Enterprise Single Sign-On
City Hospital Cures Password Pain

Stephen Furstenau
Operations and Support Director
Imprivata, Inc.
www.imprivata.com
Application Security

“Most organizations could completely secure themselves if they could remove two vulnerable components: people and software”

Gartner Group

- Passwords are often the only defense against unauthorized system, application or data access
- Password “strength” or resiliency to being broken is often confused with password security
- Application vulnerabilities exist when passwords are managed by users
City Hospital – A Case Study for ESSO

- Regional Hospital with 1000 Employees
- Handles 8000 inpatients and 150,000 outpatients per year
- Heavy dependency on Meditech – 600 users
- Supporting shared workstations and mobile workstation

Key challenges:
- Meet HIPPA Security requirements
- Provide security with alienating the medical staff
- Reduce help desk calls
- Need to support a wide range of applications
- Simple implementation and ongoing management
- Low initial investment – deploy quickly
HIPAA Compliance

- Administrative Safeguard Standards
  - Review and monitor
  - Authentication and authorization
  - Information access management
  - Password management
  - Identity based event logs

- Physical Safeguard Standards
  - Workstations environments

- Technical Safeguard Standards
  - Unique identities for all users

“Ease of use drives good security…” – Christopher Paidhrin
## Why are passwords a problem?

<table>
<thead>
<tr>
<th></th>
<th>5 years ago...</th>
<th>Today...</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>More passwords</strong></td>
<td>The average user had had 1 or 2</td>
<td>8+</td>
</tr>
<tr>
<td><strong>Regulatory compliance</strong></td>
<td>NO regulations</td>
<td>HIPAA, SOxA, GLBA, others</td>
</tr>
<tr>
<td><strong>Password Security</strong></td>
<td>90% of companies had no password policies</td>
<td>Companies are either: thinking about; trying to; or have implemented policies</td>
</tr>
<tr>
<td><strong>Control over information access</strong></td>
<td>Access only within the enterprise</td>
<td>Web applications and remote users extend access</td>
</tr>
</tbody>
</table>
City Hospital – Password Security Policy Objectives

- **Password policy elements**
  - Strong password - lengths and entropy “A12bfRe6@%sQ”
  - Frequently changed – every 30 or 60 days
  - Uniqueness – dissimilar from previous, non-repeating
  - Audited for compliance
  - Applied to different roles
  - Enforced by corporate policy

- **Enhance with strong authentication**
  - When passwords alone do not provide enough security

- **Define unique accounts & roles for all users**
  - Admins, clinicians, execs, partners, affiliates
Password strength improves security, but....

- To compensate for login complexity, users:
  - Write down their passwords
  - Reuse familiar, “weak”, or cherished passwords
  - Use the same password for all applications
  - Share common passwords with others
  -Forget their passwords and ask the Help Desk for resets

- UK survey finds valid system password at 1 out of 3 desktops - typically under the keyboard
- Helpdesk password resets can lead to unauthorized access
- Potential vulnerability exists as long as users are aware of their passwords
City Hospital - Password Policy Challenges

- Adoption – user acceptance is largest problem
- Audit – complex environments, application centric logs
- Administration – new processes, more responsibilities
- All Adds up to higher operating costs
  - Lost productivity
  - User frustration
  - Additional resources required
  - Poor compliance, or…
  - Increased calls to helpdesk are a sure sign of compliance

…passwords are free but not cheap
Password Management Hits the Mainstream

DILBERT®

BY SCOTT ADAMS

© UFS, Inc.
How to Overcome Password Policy Challenges?

- **Password synchronization – make them all the same**
  - Users required to enter the same password
  - Back end connectors/scripts to sync password changes
  - Password strength determined by “weakest” app

- **Reduced Sign On using LDAP, Kerberos, AD**
  - Front end application modifications required
  - Difficult/Impossible with legacy or COTS applications
  - Costly to maintain the connectors
How to Overcome Password Policy Challenges?

- **Password vaults**
  - Store the password in an encrypted vault accessible by strong password
  - Users enter the appropriate login credentials into the application
  - Passwords in the vault must be kept in sync with application passwords
  - A lost vault denies access and compromises security

- **Automation through scripting**
  - Custom develop scripts to monitor for application launch and then deliver logon credentials
  - Difficult to recognize screen context for all applications
  - Costly to maintain the scripts
  - Inadequate data security for credential creation vulnerability

- **Replace with Biometrics, Tokens, or Smart Cards**
  - Difficult to interface with existing applications

Is Single Sign On the Answer?
Previous SSO Solutions

- **Require extensive scripting**
  - Build front-end or back-end connectors to each application for SSO
  - Leaves administrators with maintenance of SSO scripts
  - Password sync can result in lower password security

- **High Total Cost of Ownership**
  - Months to implement – years to roll out
  - Need to maintain connector code as SSO applications change over time

- **Difficult to Use**
  - Requires system changes and security expertise to properly setup
  - Train users to interact with SSO program

- **Solution designed for F1000**
What is Enterprise Single Sign-On (ESSO)?

- Single system authentication leads to seamless access to all enterprise applications
  - Windows/Client Server
    - Java, VB, C++, custom controls
    - Legacy and Host Applications
    - Terminal emulators, Command line, Telnet, SSH
  - Web based Applications
    - Internal and 3rd party hosted apps – Javascript, Applets, Active X, Web Dialogs
  - Server-based computing
    - Terminal Servers, Citrix, Web-to-Host sessions

- Allow application access only from within a secure session:
  - Authenticate user to the network for an ESSO session
  - Manage and monitor application access within the session
  - Automated entry of stored passwords to known logon forms
  - Automatic synchronization of credentials following password changes
  - Log application access and credential use by user
  - Monitor session locking for inactivity or walk away events

- Removes the user from having to know, manage or enter credentials
- Provides a security model for storage, transport and delivery of credentials
How ESSO Supports a Password Policy

- **Adoption – policy compliance made easy**
  - Users end up with 1 or no password to manage

- **Audit**
  - Centralized, easy for admin, and transparent to users
  - Automation enforces password policy without user burden
  - Reports SSO applications use by user’s system identity

- **Administration**
  - Application passwords managed transparently under central policy
  - SSO-enablement controlled by central policy

- **Helpdesk help**
  - 1 primary authentication mode to support
  - Self-service password reset eliminates Monday morning calls
  - Minimal training or changes for user desktops
The Business Case for Solving the Problem

- **Hard Savings**
  - Helpdesk/IT cost reduction (calculator)
  - Reallocate IT resources onto tasks with business impact

- **Increased Productivity**
  - User productivity increased
  - User satisfaction increased

- **Enhanced Security and Compliance**
  - Security posture improved
  - Audit and regulatory compliance improved
ESSO in for City Hospital

**Problems:**
- HIPAA compliance creating PW mgt headaches for Doctors
- Clinician downtime during PW change process
- User complaints and loss in productivity

**Requirements:**
- ESSO must support legacy systems without code modifications
- PW change process must be automated for users
- Must support shared workstations in clinical areas
- Walk away workstation locking – either manual or automatic

**Imprivata OneSign Solution:**
- ESSO support for ALL clinical systems – especially legacy applications
- Automated PW change management
- Shared workstation with ESSO enabled for HIPAA compliance
- Finger biometric identification or active proximity cards
- Clinicians praising IT
City Hospital – ESSO Implementation Objectives

- Regional Hospital with 1000 Employees
- Handles 8000 inpatients and 150,000 outpatients per year
- Heavy dependency on Meditech – 600 users

ESSO Objectives:
- Meet HIPPA Security requirements
- Decrease Helpdesk password calls
- Eliminate need for multiple passwords
- Provide application usage reports by user
- Enhance user authentication modalities
- Offer Self-Service password reset
- Low initial investment – deploy quickly
City Hospital – ESSO Program

- **Evaluation:**
  - SSO enable critical apps – Meditech (HIS), Stentor (PACS), IT Call support apps
  - Two days for setup and training

- **Pilot group:**
  - Small group of IT savvy physicians and nurses
  - 2 week test period – watch for difficulties or problems
  - Users have willingness to try – computer literacy not required
  - Proactive Approach of working with users – “go to them”

- **Departmental rollout:**
  - Clinical departments first
  - Business departments as needed

- **Customer reaction:**
  - Easy of use – no need for user training
  - Convenience – no need to remember or enter passwords
  - Compliance – meets HIPPA needs
ESSO Technology today

Imprivata OneSign™ is an easy, smart and affordable Enterprise Single Sign-on appliance for mainstream IT organizations that need to quickly and effectively solve password security and user access issues.
Questions?

Stephen Furstenuau
sfurstenuau@imprivata.com
(781) 674 2713

sales@imprivata.com