

Biometric Secure Single Sign-On Demonstration

Presented to:
Ohio HIMSS



Page 1

Agenda

- Introduction
- Challenges
 - Traditional Security
 - Password Management
- Biometrics Advantages
 - Single sign-on
- Q&A
- Next Steps

Page 2

Problems With Traditional Security



- Secure tokens can be stolen
- Passwords can be compromised
- Digital certificates are password protected

Page 3

Password Management

- Morgan Keegan Report, "Biometrics & Natural Interface Technologies" mentions the cost factor about passwords:
 - "We estimate that 25-35% of all calls received by IT help desks involve password issues and cost between \$100 and \$200 per user per year. IT workers are a precious commodity and do not need to be spending there time keeping workers passwords straight."

Page 4

Password Management Impacts:

- Help desk time and resources
- IT administration time
- Employee productivity
- Management time and resources
- Plus, BackOffice risk

Page 5

Password Business Case

What are the costs of a 30 minute password incident?

Resources consumed by the solution are:

1. User's time	30 minutes	=	\$16.35
2. Telephone	30 minutes	=	\$.50
3. Call Desk time	15 minutes	=	n/a
4. Call Desk IS facilities	1 call	=	\$18.00
5. Management time	15 minutes	=	\$ 8.18
6. Management IS facilities	15 minutes	=	\$ 1.50

Total resources consumed by a 30 minute solution = \$44.53

Price Waterhouse Coopers

Page 6

Password Business Case

What resources are idled by a password incident?

Resources idled by this problem are:

1. User productivity 30 minutes = \$16.35
2. User IS resources 30 minutes = \$ 3.00
3. Call Desk productivity 15 minutes = \$ 8.18
4. Management productivity 15 minutes = \$ 8.18

Total cost of resources idled = \$35.71

Total cost of one 30 minute password incident = \$80.24

Costs of Fraud are Real

Type of Crime	% Victimized	Average Loss Per Incident
Unauthorized Insider Access	55%	\$143,000
Theft of Proprietary Information	26%	\$1,848,000
Telecom Fraud	17%	\$27,000
Financial Fraud	14%	\$1,471,000
System Penetration by an Outsider	31%	\$103,000
Sabotage of Data or Networks	19%	\$164,000
Denial of Service	32%	\$116,000
Insider Abuse of Net Access	97%	\$93,500
Telecom Eavesdropping	13%	\$76,500
Virus Infection	90%	\$45,500
Active Wiretapping	2%	\$20,000
Laptop Theft	69%	\$87,000

1998 Computer Security Institute and the FBI
521 companies surveyed and 31% responded with specific cost data

Biometric Log On

- Multiple biometrics were considered.
 - ▶ Finger, iris, and face
 - ▶ Biometric chosen will depend highly on environment
 - Office versus operating room
 - ▶ Advantages and disadvantages of each type of biometric
- Introduction of biometrics adds an enrollment step for new employees.
- Biometric needs to be stored in order to do comparisons later for log on.

Fingerprint as a Biometric

- Most widely used biometric in industry today
- Advantages
 - ▶ Many vendors and implementations
 - ▶ Advantages and disadvantages well known
 - ▶ Most inexpensive
 - ▶ Relatively easy for users to learn how to use
- Disadvantages
 - ▶ Clinical and hospital settings may not be applicable
 - Use of gloves
 - Constant washing and powders used in gloves dry fingers too much to be read
 - ▶ More expensive fingerprint scanners can help compensate

Iris as a Biometric

- Not as widely used in industry today
- Advantages
 - ▶ Considered the most accurate of the 3 biometrics
 - ▶ Non-intrusive
 - No physical contact to pass germs
 - No intensive light into the eye (as seen in movies) for retina scans
 - ▶ Slightly more difficult for users to learn how to use
- Disadvantages
 - ▶ Limited number of vendors
 - ▶ Some demographics are more difficult to capture
 - More expensive cameras help mitigate
 - ▶ Most expensive of the 3 choices

Face as a Biometric

- Not as widely used in industry today for log on applications
- Advantages
 - ▶ Most non-intrusive of all the biometrics
 - ▶ Easiest for users to use
 - ▶ No physical contact to pass germs
- Disadvantages
 - ▶ Limited number of vendor support for face for log on
 - ▶ Most inaccurate of the 3 biometrics
 - ▶ Some demographics are more difficult to capture

Biometric System Components

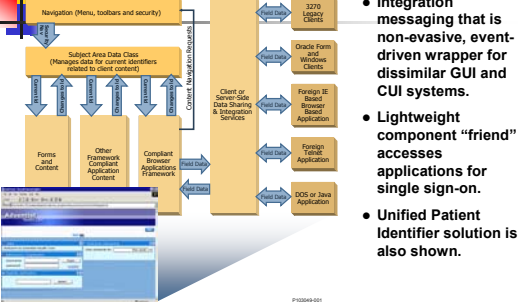
- Hardware and Software Components
 - ▶ Some sort of scanner is required to attach to all PCs, Macs that require log on to other systems
 - Fingerprint scanner or an iris or face camera
 - ▶ Software to support the scanners
 - Software to support biometric enrollment
- Will require the storage of the biometric in some database
 - ▶ May be able to store the biometric image in an existing NIH LDAP or Active Directory

Page 13

Single Sign-On

Page 14

Using a "Friend" in a Web-enabled Environment



- Integration messaging that is non-invasive, event-driven wrapper for dissimilar GUI and CUI systems.
- Lightweight component "friend" accesses applications for single sign-on.
- Unified Patient Identifier solution is also shown.

Page 15

Objective

- Ability to use technology as a secure biometric single sign-on to access disparate clinical systems
- Artificial intelligence use
- Biometric management Directory/LD

Page 16

Advantages of Single Sign-On with Biometrics

Biometric log on

- Simple and quick
- More secure
- Eliminates need for users to remember passwords
- Biometric device independent
- Reduces costs by reducing the need to administer passwords
 - ▶ Password resets, password administration
 - ▶ Does not eliminate password administration completely
- Open standards
 - ▶ BioAPI

Page 17

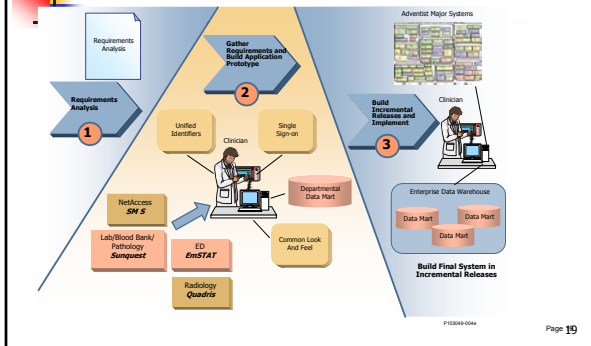
Advantages of Single Sign-On with Biometrics

Single Sign-on

- Simple and quick
- Cost effective, non-invasive adaptation of current applications
- Access all password-protected applications with a single sign-on
- Secure from desktop to application
- Auditable
- Hardware/software vendor neutral
- Lightweight front-end
- Open standards
 - ▶ SSO Client Certificate for Portals

Page 18

Typical Hospital Information Systems Environment



Page 19

Biometric Applications

- Today:
 - Personnel movement in facilities
 - Prison release and booking
 - Back office protection
 - Immigration fast pass
 - Time and attendance
- Emerging
 - ATMs
 - At-home banking
 - On-line trading
 - Medical record access and audit
 - Air passenger boarding and baggage
 - Drug dispensing

Page 20

Very Large PBM Success Story

Raytheon

21

PBM Background

- Business to Business, Healthcare, Pharmaceuticals Distributors providing prescription benefit & patient health management programs.
- The nation's leading provider of high quality, affordable prescription drug care serving more than 65 million members.
- Clients include Fortune 500 corporations, unions, HMOs, BCBS plans, insurance carriers & similar organizations providing health benefit coverage.

Page 22

PBM Background

- Educational programs & sophisticated information systems link patients, pharmacists & physicians, to ensure appropriate drug use for each individual based upon their health profile, best clinical practices & benefit plan coverage.
- Weekly dispense nearly 1.2 million prescription drugs through their mail order service pharmacies, & manage another 6 million more drug claims from retail stores, that are part this PBM's Network.
- Services are designed to help control total health costs, improve quality of care, & increase member satisfaction.

Page 23

Business Issues

- Operate 14 in-house pharmacy operation units in 11 states with over 6,000 pharmacists filling over 50,000,000 prescriptions per year.
- Must conform to the regulatory & security requirements of the Board of Pharmacy regulation for each state in which they operate.
- Many states require mandatory 2 factor authentication for pharmacists as part of the logon process to the IT network & application programs.
- 2 factor authentication used:
 - NT password & SecurID token

Page 24



Business Problem

- Modernize & automate workflow to gain higher levels of cost effectiveness.
- Increase data security to conform to the demands of HIPAA & various state regulatory agencies.
- Link workflow actions to specific individual pharmacists in their pharmacy database application which maintains subscriber medical records, billing information, drug interaction databases, & workflow history.

Page 25



Biometric Solution

- Increased convenience
 - Provided pharmacists with fast & easy access to IT network & application programs
 - Increased user satisfaction by simplifying the logon process (fingerprint)
- Increased security
 - Added stronger authentication by deploying fingerprint authentication for both pharmacy database application logon & linked workflow actions to specific pharmacists
 - Enabled dynamic policy-based authentication
 - Conformance to HIPAA demands & state regulatory agencies
- Reduced costs and complexity
 - Simplified implementation of strong user authentication
 - Streamlined authentication management
 - Replaced SecurID as secondary authentication method
 - Reduced costs by decreasing seconds through simplified logon solution

Page 26



Implementation Success

- Installed BAS server & database in 12-minutes on a Compaq Fiber Optic SAN
- Enrolled 800-Users in 2-methods with an average of 2-fingers/per hand for fingerprint & set Biometric passwords over 3-day period
- Enrollment process completed in under 2-minutes/PP
- WAN response time between 2-States in Midwest and Northeast in under 3-seconds
- Client reports virtually no problems with Biometric solution and fingerprint devices

Page 27



CONTACT

Joyce Hunter
Vulcan Enterprises
301-384-0699
Joyce.hunter3@verizon.net

Page 28