

The Ubiquitous Password Problem

How 3 companies are solving it with SSO

*Presented by: Bill Moore
Tribridge, Inc.*

“Risk and security is nearly always top of mind among CIOs; indeed, among the top 10 IT priorities in the TechTarget study were three types of security projects (network security, identity and access management and endpoint security – each with implementations planned for 2009 at about a third of respondents' organizations). **In a challenged economy, disgruntled or soon-to-be-former employees pose more risk than ever, and crime tends to rise. So don't be caught unaware.”**

Anne McCrory – Managing Editor, TechTarget

Why Have Passwords Become so Problematic?

In 2000

Today...

| | | |
|--|---|---|
| User Convenience | The average corporate user had 2 passwords | Average user has 10-15 passwords to remember |
| Regulatory compliance | NO regulations | SOX, HIPAA, GLBA, PCI, FFIEC, Global issue |
| Password Security | 90% of companies had no password policies | Companies are either: thinking about; trying to; or have implemented PW policies |
| Control over information access | Access limited to within the enterprise | ASP's, third-party web applications, remote users |

The Truth About Passwords

- **“Good” Passwords are designed to be user unfriendly**
 - Simple passwords are weak
 - Complex passwords are stronger but difficult to remember
 - Confusion across numerous passwords
- **Social engineering can defeat most password security**
 - Using the same password for all applications
 - Sticky note reminders for credentials
- **Password change events cause loss of productivity**
 - Average user maintains 7-10 changing passwords
 - 50% of Help Desk calls relate to forgotten or incorrect passwords
 - Average of 45 minutes lost productivity
- **Roaming and remote users constantly re-enter credentials**

Login Password:

Confirm Password:

Enable Password:

Confirm Password:



What is Enterprise Single Sign-On (ESSO)?

A single authentication to the network providing seamless access to a full range of enterprise applications, including:

- **Windows/Client Server**

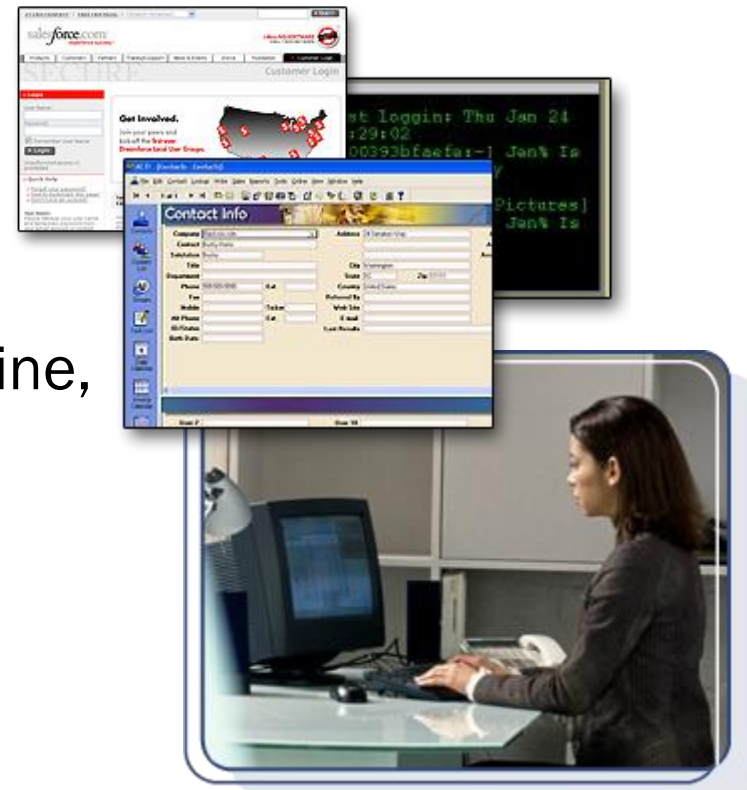
- Java, VB, etc.

- **Legacy Applications**

- Terminal emulators, Command line, Telnet, etc.

- **Web Applications**

- Including 3rd party hosted/ ASP



How are people solving the Password Problem?

- **Summary**

- Vacation Club Division - Hilton Hotels Corporation
- Over 3,900 employees across 50 locations worldwide

- **Problem**

- Too many password resets
 - Running around 2,000/month
 - Made up 60% of all help desk calls
- Large heterogeneous environment – Windows, Sun, Unix, Linux
- More effectively utilize IT Resources

- **Initial objectives**

- Dramatically reduce password resets
- Provide greater user convenience



- **Requirements**

- Work with Windows, Unix, Solaris, and Linux applications
- Ease of configuration and roll-out
- Low cost of on-going management and maintenance

- **Results with Imprivata OneSign**

- Fast deployment with dedicated appliances, low on-going maintenance
- Rolled out to all 3900 users
- Complete SSO to all their applications - no scripting
- Reduced password resets by over 30% in the 1st month
- Users were delighted

- **Unexpected Benefits**

- No need to establish User Training Course
- Enabled use of strong password policies

- **Summary**

- Named one of Top Cancer Centers in America by US News & World
- Based in Tampa, Florida
- Admits over 200,000 patients annually

- **Problem**

- Need to comply with HIPAA requirements
- Over 100 individual applications in use

- **Initial objectives**

- Provide secure passwords for each individual user
- Maintain HIPPA compliance while allowing shared workstations

- **Requirements**

- Affordable solution with fast deployment
- Easily extensible to over 100 applications
- Ability to be managed in-house

- **Results with Imprivata OneSign**

- Rapid initial set-up time
- Rolled out to over 2,600 users & 300 researchers
- SSO to over 100 applications
- Dramatically improved end user productivity

- **Unexpected Benefits**

- Patients can now access their own data
- Strong passwords now enforced in all systems

- **Summary**

- “Florida’s Most Convenient Bank”
- 100+ Locations
- Over 2,300 customer facing , management and administrative employees

- **Problem**

- Increasing complexity of multiple systems
- Teller frustration of constantly logging in/out of critical applications
- Rising help desk costs

- **Initial Objectives**

- Reduce employee password burden
- Strengthen access security
- Regulatory compliance



Florida's Most Convenient Bank

- **Requirements**

- East to install and run
- Low cost to implement and maintain
- Ability for tellers to share workstations

- **Results with Imprivata OneSign**

- Rolled out to smaller locations with very positive results
- Deployed to 100 locations in two months
- SSO to all critical applications
- High user satisfaction

- **Unexpected Benefits**

- Compliance with SOX privacy mandates
- Enhanced customer service by increasing teller productivity



Florida's Most Convenient Bank

- **User adoption will make or break you – make it easy**
- **Choose an IT champion within the user community**
- **Design to streamline user workflow**
- **Provide a choice of authentication modes for users/roles**
- **Standardization of devices will help you**
- **You can never have too much communication/ education/promotion surrounding your implementation – Users Love It!**
- **Educating everyone once and one way is not enough**
- **Holding the users' hands can take some time - but can help keep you employed**

Imprivata OneSign

Seamless, Integrated Capabilities

Authentication Management



Single Sign-On/Password Mgmt



Monitoring and Reporting

| | | | | | |
|-----------------------------|---------------------------|-------------------------------------|---------------------------------------|-------------------------------|----------------------------|
| 8:15 AM Entered building | 8:27 AM Entered Zone A | 8:35 AM Authenticated to Network | 10:10 AM Logged into Application Y | 5:15 PM Logged off Network | 5:32 PM Exited Building |
|-----------------------------|---------------------------|-------------------------------------|---------------------------------------|-------------------------------|----------------------------|

Location-based Authentication



Which clinician accessed what, when, and *from where*



Questions?

Authentication – Its all about identifying the user



What you know:

- Passwords
- Strong passwords



What you are:

- Fingerprint
- Iris scans



What you have:

- ID Tokens
- Smart Cards
- Passive Proximity Cards
- Active Proximity Cards



Where you are:

- Converged logical-physical access
- RFID tags

Technology is only part of the solution – understanding your user requirements is critical