



IBM eServer™

Session M05

Enterprise Identity Mapping: Getting User Identities to Work for You

Networking and Security Technical Conference
October 25-28, 2004
Anaheim, California

Peggy LaBelle

IBM Corporation, RACF Development

(845) 435-5910

plabelle@us.ibm.com

Disclaimer

The information contained in this document is distributed on an “as is” basis without any warranty either expressed or implied. The customer is responsible for use of this information and/or implementation of any techniques mentioned. IBM has reviewed the information for accuracy, but there is no guarantee that a customer using the information or techniques will obtain the same or similar results in its own operational environment.

In this document, any references made to an IBM licensed program are not intended to state or imply that only IBM's licensed programs may be used. Functionally equivalent programs may be used instead. Any performance data contained in this document was determined in a controlled environment and therefore, the results which may be obtained in other operating environments may vary significantly. Users of this document should verify the applicable data for their specific environment.

It is possible that this material may contain reference to, or information about, IBM products (machines and programs), programming, or services that are not announced in your country. Such references or information must not be construed to mean that IBM intends to announce such IBM products, programming, or services in your country.

IBM retains the title to the copyright in this paper as well as title to the copyright in all underlying works. IBM retains the right to make derivative works and to republish and distribute this paper to whomever it chooses.

Trademarks

The following are trademarks or registered trademarks of the International Business Machines Corporation in the United States, other countries, or both:

AIX

DB2

eServer

OS/400

pSeries

RACF

xSeries

z/OS

zSeries

The Open Group:

UNIX is a registered trademark of The Open Group in the United States and other countries

Other company, product or service names may be trademarks or service marks of others.

Agenda

- Demonstrate how EIM can be used by servers to provide
 - Better access control
- EIM Background
- Using EIM with the HTTP Server
 - Planning and Setup
 - Writing the CGI application
 - Demonstrating how it works

Enterprise Identity Mapping

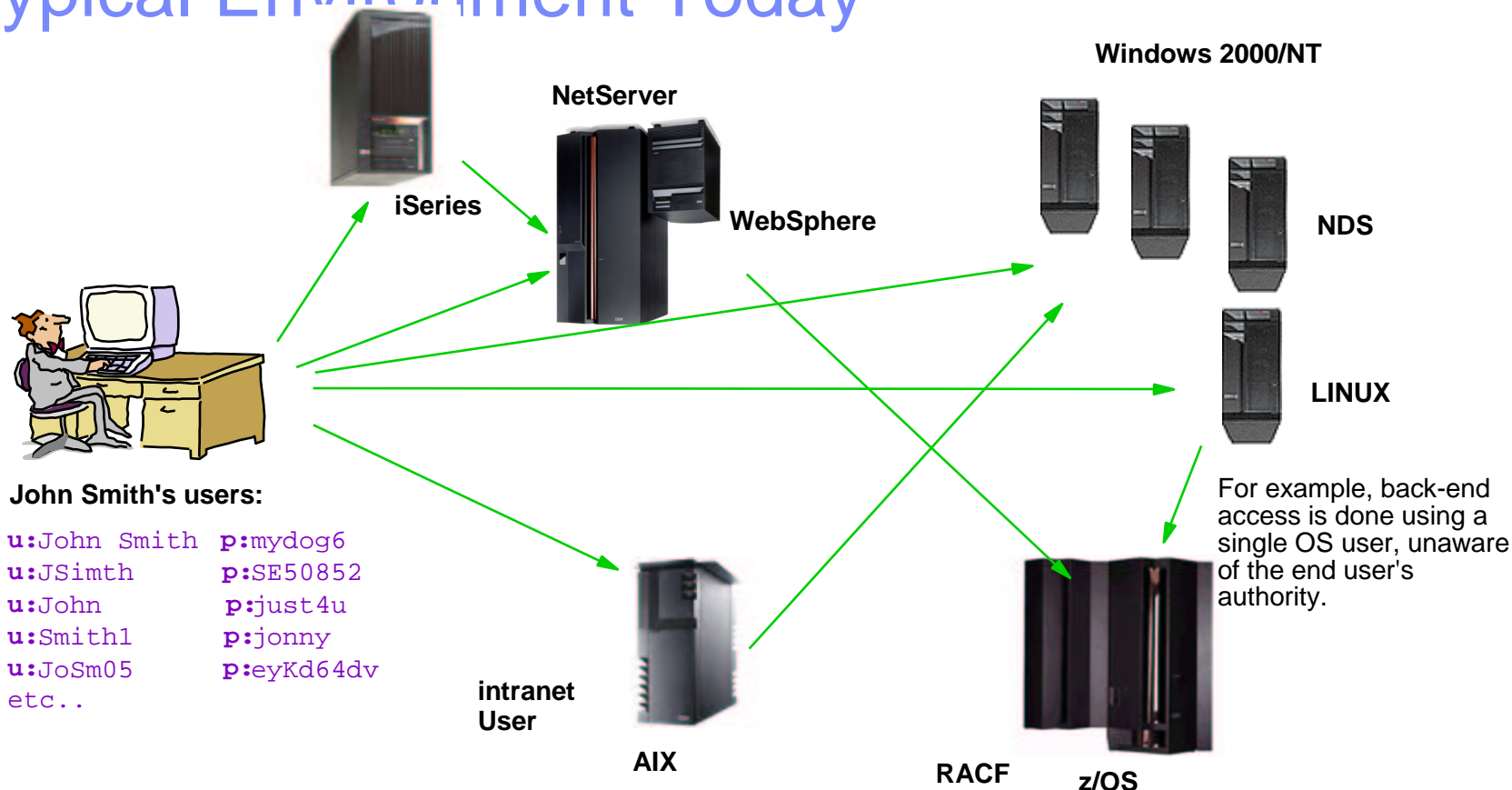
- **Observation:**

There is a lot of software in an enterprise that map one user id to another.
- **Idea:**

Store the mappings in a central location accessible to all of the software.
- **Result:**

Seamless distributed applications with better security

Typical Environment Today

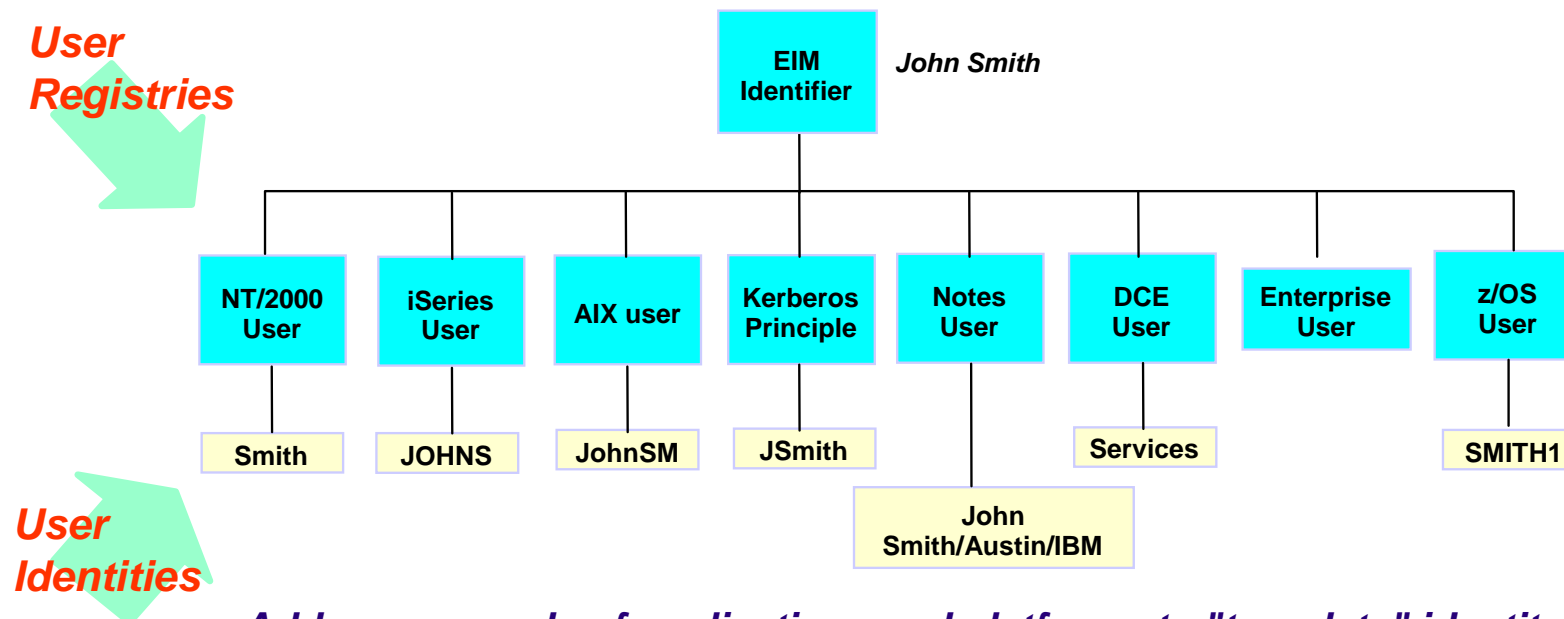


*Administrative Nightmare !!
Enterprise "Trust Scope"?*

*X-model transactions ?
Single Sign-on?*

Enterprise Identity Mapping

- **EIM defines** associations between an identifier and user ids in registries that are part of OS platforms, applications, and middle-ware.
- The identity associations (*mappings*) are stored in a well known location, e.g. LDAP, with common services across platforms to access the mappings.



Addresses needs of applications and platforms to "translate" identity when crossing platform and registry boundaries.

Ideas for EIM...

- Replace side files that contain mappings of user IDs
- Retrieve a mapping at exit points in servers where a host user ID/password is usually required (aka “single sign-on”)
 - Note: ensure trusted source
- Write an application that uses EIM mappings to correlate audit data across systems

Writing EIM Applications

C/C++ Lookup Application

```
/* obtain an identity, ex. principal @ realm */  
call eimCreateHandle (...)  
call eimConnect(...)  
  
call eimGetTargetFromSource(...)  
/* assert the new identity */  
/* access local resources */  
  
call eimDestroyHandle(...)
```

EIM DLL

LDAP client

ldap://some.host/

LDAP
Server

My Domain

enterprise identifier

user ID in
registry 1

user ID in
registry 2

user ID in
registry 3

EIM APIs

Lookup APIs

eimGetTargetFromSource, eimGetTargetFromIdentifier,
eimGetAssociatedIdentifiers

Administration APIs

Domain operations

Registry operations

EIM Identifier operations

User Management operations

Common APIs

EIM “handle” operations

System operations

Configure system with a default domains, bind credentials, and
registry names

Planning Considerations for EIM

Recommendation:

- Let applications and users drive initial deployment of EIM

Information needed about the application

- The platforms you plan to run the application on
- The types and names of the local registries
- Types EIM associations required and additional information
 - Source, Target, Admin
- Any system specific configuration requirements
 - ex. IRR.EIM.DEFAULTS or IRR.PROXY.DEFAULTS profiles
- EIM connection protocol required (i.e. LDAP bind protocol)
 - simple, simple + CRAM-MD5, Kerberos, SSL
- General idea of who in your enterprise will use the application

Planning Considerations for EIM...

- Choose an IBM LDAP directory for hosting the EIM domain controller
 - > Must be accessible to the components of the application
 - > Must support the EIM connection protocol
- Options for the LDAP server
 - > One server, referrals, master and replicas, sysplex
 - > Dedicated directory server or shared with other applications

Planning Considerations for EIM...

Administration of the EIM domain

- LDAP administrator and/or
- EIM administrator
- EIM identifier administrator
- EIM registries administrator
- EIM registry xyz administrator

Naming conventions for

- The domain
- The registries
 - By type and/or system and/or location in network ...
- The enterprise identifiers
 - A person's name vs employee number vs ...

Setting Up an EIM Domain Controller

Create LDAP BIND credentials at LDAP server hosting the domain

- Administrators – domain, registries, registry, identifiers
- applications – mapping operations (i.e. lookup)
- LDAP administrator has full access to the EIM domain

Create the EIM domain

Give the credentials the required access to the EIM domain

Define the registries

Add the EIM identifiers

Add the EIM associations

Using z/OS LDAP as the Domain Controller

z/OS V1R4 Security Server LDAP or later

Required attributes and object classes

- ibm-entryUUID

- lbmattributetypes

- aclEntry, aclPropagate, aclSource,
entryOwner, entry Propagate,
entrySource.

New attribute types and object classes for EIM
(schema updates)

TDBM backend required

SDBM (RACF) backend is optional, but can be useful

OW55078 (PTF UW92346)

z/OS EIM Client APIs and eimadmin utility

z/OS V1R4 Security Server LDAP or
z/OS V1R5 Integrated Security Services EIM

EIM applications must

Reside in the HFS

APF authorized

simple binds, SSL server side (z/OS V1R4)

simple binds+CRAM-MD5, Kerberos, and SSL (z/OS V1R5)

eimadmin utility

USS shell command

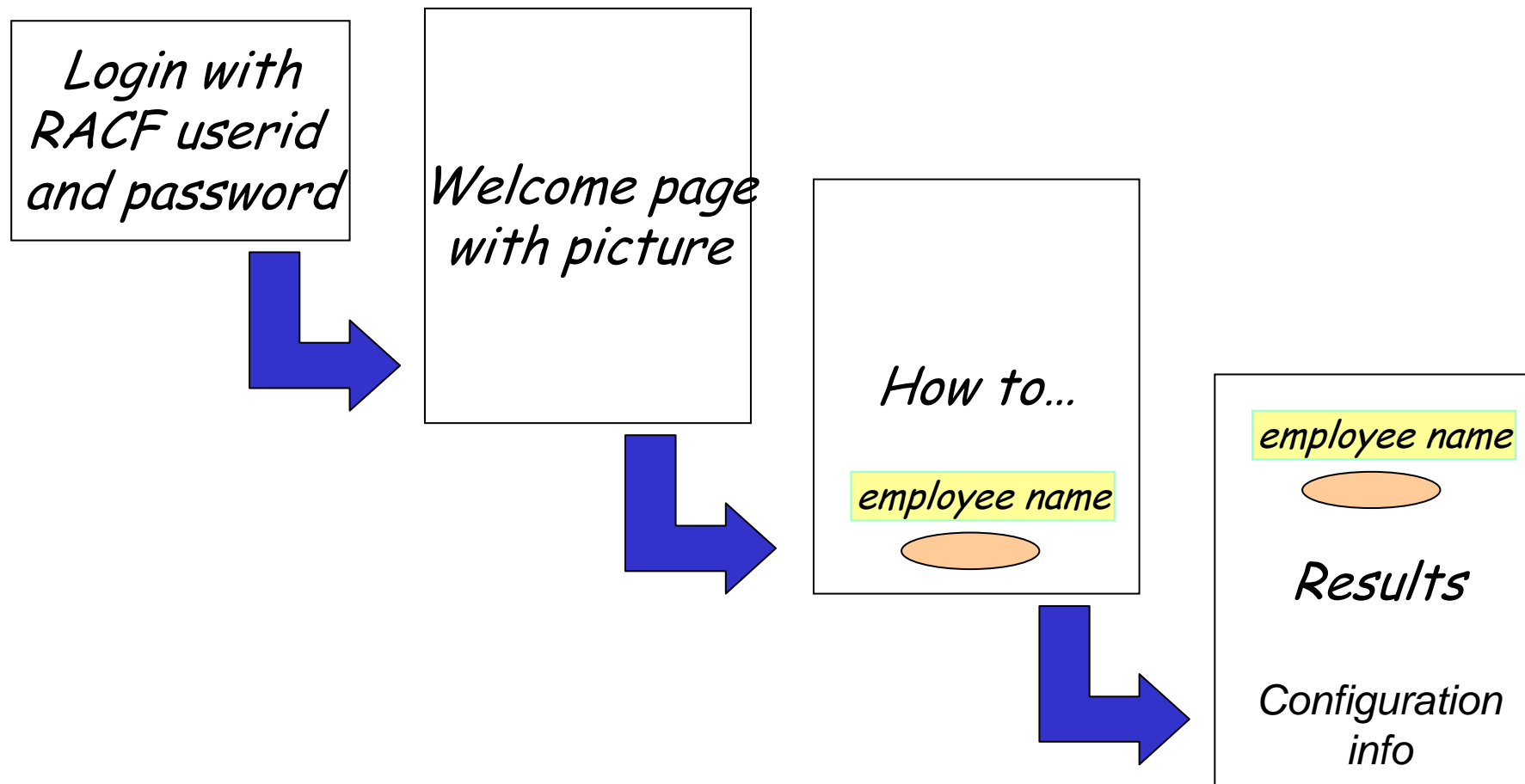
Command or file input (ex. Output from RACF's DBUNLOAD)

Updates ANY EIM domain controller (any platform)

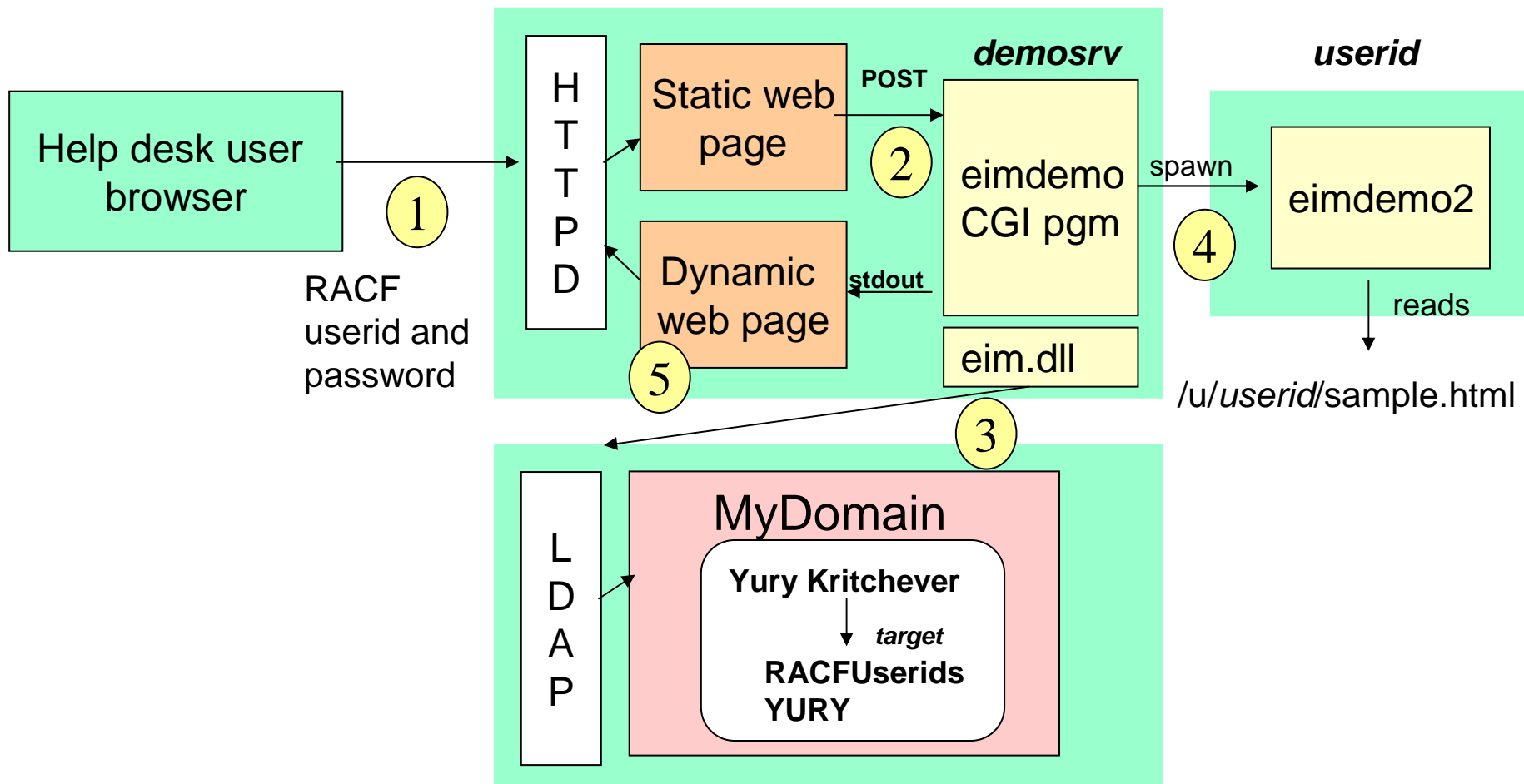
EIM and HTTP Web Application Example

- “Help desk” Web application that displays information about an employee.
- Catch..some of the information must be obtained using the employee’s local user id

The application sketch



Web Application - Below the Surface



Setup

- HTTP Server on z/OS
 - Access to the ldap and eim clients
 - User id of the cgi program has daemon authority
- LDAP on z/OS
 - Configured for TDBM
 - A bind dn defined for mapping operations
- EIM on z/OS
 - ldap administrator can run eimadmin utility
- RACF or equivalent
 - Will be defining/updating profiles in the FACILITY, LDAPBIND, and USER classes

Parts

- eimdemo.welcome.html, eimdemo.html – static web page
- eimdemo.c, eimdemo2.c
 - Obtains the employee name from the static web page
 - Performs an eimGetTargetFromIdentifier to get employee's local user id
 - Performs an eimListIdentifiers to get general info about the employee from EIM
 - Spawns a program (eimdemo2.c) that reads a file owned by the local user id
 - Creates a dynamic web page with the information
- /u/...../sample.html
 - A file that can only be read by the owner

Configuring and Setup of EIM

- Create domain
 - `ibm-eimDomainName=MontpellierEnterprises,c=au`
- Add a registry
 - MV08RACF
- Add identifiers, aliases, and descriptions
 - Yury Kritchever; 9999; Mr. Q & A
 - Jon Briggs; 8888; Mr. Admin
- Add a TARGET association
 - Yury Kritchever to his RACF user ID YURY
- Grant MAPPING access to the domain
 - `cn=eimLookup,c=au`

Create a domain

```
eimadmin -aD -d 'ibm-eimDomainName=MyDomain,c=us'  
-h ldap://some.big.host:389  
-b 'cn=ldap administrator' -w passwd
```

```
eimadmin -aR -r MV08RACF -y RACF ...
```

```
eimadmin -al -i 'Yury Kritchever' ...
```

```
eimadmin -aA -i 'Yury Kritchever' -r MV08RACF -u YURY ...
```

```
eimadmin -aC -q 'cn=eimLookup, c=au' -c MAPPING ...
```

Configuring RACF for EIM

- Configure default local registry name

```
rdefine facility irr.proxy.defaults eim(localreg(MV08RACF))
```

- Configure domain and bind info for the CGI pgm

```
rdefine ldapbind MyDomain +  
proxy(ldaphost(ldap://...) binddn(cn=eim...) bindpw(secret)) +  
eim(domaindn(ibm-eimdomainname...))
```

```
altuser demosrv eim(ldapprof(MyDomain))
```


Other considerations

- Give the webserver authority to switch to the demosrv userid
 - BPX.SRV.userid profile in the SURROGAT class
- Give the demo server (demosrv) the authority to spawn another process with a new user id
 - BPX.DAEMON profile in the FACILITY class
 - Program controlled or demo server has UID(0)
- EIM APIs require the caller to APF authorized
 - extattr +a eimdemo
 - ls -E eimdemo

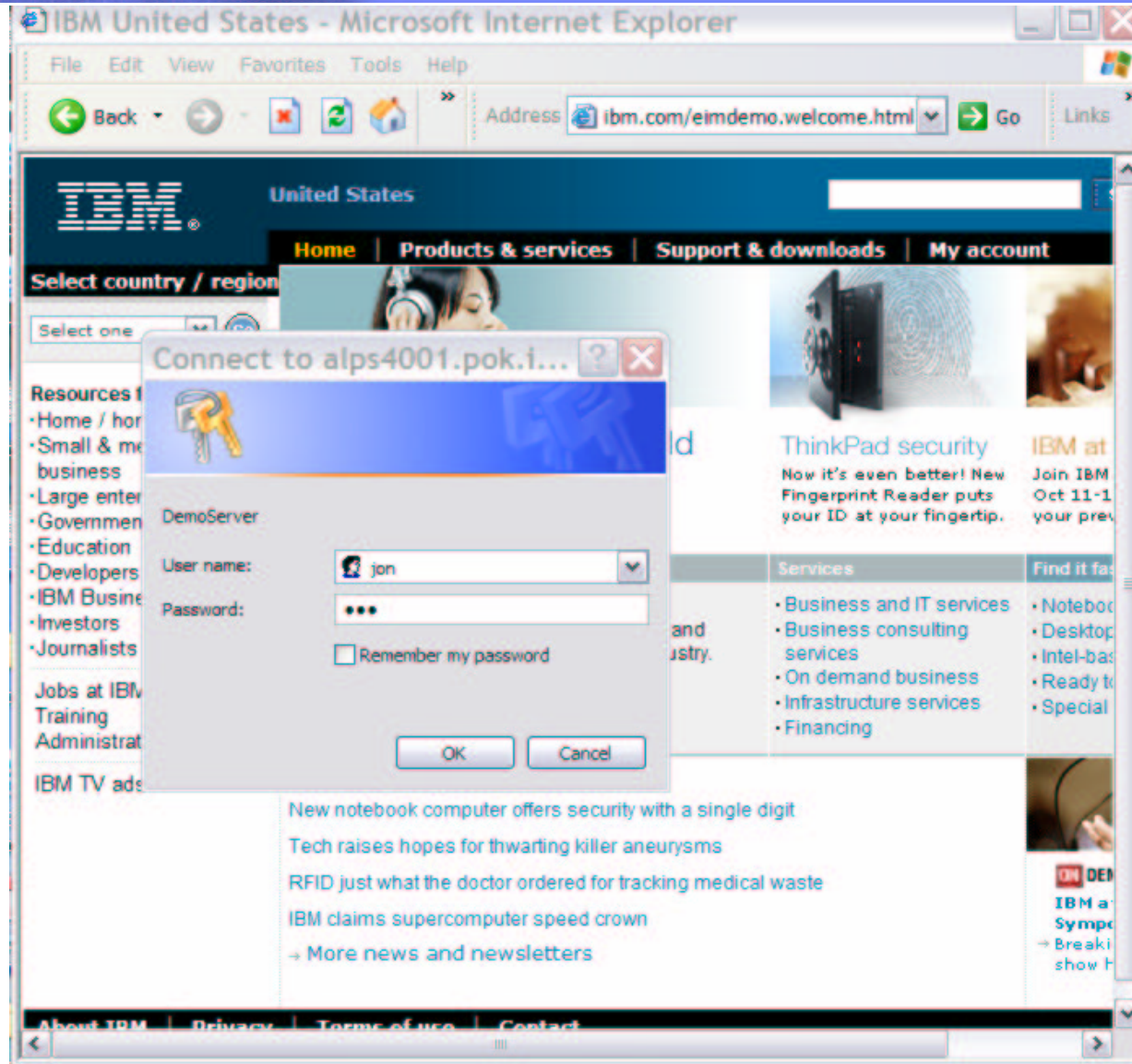
Final setup and demonstration

```
tl4 - ibmuser
File Edit View Communication Actions Window Help
YIBMUSER:/u/YURY$ su YURY
FSUM5019 Enter the password for YURY:
YIBMUSER:/u/YURY$ id
uid=1001(YURY) gid=1(SYS1)
YIBMUSER:/u/YURY$ ls -Fla sample.html
-rux----- 1 YURY      SYS1      19 Oct  5 15:21 sample.html*
YIBMUSER:/u/YURY$ more sample.html

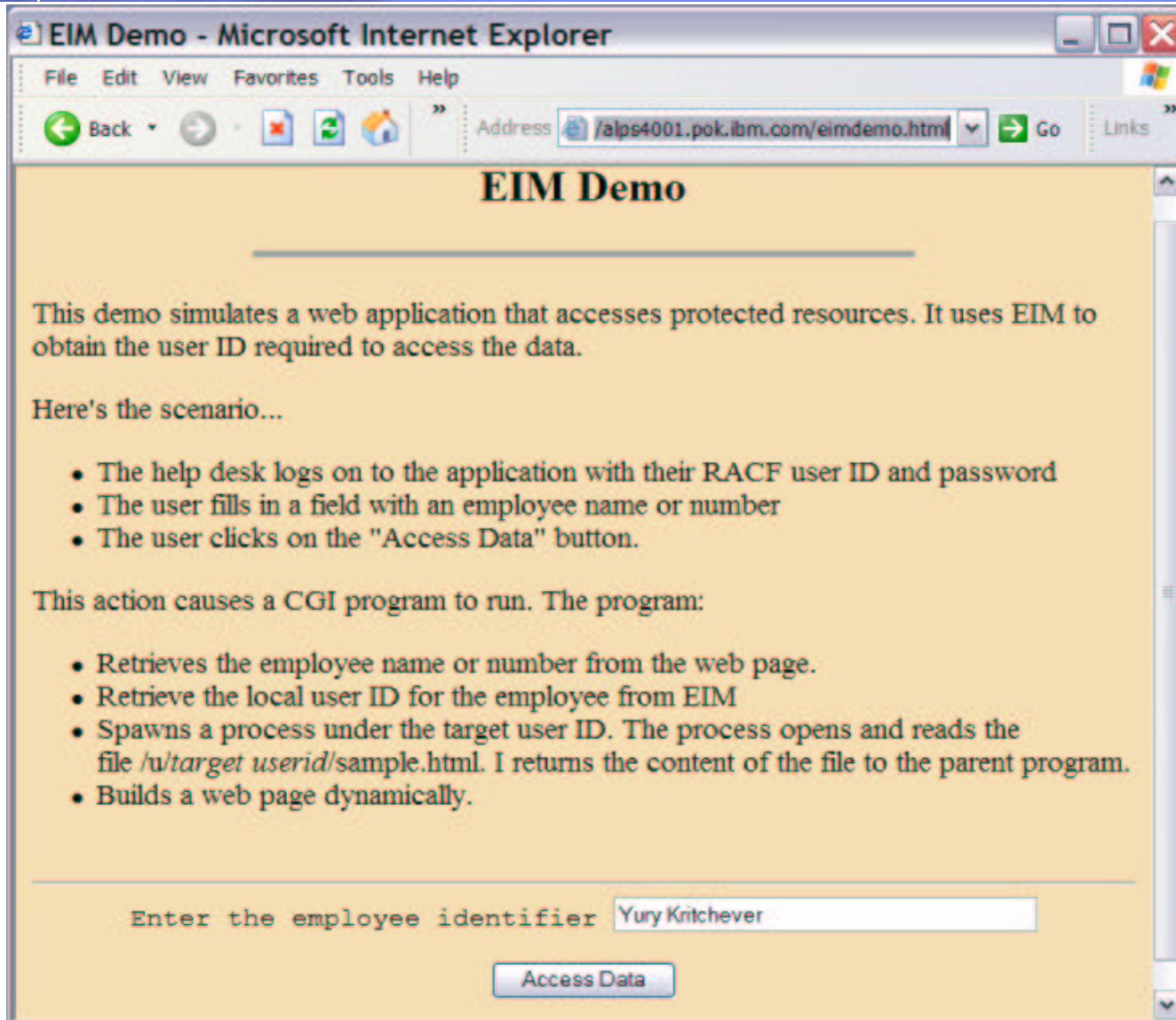
This is test data.
Ysample.html" (EOF)

YIBMUSER:/u/YURY$ YIBMUSER:/u/YURY$

===> _
RUNNING
ESC=␣  1=Help      2=SubCmd    3=HlpRetrn  4=Top       5=Bottom    6=TS0
        7=BackScr   8=Scroll   9=NextSess 10=Refresh  11=FwdRetr  12=Retrieve
MA c 21/007
Connected to remote server/host pokvmtl4.pok.ibm.com using port EPSON Stylus C60 Series on USB001
```







EIM Demo

This demo simulates a web application that accesses protected resources. It uses EIM to obtain the user ID required to access the data.

Here's the scenario...

- The help desk logs on to the application with their RACF user ID and password
- The user fills in a field with an employee name or number
- The user clicks on the "Access Data" button.

This action causes a CGI program to run. The program:

- Retrieves the employee name or number from the web page.
- Retrieve the local user ID for the employee from EIM
- Spawns a process under the target user ID. The process opens and reads the file `/u/target userid/sample.html`. It returns the content of the file to the parent program.
- Builds a web page dynamically.

Enter the employee identifier

EIM Demo

Employee

Employee Information For: Yury Kritchever

Additional Data This is test data.

DEMO Configuration Information

<i>EIM Domain</i>	LDAP://ALPS4001.POK.IBM.COM/ibm-eimdomainname=MontpellierEnterprises,c=au
<i>Domain Bind DN</i>	cn=eimLookup,c=au
<i>Unique Name</i>	Yury Kritchever
<i>Description</i>	Mr. Q & A
<i>Other Name(s)</i>	Yury Kritchever; 9999

EIM Demo

Employee Jon Briggs

Access Data

Employee Information For: Jon Briggs

Additional Data No additional information

DEMO Configuration Information

<i>EIM Domain</i>	LDAP://ALPS4001.POK.IBM.COM/ibm-eimdomainname=MontpellierEnterprises,c=au
<i>Domain Bind DN</i>	cn=eimLookup,c=au
<i>Unique Name</i>	Jon Briggs
<i>Description</i>	Mr. Admin
<i>Other Name(s)</i>	Jon Briggs; 8888
<i>Target Registry</i>	MV08RACF
<i>Target User ID</i>	

EIM Demo

Employee

Employee Information For: Pekka Hanninen

Additional Data No additional information

DEMO Configuration Information

EIM Domain LDAP://ALPS4001.POK.IBM.COM/ibm-eimdomainname=MontpellierEnterprises,c=au

Domain Bind DN cn=eimLookup,c=au

Unique Name

Description

Other Name(s)

Target Registry MV08RACF

Target User ID

EIM Available...

Platform	EIM Domain Controller	EIM Client	IBM EIM Admin Tools
OS/400 on iSeries	OS/400 V5R2	OS/400 V5R2	OS/400 V5R2
z/OS on zSeries	z/OS V1R4 LDAP	z/OS V1R4 LDAP SPE OW57137	z/OS V1R4 LDAP SPE OW57137
AIX on pSeries		AIX V5.2	
Windows 2000 on xSeries		Download + IBM Directory V4.1 Client	
LINUX - SLES8 on PPC64 - Red Hat 7.3 on i386 -SLES7 on zSeries		Download + IBM Directory V4.1 client or Download + OpenLDAP V2.0.23 client	

Latest list see <http://www-1.ibm.com/servers/eserver/security/eim/availability.html>

Available for download:

- **Java EIM Client** (<http://www.ibm.com/servers/eserver/security/eim/availability.html>)

- *EIM Connector for Tivoli Identity Manager available for download!*

Fix 4.5.1-TIM-0010

EIM Applications

Lookup

OS/400 on the iSeries

Administration

IBM Tivoli Identity Manager

z/OS eimadmin utility

iSeries Operations Navigator

Safestone's AxxessIT

TriAWorks Identity Manager for Single Sign-On

BlueNotes EIM Administrator

Session Summary

- Demonstrate how EIM can be used by servers to provide
 - Better access control
- EIM Background
- Using EIM with the HTTP Server
 - Planning and Setup
 - Writing the CGI application
 - Demonstrating how it works
- Q & A

Publications

- Publications References, e.g.:

- ▶ Integrated Security Services Enterprise Identity Mapping (EIM) Guide and Reference
- ▶ Security Server (RACF) Command Language Reference
- ▶ Security Server (RACF) Callable Services
- ▶ eServer Information Center
 - ▶ <http://publib.boulder.ibm.com/eServer>
 - ▶ Follow links for your geography

Session M05 - EIM

- This slide intentionally left blank.