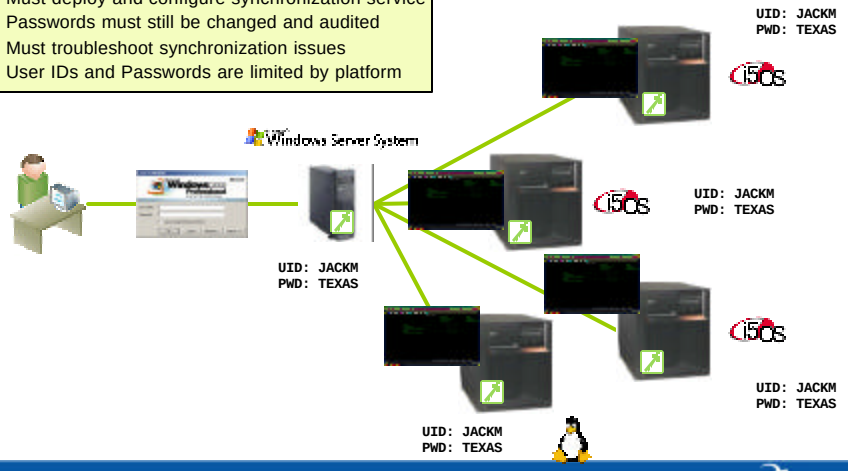
- Management
- Implementation
- Acquisition

2006 Copyright The PowerTech Group, Inc. All rights reserved

Synchronization SSO Approach

User ID/Password Synchronization

- No end user productivity gains *(not really SSO)*
- Must deploy and configure synchronization service
- Passwords must still be changed and audited
- Must troubleshoot synchronization issues
- User IDs and Passwords are limited by platform

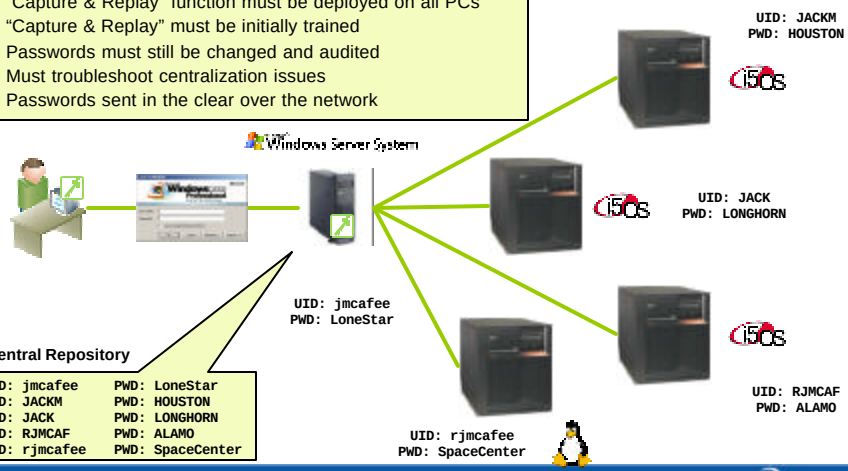


2006 Copyright The PowerTech Group, Inc. All rights reserved

Centralization SSO Approach

User ID/Password Centralization

- End user productivity gains
- "Capture & Replay" function must be deployed on all PCs
- "Capture & Replay" must be initially trained
- Passwords must still be changed and audited
- Must troubleshoot centralization issues
- Passwords sent in the clear over the network



2006 Copyright The PowerTech Group, Inc. All rights reserved

The Password Elimination Approach

Single Sign-On Components

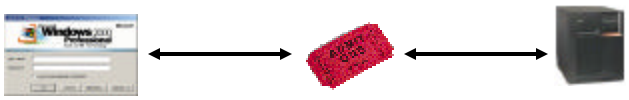
- **Kerberos** for ***authentication***
  - Uses strongly encrypted tickets and not passwords
  - Implemented on all major platforms
- **Enterprise Identity Mapping (EIM)** for ***authorization***
  - Maps people to their user identities on various registries
  - Registry might be a platform, application, or middleware
- **Applications** enabled for Kerberos and EIM
  - IBM has enabled many popular services in V5R2 and i5/OS
  - NetManage has enabled RUMBA 7.4 & OnWeb Web-to-Host 5.2
  - You can also enable your own applications

2006 Copyright The PowerTech Group, Inc. All rights reserved

What is Kerberos?

Kerberos **is an Internet Engineering Task Force (IETF) standard for providing authentication.** ***Kerberos*** **works by having a central server grant an authentication "ticket" honored by networked nodes running** ***Kerberos*****.**

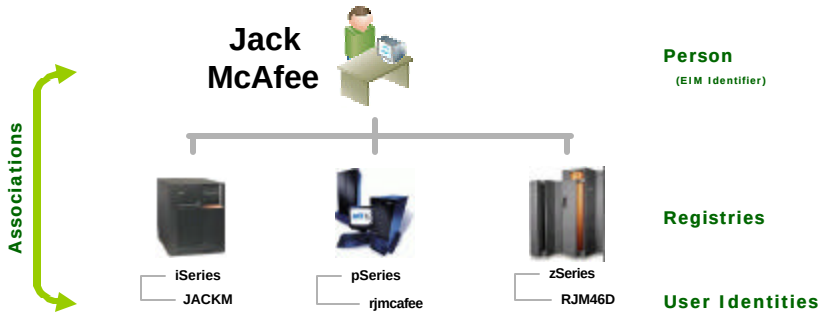
- **RFC 1510 - The Kerberos Network Authentication Service (V5)**
- **Came out of Project Athena at MIT.**
- **Based on Needham/Schroeder's trusted third-party authentication protocol**
- **IBM refers to Kerberos as NAS (Network Authentication Service)**



2006 Copyright The PowerTech Group, Inc. All rights reserved

What is EIM?

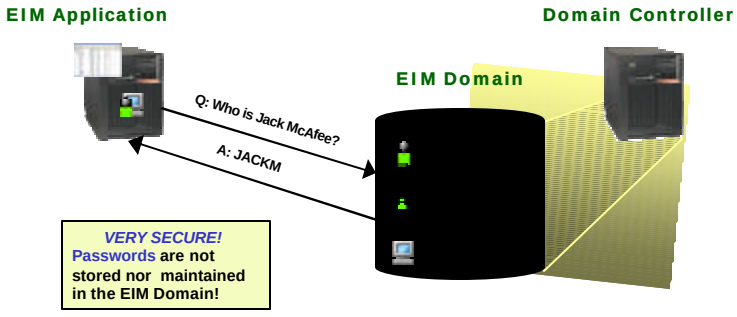
IBM's Enterprise Identity Mapping (EIM) is an infrastructure for associating a unique person with one or more user identities in various registries across the enterprise



2006 Copyright The PowerTech Group, Inc. All rights reserved

Where is the EIM Domain?

- On a Domain Controller in an LDAP directory
- IBM Directory Server offers broad platform support:
  - Windows ® 2000, AIX ®, Solaris ™, and HP-UX™
  - As well as Linux distributions for Intel™, and
  - IBM eServer **iSeries**, pSeries, and zSeries platforms

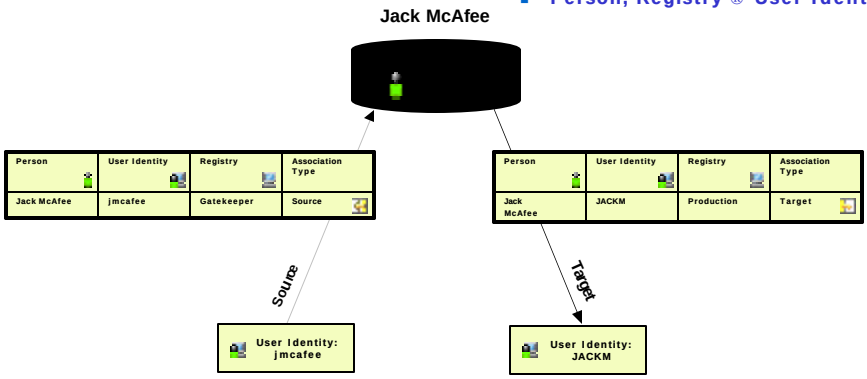


2006 Copyright The PowerTech Group, Inc. All rights reserved

Source and Target Associations

> **Source**
- For initial authentication
- Usually Windows AD Log-On
- **User Identity, Registry ® Person**

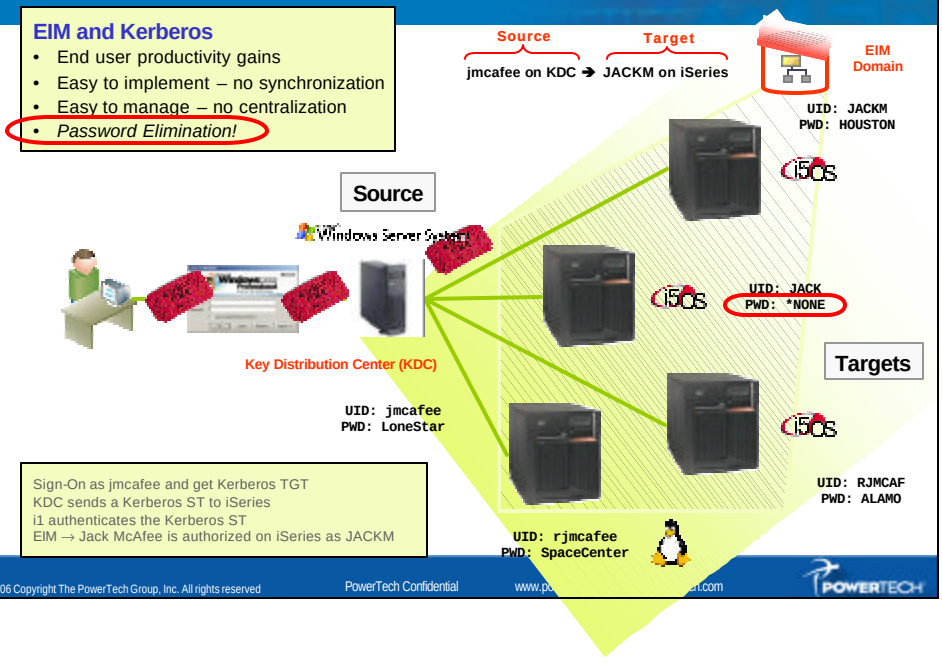
> **Target**
- For subsequent authentication
- Other registries, systems
- **Person, Registry ® User Identity**



2006 Copyright The PowerTech Group, Inc. All rights reserved

The Password Elimination Approach

EIM and Kerberos
- End user productivity gains
- Easy to implement – no synchronization
- Easy to manage – no centralization
- *Password Elimination!*



Sign-On as jmcafee and get Kerberos TGT
KDC sends a Kerberos ST to iSeries
i1 authenticates the Kerberos ST
EIM → Jack McAfee is authorized on iSeries as JACKM

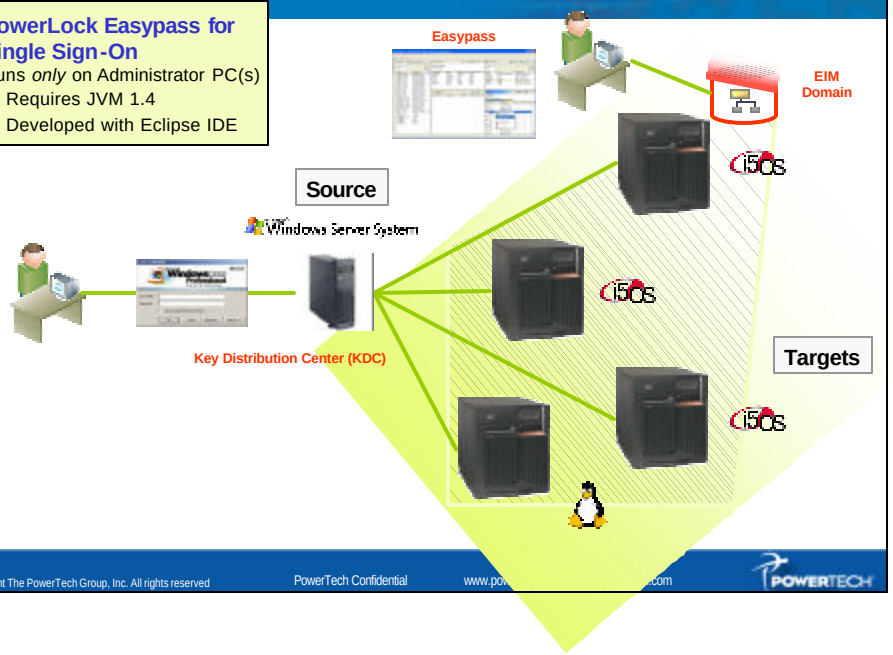
2006 Copyright The PowerTech Group, Inc. All rights reserved

PowerLock EasyPass

PowerLock Easypass for Single Sign-On

Runs *only* on Administrator PC(s)

- Requires JVM 1.4
- Developed with Eclipse IDE



2006 Copyright The PowerTech Group, Inc. All rights reserved

The Elimination Approach

Services or Applications enabled by IBM

- OS/400 V5R2
  - iSeries Access
  - iSeries Navigator
  - Telnet (includes PC5250)
  - ODBC/JDBC/DRDA
  - LDAP
  - QFileSvr.400
- Post V5R2 GA
  - Apache Web Server (PTF Group SF99098)
  - IBM WebSphere Host On-Demand (PTF level IP22748)

2006 Copyright The PowerTech Group, Inc. All rights reserved

SSO Approach Comparison

Cost to...	Password Elimination	Password Synchronization	Password Centralization
Acquire	Infrastructure is already integrated into all IBM eServer operating systems, or can be downloaded for free and run on Windows and Linux	Infrastructure provided by ISVs	Infrastructure provided by ISVs
Implement	No server agents nor end user workstation function to deploy; Rule-based associations can be quickly and centrally created between people and their various user identities on all registries	Synchronization service agent must be deployed on all servers and configured for each application; Passwords must be initially synchronized	"Capture and replay" function by be deployed on every end user workstation; Passwords must be initially captured Commandeered authorization prompts must be trained
Maintain	Passwords are no longer used for target authentication (Kerberos tickets, Identity Tokens, etc. are); These passwords can later be eliminated and thus do not require management by administrators and/or end users; Help desk password reset calls will be dramatically reduced!	Synchronization service is not always reliable; End users must still change all passwords per company policy (every 30, 60, 90 days); IT administrators must troubleshoot when all end user passwords do not match; Passwords are still sent across the network	End users must still change all passwords per company policy (every 30, 60, 90 days); IT administrators must troubleshoot when replay passwords do not match registry passwords; Passwords are still sent across the network

2006 Copyright The PowerTech Group, Inc. All rights reserved

Password Elimination Approach Benefits

- **End Users**
  - Increased productivity
  - No longer need to write down multiple passwords
  - Only need to remember a single, strong password
- **Administrators**
  - Less time resetting passwords
  - More secure enterprise (including *NONE passwords)
  - No need to secure or synchronize another registry
  - Platform authorization schemes are not changed
  - Incremental roll-out
- **Programmers**
  - Increased productivity
  - User identities and passwords no longer hard coded
  - Utilize same EIM domain maintained by administrators

2006 Copyright The PowerTech Group, Inc. All rights reserved

Web Applications - Using EIM and Identity Tokens

Single Sign-On Components

- **Client** – Web browser
  - Any web browser
  - No change to WAS authentication model
- **Middleware** – WebSphere Application Server (WAS)
  - WAS V5 or Express V5
  - IBM Java Toolbox (JT400) Java Connector Architecture (JCA)
- **Application** – Enabled to create Identity Tokens
  - iSeries Access for Web
  - WebFacing
  - WebSphere Development Studio Client (WDSc) Web Tools
  - And *YOURS!*
- **Back-end Server** – V5R2 or i5/OS V5R3 iSeries
  - Using the Java Toolbox (JT400)
  - Which uses the iSeries Access host servers

2006 Copyright The PowerTech Group, Inc. All rights reserved

Using EIM and Identity Tokens

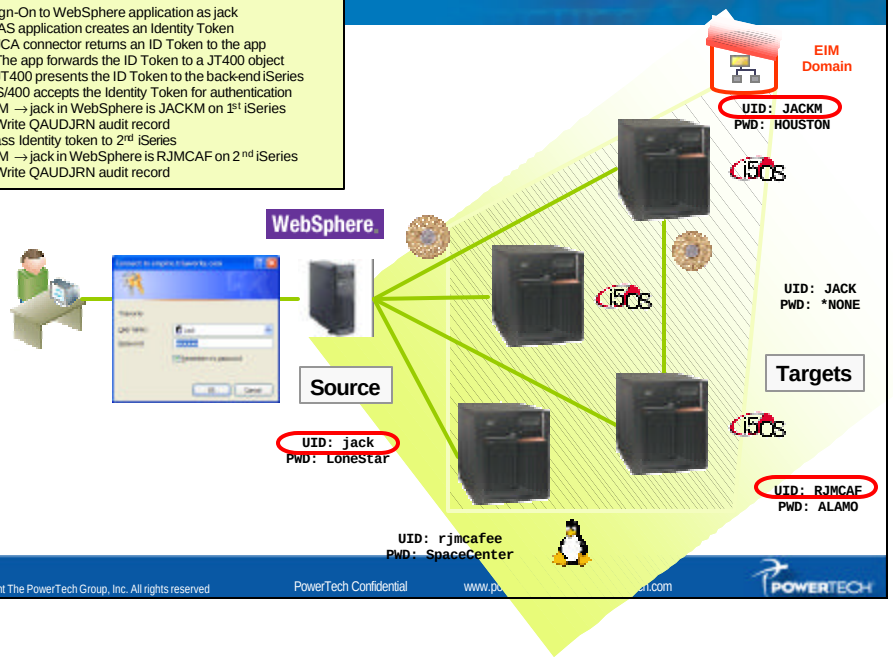
Enabled Single Sign-On Host Servers

- Sign-on server
- Central server
- File server
- Database server
- DRDA and DDM server
- Data queue server
- Remote command server
- Distributed program call server
- Network print server

2006 Copyright The PowerTech Group, Inc. All rights reserved

Using EIM and Identity Tokens

1. Sign-On to WebSphere application as jack
2. WAS application creates an Identity Token
   JCA connector returns an ID Token to the app
   The app forwards the ID Token to a JT400 object
   JT400 presents the ID Token to the back-end iSeries
3. OS/400 accepts the Identity Token for authentication
4. EIM → jack in WebSphere is JACKM on 1st iSeries
   Write QAUDJRN audit record
5. Pass Identity token to 2nd iSeries
6. EIM → jack in WebSphere is RJMCAF on 2nd iSeries
   Write QAUDJRN audit record



2006 Copyright The PowerTech Group, Inc. All rights reserved

Client Configuration

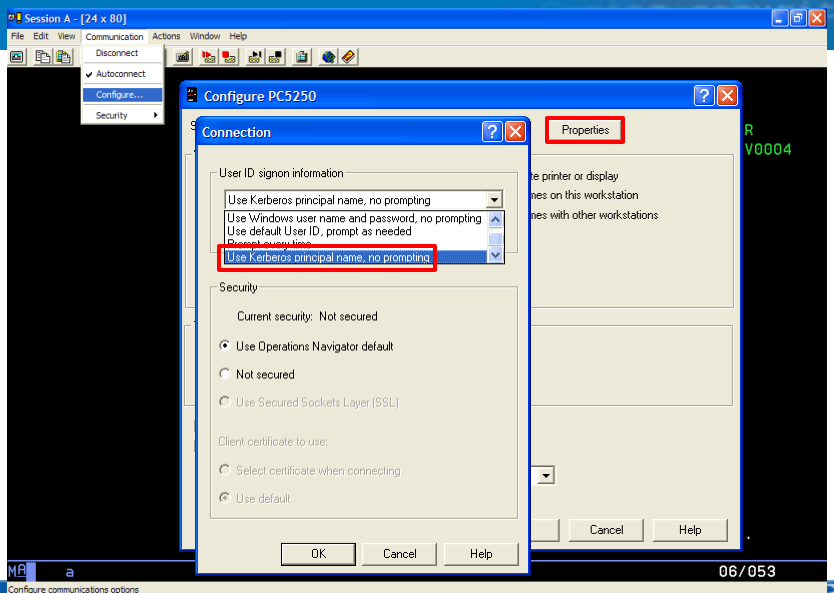
End users will not be enabled for SSO until they configure their clients to utilize Kerberos for authentication.

Two examples:

1. PC5250
2. iSeries Navigator

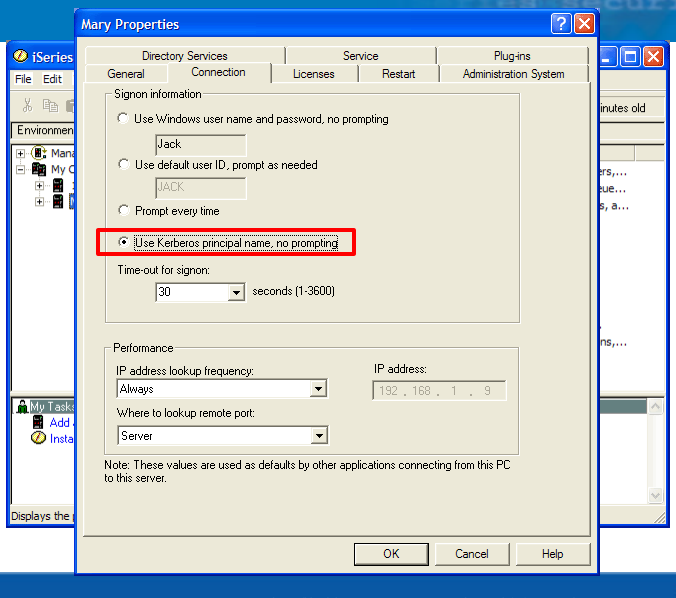
2006 Copyright The PowerTech Group, Inc. All rights reserved

PC5250



2006 Copyright The PowerTech Group, Inc. All rights reserved PowerTech Confidential www.powertech.com info@powertech.com

iSeries Navigator



2006 Copyright The PowerTech Group, Inc. All rights reserved PowerTech Confidential www.powertech.com info@powertech.com

Summary

The Password Elimination approach:

- Leverages ***existing infrastructure*** to
- Significantly reduce IT and end user ***password burden***

The existing infrastructure includes:

- Enterprise Identity Mapping (EIM) for ***authorization***
- Kerberos or Identity Tokens for ***authentication***

Kerberos used for Windows based applications
Identity Tokens used for WAS based applications
Plug-ins can be created for other platforms

2006 Copyright The PowerTech Group, Inc. All rights reserved

PowerLock EasyPass Software

PowerLock Easypass for Single Sign-On

> Designed specifically to manage EIM domains.

EasyPass makes it easy for a security administrator to **quickly** and **accurately** create and maintain associations between a unique person and different user identities on multiple registries across the enterprise.

EasyPass allows you to:

1. Use wizards to quickly **populate EIM**
2. Use rules to quickly **create associations**
3. Run reports to **maintain SSO integrity**

2006 Copyright The PowerTech Group, Inc. All rights reserved

For More Information

Links can be found on www.powertech.com

- Windows-based Single Signon and the EIM Framework on the IBM eServer iSeries Server **Redbook**

- Experts' Guide to OS/400 & i5/OS Security by Patrick Botz

- http://www-1.ibm.com/servers/eserver/security/eim/

- http://web.mit.edu/kerberos/

2006 Copyright The PowerTech Group, Inc. All rights reserved

Thank you!

Questions?

www.powertech.com

2006 Copyright The PowerTech Group, Inc. All rights reserved