

---

# **SSO: When are we going to get there ?**

Mike McNamee

e3 Sciences

Mikem@e3sciences.com

# Agenda

---

- Promise of SSO
- The reality of SSO implementation
- Alternative Strategies
- Are standards the way forward
- Is SSO becoming redundant ?

# The promise of SSO

---

- Introduction of Distributed Systems caused major security issues
  - Too many userids/passwords to securely keep for the average user
  - Users devised their own solutions that were not desirable

# The promise of SSO

---

- SSO Systems would take all the pain away !
  - Logon once
  - Security is enhanced
  - Life becomes easy !

# The promise of SSO

---

- For vendors the lure of a huge market beckoned

Considering just IBM Mainframe sites ...

# The promise of SSO

---

Region	Number of Mainframe Sites
United States	3,981
Europe	3,342
Japan	892
ROW (Including Asia/Pacific)	1,975
<b>Total WW</b>	<b>10,190</b>
Germany	803
France	572
United Kingdom	391
Italy	531
Netherlands	186
Belgium / Luxemburg	136
Sweden	139
Denmark	97
Norway	40
Finland	44
Switzerland	131
Austria	92
Spain	180
<b>Total Europe</b>	<b>3,342</b>

# The promise of SSO

---

- Average SSO sale of \$80,000 .....
- There are 10,000 IBM mainframe sites alone - market of \$800m for this market segment alone

# The reality of SSO implementation

---

- Prohibitive deployment costs
  - Visit every workstation ( rollout in some cases costing > \$1m )
  - Management of logon scripts
- Proprietary solutions
  - Vendor lock-in
  - Lack of application support - can this problem be solved by a single vendor using proprietary technology ?
  - Vendors generally did not adopt standards (XSSO) or co-operate

# The reality of SSO implementation

---

- Operational issues
  - Centralized Sever
    - Scalability problems
    - Network outages are catastrophic as no one can log on
  - Extra administration as the SSO was yet another system to manage

# The reality of SSO implementation

---

- Success Stories
  - Small in number
  - Small implementations
- Vendors sold small number of licenses

# The reality of SSO implementation

---

- Many issues have been resolved in recent times in vendor products
- Many users have already passed by SSO

# Alternative Strategies

---

- To combat these problems vendors and users adapted their strategies :

# Alternative Strategies

---

- Users :
  - If in doubt : DO NOTHING !!!
  - Implement limited scope projects
  - Have a go at the free software Computer Associates had given them ( Unicenter SSO )
  - Have a go at the free software Microsoft had given them ( SNA Server SSO )

# Alternative Strategies

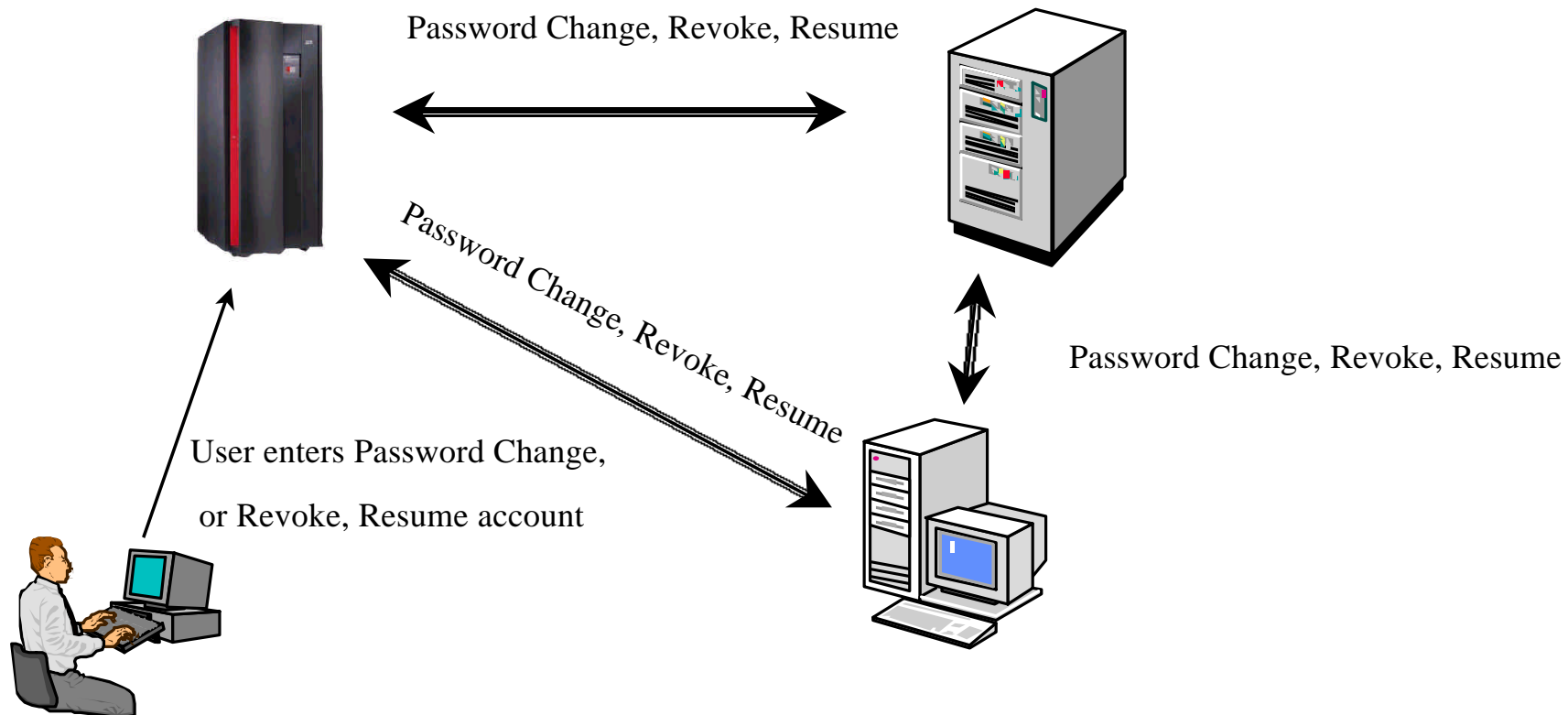
---

- Vendors :
  - Offer simpler solution : Consistent Sign On (CSO)
  - Discount/Bundle the software
  - Step up Marketing

# Consistent Sign On

---

- Server based solution to provide consistent account status - changes replicated around network



# Consistent Sign On

---

- Provide a consistent logon environment
  - Synchronize Account status
  - Provide an easier environment for users
  - Provide an easier environment for Administrators and Help Desk
  - Server Based solution provides some of the benefits of SSO without the huge implementation costs associated with SSO
- Provides some degree of improved security by allowing lock out to be network wide instead of just one platform

# Consistent Sign On

---

- Examples :
  - Proginet SecurPass
  - Axent PassGo InSync
  - Blockade

# Discounted Software

---

- Many organizations will accept “free” or “inexpensive” software and make great efforts to make it work

Q: If it's free what have we got to loose ?

A: Time, Money and possibly your sanity

# Are standards the way forward ?

---

- The proprietary nature of solutions have been a major weakness
  - Deployment is an issue
  - Interoperability is an issue
  - Vendor reach is an issue
    - Limited application support

# Are standards the way forward ?

---

- A number of standards exist that are well accepted in the industry :
  - Kerberos ( RFC 1510 )
  - Digital Certificate ( X.509 )

# Are standards the way forward ?

---

- Kerberos ( RFC 1510 )
  - Implemented in many SSO solutions
  - Generally needs to be installed separately to the OS
  - Many legacy applications need change to support Kerberos
  - Interoperation between Kerberos solutions is an issue

# Are standards the way forward ?

---

- Windows 2000 with free added Kerberos !
  - NT Lan Manager ( NTLM ) protocol replaced with Kerberos - shipped with product
  - Imbedded into Win2K software - no changes to end-user operation or applications
  - No additional cost for software
  - Kerebros usage will now massively increase

# Windows 2000

---

- Microsoft promising free supplied SSO for Win2K & UNIX environments
  - Implementation semantics make it incompatible with other Kerberos implementations
    - Microsoft have been “enhancing” the standard
  - Is this another example of “assimilate and exterminate” ?

# Windows 2000

---

- Microsoft offer SSO for Mainframe and AS/400 via the Host Integration Server (Babylon) product. Previously known as SNA Server
  - Insecure ( sends passwords in clear-text )
  - Assumes SNA is being used

# Digital Certificate ( X.509 )

---

- A well defined standard for representing user credentials
  - Does not require prior knowledge of user
  - Good compatibility across implementations
    - Universal Semantics for defining users
  - Not easily supported by legacy applications
    - Is this where SSO solutions will plug a gap ???
  - Smart-Card deployment looking practical and secure

# Is SSO becoming redundant ?

---

- SSO was the answer to a problem :
  - User needs application access
- EAI solutions provide an alternative
  - If applications are integrated then do we need to access all of them ?
  - XML provides framework to describe data exchange between applications

# Is SSO becoming redundant ?

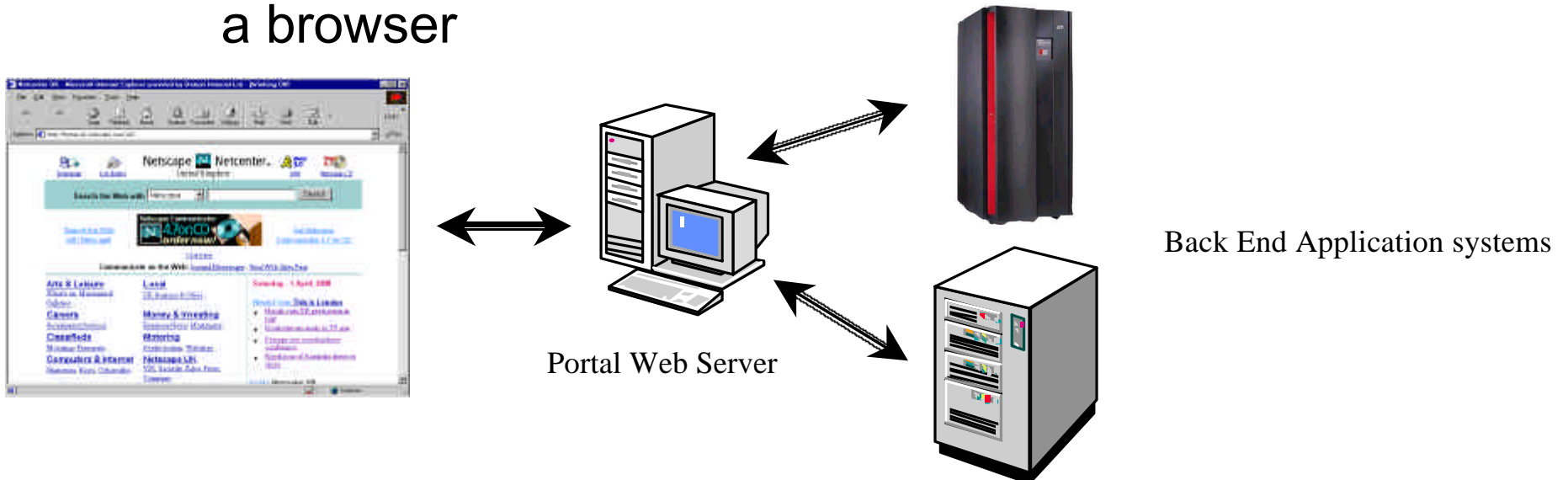
---

- Portals provide an alternative ?
  - Many organizations are giving their existing applications browser access : e-business is a strong motivator
    - Traditional sign on in many cases not required
    - CSO provides consistent credentials across back-end security systems
  - Portals are a necessity for many organizations who have implemented Web based applications with no overall control
    - Now have numerous applications on many sites with bespoke security systems

# Is SSO becoming redundant ?

---

- Are Portals the new SSO ?????
  - Instead of taking the user to the application - take the application to a user in a browser
  - User authenticates themselves using userid, certificate or token and application is presented on a browser





?

?

?

?

?

?

?

?

?

?

# Questions ?

?

?

?

?

?

?

?

?

?

?

?

?

?

?