Authentication: Password Madness

MSIT 458: Information Security
Group Presentation

The Locals

Password Resets

- United Airlines = 83,000 employees
- Over 13,000 password reset requests each month through the IT Service Desk
- Intranet, email and one other system make up approximately 75% of all password resets

Voice of the User

- Passwords expire too often
- They must remember too many passwords
- Password authentication is too strict

UNITED

> “Why is it that it’s harder to get into my email box at United than my Chase bank account?”
>
> ~SFO Flight Attendant

Single Sign-On

This ain’t your parents’ SSO

The old way of thinking about SSO

- Requires modification of target apps
- Lengthy and costly implementation

A new way of thinking

- No modifications required. Apps are “trained” to “sense” sign-in screens.
- Out-of-the-box implementations (3 to 6 months)
- Cost effective

Advantages for the User

Provides user with one username and one password for accessing multiple systems

- Reduces time spent on login/logout activities
- Eliminates "password fatigue" by reducing the number of usernames and passwords to be maintained
- Can reduce incidence of phishing attacks, since users know they shouldn't be entering passwords

Advantages for the Admin

Simplifies user account management by reducing the number of accounts and passwords

- Centralized management of user credentials allows for more efficient identity management
- New user setup done once and propagated across enterprise
- Authentication/password rules, account lockout and auditing policies are enforced more effectively with relatively reduced cost and effort
- Easier to detect anomalous behavior thus improving security of network

How SSO Works

Types

- E-SSO, Web, and Federated

Features

- Enables user to log in/out only once in a given session
- User can access all systems that he or she is authorized to access within that session without multiple login/logout activities
- Access to multiple apps/systems are authenticated with a single set of credentials

How E-SSO Works

Setup/configuration

- Graphical wizard used to "train" the product to recognize various sign-on, password change, post-sign-on automation and sign-off events.
- Wizards write scripts or XML parameter files

Back-end repository

- Active Directory
- LDAP
- Relational database management systems (RDBMSs)

How E-SSO Works

Architecture

- ***Two-tier***, where E-SSO agents interact directly with directory infrastructure
- ***N-tier***, where E-SSO provides middle layer between agents; brokers interactions with directory

Reporting

- Log entries provide basic information about application access
- Canned reporting functionality
- Export log data to third-party reporting or system management tools

Options

- Windows integrated authentication (i.e. Kerberos)
- Password synchronization
- Software packages
  - PassLogix, acquired by Oracle (Oct 2010)
  - Imprivata OneSign SSO
  - IBM Tivoli Unified Single Sign-On
  - And of course, SSO for the "Cloud,"
    SinglePoint Universal Sign-On from Symplified

If the USPS can do it…

800,000 employees

157,000 computers in **20,000** buildings

1000 internal applications

6000 external applications

UNITED STATES
POSTAL SERVICE ®

USPS chose PassLogix

- Does not require application modification or scripting
- Initial configuration completed in 30 days
- Testing and engineering took 90 days
- Total roll-out time was 8 months

Applications included in deployment:

- Web applications
- Win32 applications
- Mainframe applications
- VAX applications
- Java applications
- Windows Terminal Services

passlogix®

+

UNITED STATES POSTAL SERVICE®

What does it cost?

- Depends upon size and scope
- Analysis by Gartner (Sept 2010):

Scenario 1: Regional Hospital	Scenario 2: Manufacturing Company
4 locations. If a location fails, it must be handled by another location.	1 location
1,000 users	5,000 users
Exchange, SAP, Lotus Notes, six thick-client Windows apps and six Web apps	Standard Web, Windows and terminal applications

What does it cost?

Regional Hospital	Manufacturing Company
Shared kiosk/workstation support for 500 of the users	Remote access required for 1,000 of the users on unmanaged machines
Passive proximity card integration for all users	No new authentication methods or shared kiosks
The average price was $69,000, down from $86,000 in 2008-2009.	The average price was $219,000, down from $264,000 in 2008-2009.
Average $69/user.	**Average $43.80/user.**

Industry Applicability

- Cross-industry problem, cross-industry solution
- Best in environments with multiple applications/login that cannot be “fixed” to integrate with directory services
- Particularly useful in health-care industry
  - Clinical environments with mobile users logging into arbitrary workstations
  - Need quick login
  - Sentillion - SSO provider specifically for health care. Recently acquired by Microsoft.

Limitations

Current packages struggle detecting login screens with web technologies

- Rich Internet Applications
- Flash
- Java

“Keys to the castle” if user credentials are breached

- Combine with additional security (smart cards, biometrics, etc.)
- With only one password to remember, can force strengthening of passwords

SSO server becomes a single point of failure/bottleneck

Business Consequence

Enterprises that adopt ESSO products must incorporate ESSO testing into the enterprise change management process.

- Automated sign-on logic can fail when sign-on or password update prompts change with new releases of target applications or operating systems.
- Administrators must then retrain the ESSO product to recognize the new prompt.

Legal Consequence

The ESSO solution and target apps must be in compliance with various privacy regulations

- ***US Privacy Act of 1974*** protects records that can be retrieved from a system of records by personal identifiers such as a name, social security number, or other identifying number or symbol.
- ***Health Insurance Portability and Accountability Act of 1996 (HIPAA)*** protects the privacy of individually identifiable health information

Trends

OpenID

- Created in 2005 by the open source community
- The "driver's license for the entire Internet."
- You control how much information is shared.

Facebook Connect

- Launched in December 2008; code owned by Facebook
- Users take their Facebook identity, network, and privacy settings with them as they browse sites.
- Users interact with their Facebook friends on other websites, and can stream their activity back into the Facebook news feed.

Trends

Biometric Coupling

- Biometric input devices coupled with SSO framework provides a much more secure solution
- Fingerprint biometric technologies
- Proximity badges
- One-time password (OTP) tokens
- Smart cards

Conclusion: SSO at United

- Moving from eDirectory to Active Directory
- Pick apps from United and Continental that will use AD for SSO
- Cost
- Timeline:
    - Migration planning has already commenced
    - Migration is to be completed by the end of 2012

Thanks.