Port Operations, Safety, Information Technology Seminar

Biometrics 101

Brad Jenson  Port of Seattle
Walter Hamilton  IDTP
Christer Wilkinson  DMJMH+N

April 25 1:30pm
Jacksonville FL

April 24-26
Christer Wilkinson

DMJM H&N | AECOM

christer.wilkinson@dmjmhn.com

Access Control

April 25
1:30pm
Jacksonville FL
Typical card reader
Typical Door
Typical Access control system
Typical Access Control System panel
Typical Access Control System Panel

<table>
<thead>
<tr>
<th>Total possible devices</th>
<th>NS2+</th>
<th>N-1000-III</th>
<th>N-1000-JV</th>
</tr>
</thead>
<tbody>
<tr>
<td>Readers or Keypads</td>
<td>2</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>Card PIN/Keypads</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Door Sensor</td>
<td>2</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>Request-to-Exit</td>
<td>2</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>Locking Relay</td>
<td>2</td>
<td>2</td>
<td>4</td>
</tr>
</tbody>
</table>

NOTE: Only one door shown. Up to two doors are supported by the NS2+ and N-1000-III, four doors by the N-1000-JV.
Typical current technology reader
Typical proximity technology reader
Typical cards
Biometric technology reader
Double sided door for zone control
Anti Piggybacking

April 25
1:30pm
Jacksonville FL

April 24-26
Jacksonville FL
Anti Tailgating
Anti Tailgating

April 24-26  
Jacksonville FL

April 25  
1:30pm
Airport Experience

- Access control has been regulated since late 80s
- Regulations updated in 1992 and 2001
- Subject to continuous SD changes
- Initial trial TWIC programs 2001-2006
Scale of Airport Systems

- 475 regulated airports
- Estimate of 400 ACS systems
- Estimate of 75,000-100,000 access controlled points
- Estimate of 5,000,000 card holder data records.
- Estimate of 2,500,000 active card holder records
Airport System characteristics

- Mostly internal doors
- About 15% external
- Many doors per airport (LAX has 1200)
- Most do not have Biometrics
- Most do not use smart cards
Biometric selection at Airports

- Seatac finger print
- SFO hand geometry
- Boston Finger print
- Sarasota Finger print

Plus numerous test sites
Environmental problems

- Cleveland  Snow
- Phoenix    Heat and Dust
- Miami      Humidity

Result: move to contact-less card
Walter Hamilton

whamilton@idtp.com

April 25
1:30pm
Jacksonville FL
Fundamentals of Biometrics
Biometric Overview

**Biometrics:** “Automated recognition of individuals based on their behavioral and biological characteristics”

Examples of Biometric Types:

- Fingerprint
- Face
- Iris
- Hand
- Signature
- Retina
- Speech
- Keystroke
- Palm
- Veins
- DNA
- Skin
Three Basic Functions

Enrollment
- Adding biometric information to a data file
  - Can include screening for duplicates in database

Verification (one-to-one)
- Matching against a single record
- Answers "Is this person who they claim to be?"

Identification (one-to-many)
- Matching against all records in the database
- Answers "Do we have a record of this person?"
How do Biometrics Work?

**Enrollment:**
- Present biometric
  - Capture
  - Process
  - Store
  - Match
  - No Match

**Matching:**
- Present biometric
  - Capture
  - Process
  - Compare
  - Match
Biometric System Components

What do I need to make it work?

- Capture device (sensor)
  - Fingerprint reader, video camera, etc.

- Algorithms
  - Processing (feature extraction)
  - Matching

- Repository
  - Place to store enrolled biometric templates (for matching)
  - Should be protected (secure area, signed/encrypted, etc.)
Reasons to Use Biometrics

Biometrics link an event to a particular individual
   – Not just to a password or token

Convenient – nothing to remember

Can’t be guessed, stolen, shared, lost, or forgotten

Prevents impersonation
   – Protects against identity theft
   – Higher degree of non-repudiation

Enhances privacy
   – Protects against unauthorized access to personal information

Complementary with other authentication mechanisms
   – Smart cards
   – Proximity cards
   – PIN entry pads
Biometrics in Ports

Employee and authorized worker access to secure areas of port facilities and vessels
Employee access to information systems
Employee timekeeping
Employment background vetting
What Makes a Good Biometric?

Unique
Permanent
Easy to use
Fast
Accurate
Low cost
Positive public perception
Biometric Technologies Suitable for Access Control Applications
Fingerprint Recognition

Measures characteristics associated with the friction ridge pattern on the fingertip

One of the oldest and most widely used biometrics

Capture techniques
- Flat scan
- Swipe across
- Rolled (“ten print”)
- Slap (four flat fingers at a time)

Sensor types
- Optical
- Multi-spectral imaging
- Silicon
- Ultrasonic
Fingerprint Recognition

Features

- Mature - proven
- Each finger is unique
- Patterns don’t change with age
- High accuracy
- Easy to use with some training
- Supports both 1:1 verification and 1:N identification
- Databases already exist for background checking
- Numerous vendor choices

Considerations

- Small % of population have poor prints due to injury, age, disease, or occupation
- Requires physical contact with sensor
- Historical association with law enforcement
Fingerprint Minutiae Template

Starts with fingerprint image
Typical size 70-90 KBytes
Fingerprint Minutiae Template (cont.)

Find Minutiae:
- Ridge Endings
- Ridge Bifurcations
- Ridge Direction

Assign values to Minutiae:
- \( X, Y \) position in coordinate space
- \( \Theta \) (Theta) angle from the minutiae point along the ridge
Fingerprint Minutiae Template (cont.)

Generate template record
Store in template repository
Typical size <500 bytes
Iris Recognition

Measures features associated with the random texture of the colored part of the eye
Measures up to 266 unique features
Uses near infrared sensor from a distance of 6 in. to 2 ft.
Popular for facility access and transportation/border security
Iris Recognition (cont’d)

Features
- Highly accurate
- Very stable over lifetime
- Works through glasses and contacts
- No physical contact required
- Not affected by common eye surgeries
- Less prone to injury
- Supports both 1:1 verification and 1:N identification

Considerations
- Can be obscured by eye lids, lashes, reflection
- Public perception that scanning may be harmful
- Can be difficult to capture
  - Requires more training
- No existing database
Hand Geometry

Measures dimensions of hand, including shape and length of fingers
Used extensively for physical access control
  – Installed at SFO
Also widely used for employee timekeeping
Hand reader configuration
  – Typically lay hand flat
  – Pegs guide placement
  – Cameras positioned above
    and to side
Hand Geometry (cont’d)

Features

- Easy to use
- High public acceptance
- Very low Failure to Enroll Rate
- Proven over many years of use
- Primary applications are physical access and time/attendance
- Very small, adaptive template
  - Fits on any card media
- Works well in outdoor environments
- Rugged

Considerations

- Not as accurate
- Characteristics may change with age
- Best used in 1:1 contexts
- Sensor is relatively large
Is There One Best Biometric?

No - A biometric should be selected based on specific application requirements

Each technology exhibits differences in

- Cost
- Ergonomics
- Matching accuracy
- Physical packaging
- User acceptance
- Maturity
Accuracy

Generally defined in terms of two parameters:

- **False Reject Rate (FRR):**
  - Measures how often an authorized user, who should be granted access, is not recognized
  - FRR = Percentage of false rejections of the total number of valid recognition attempts
  - Also called “False Non-Match Rate”

- **False Accept Rate (FAR):**
  - Measures how often a non-authorized user, who should not be granted access, is falsely recognized
  - FAR = Percentage of false acceptances of the total number of imposter recognition attempts
  - Also called “False Match Rate”
Accuracy (cont’d)

Equal Error Rate (EER):

- Point where FRR = FAR

FAR/FRR are inversely related
Match Score distribution

Non-matching

Matching Threshold

Matching

False Rejects

False Accepts

(imposters)

(legitimates)
Additional Performance Consideration

Failure to Enroll Rate (FTER)
- Measures how often users are unable to enroll a biometric characteristic
  - Physical characteristic of user prevents creation of template
    - Characteristic not present or obscured
  - User is not capable or willing to present biometric properly

FTER = Percentage of failures to enroll of the total number of enrollment attempts
Biometrics & TWIC

Biometric credential for maritime workers mandated by Maritime Transportation Security Act

Ten finger images captured for background check
Two finger images converted to minutiae templates and stored in chip memory of TWIC card
Readers will use contactless interface to transfer templates to reader for matching

Expected reader performance requirements
– Must be capable of working in harsh maritime environment
– Transaction time of 3 seconds or less
– Matching accuracy of at least 99%

Coast Guard and TSA planning pilot reader tests in 5 locations this year
– Mandated by SAFE Ports Act
Seattle-Tacoma International Airport (SEA)
Seattle Seaport Harbor
Fishing and Pleasure Boat Moorage
Cruise Terminal Facilities
Other Commercial Operations
Seaport Statistics - 2006

Total TEU Containers: 1,987,360
Total Cruise Passengers: 735,000

Total Vessel Calls:
Container – 814  Cruise - 196

1,200 Active Cardholders
Access Control deployed March 2004

Source: www.portseattle.org
Airport Statistics - 2006

Total Air Passengers: 29,979,097
Total Aircraft Operations: 340,058
Total Air Cargo (metric tons): 341,844
15,000 Active Cardholders
Biometric Cards October 2003

Source: www.portseattle.org

April 25
1:30pm
Jacksonville FL

April 24-26
Changes in ID Badge Technologies

Photo Technology... Specialized PC Technology...

April 25
1:30pm
Jacksonville FL

April 24-26

AAPA
American Association of Port Authorities
Alliance of the Ports of Canada, the Caribbean, Latin America and the United States
Security System Technology Changes

- Proprietary solutions gave way to Windows desktop standards
- Use of standard SQL databases rather than proprietary or desktop-grade file systems
- Field devices, door readers may be IP addressable
- Wireless technology
- The IT department meets the Security Department
What IT Can Offer

• System integration skills. Was a non-issue in the proprietary era

• Setting technology standards to reduce maintenance costs

• Handle data privacy issues. Systems may now require more PPI

• Best practices for cyber security & evaluating vendor compliance
The Port of Seattle had plans to construct and implement a new access control system at Seattle-Tacoma International Airport using standard proximity card technology. This new system was critical to completion of a $587M airport terminal expansion project.
But the world changed... and so did we
Following 9/11

• Increased focus on biometrics
• Emphasis on identification and authentication of transportation workers – TWIC emerges on scene
• Formation of the TSA, DHS, etc
• Development of information sharing networks and systems
• Grant funding for Seaport Security
Our directives...

• In light of 9/11, reevaluate our plans
• Install a forward looking biometric solution
• Identify and recommend viable, cost effective biometric technologies
• Insure that it would not jeopardize airport terminal construction project
• Integrate into existing project for access control system replacement
Reasons for Our Biometric Success

• Stakeholder involvement
• Scheduled/Managed Re-issuance
• FAQ’s provided to cardholders
• Running in parallel with old ACS
• Cardholder used test reader first
• Skilled and dedicated team
• Examined Privacy Concerns
• Labor Relations Issues
Seattle’s Card Reader:
BIO, PIN, LCD, MIFARE

April 25
1:30pm
Jacksonville FL

April 24-26

AAPA
American Association of Port Authorities
Alliance of the Ports of Canada, the Caribbean, Latin America and the United States
Non-Bio Card Reader: 
Card Only, or Card + PIN

- Less Expensive
- Compatible with same ID card
- Non-critical uses
- Be sure to plan for both bio and non-bio reader
Interoperability and Transition

Can your legacy access control system run in parallel with a new system during installation?

Can it be upgraded to utilize biometric technologies?

Is this the mandate you always wanted to replace a legacy system?
Biometric Readers: Wiring and Power Issues

- Biometric smart card readers are like small computers
- Higher power requirements
- Infrastructure must support required UPS/Battery backup
- New readers *may* require more wire strands than you have now or maybe wire is OK as is
Corporate ID/ Access System

Will EVERY employee requiring electronic facility access really NEED a TWIC?

Can your existing ID badge system enroll external cardholder credentials?

Will “corporate” cards share TWIC readers?

Does the existing system meet current computing standards and can it quickly adapt to a changing world?
If you adopt TWIC as the solitary Port ID card... Will that compel all types of cardholders to enter the TWIC system?
Badge Failure points

Encoded biometric data no longer matches cardholder due to finger damage

Hole severs antenna or lanyard wears through antenna

Cardholder punches their own hole to fit their preference

George Washington
Expires 7-4-2076
Cardholder Actions That Can Kill a Card

• Inform cardholder that punching holes in a card will damage it

• Educate cardholder that certain lanyards with metal clasps could damage card

• Educate guards to recognize dead cards
Biometric Deterioration

- Deteriorating finger quality due to abrasion, injury, hobbies, etc.

- If the finger (and the spare) no longer match, the cardholder will be denied access

- May require reproducing card (another trip to the TSA TWIC issuing facility)

- Seattle: Approximately 2 per month
Failure to Enroll

- Certain cardholders will be physically unable to render a biometric
- Our failure rate is 0.42%
- Not tied to any demographic
- An alternative to biometrics must be provided for unattended access points
Perceived cardholder comfort level w/ readers
(Following initial roll-out of biometric cards)

(Per ID Office Mgr)
The Biggest Cause of Reader Problems in Seattle

See next slide for the answer...
The Biggest Cause of Reader Problems in Seattle
Typical Reader Problems We’ve Seen

- Rain in Seattle !!
- Key Pads – Water, Wear & Tear on #
- Ambient light on outdoor reader
- Dirty fingers or dirty read surface
- User error and impatience
- Broken card antenna
- Ergonomics for height on vehicle access
Multi-Height Readers for Varying Vehicle Heights
Consideration of Delays

- What will you do to avoid undesired backups of cardholders due to reader usage problems?

- How will you handle problems, exceptions at the reader?

- Biometric smart cards are NOT the old “swipe and go” world
Possible Exception Handling Techniques

- Very short time out periods
- A “cancel” button on reader
- Corrective prompts on LCD
- Intercoms to guards or support staff
Primary Biometric Lessons Learned

• Educate stakeholders
• Address privacy issues
• Install non-bio readers based on usage
• Account for failure to biometrically enroll
• Staff and cardholder training
• Quality implementation team
• Test, test, test in all environmental conditions
• Consider ergonomic issues
Possible Access Control Challenges Post-TWIC C

Seattle’s Experience

- Homogenous industry
- Primarily Indoors
- Established communication channels to Cardholder
- One primary biometric device to learn
- Sensitized to Federal security requirements

In the world of TWIC

- Diverse industry
- Primarily Outdoors
- Varied and complex communication channels to Cardholder
- Transients: Multiple biometric devices
- Acquiring exposure to Federal Security issues
Q&A and Discussion

April 25
1:30pm
Jacksonville FL

April 24-26
SPARE SLIDES FOLLOW

April 25
1:30pm
Jacksonville FL
Port Operations, Safety, Information Technology Seminar

Spare slides / CHRISTER

April 24-26
Jacksonville FL

April 25
1:30pm
Port Operations, Safety, Information Technology Seminar

Typical access Control system
Components of an access control system

Port Operations, Safety, Information Technology Seminar

April 24-26
Jacksonville FL

April 25
1:30pm
Double sided door for zone control
Port Operations, Safety, Information Technology Seminar

Spare slides / BRAD
A useful resource

Framework for Evaluating and Deploying
Biometrics in Air Travel Applications:
Surveillance, Trusted Travel, Access Control

International Biometric Group  April 3, 2002
Approximate Airport Stats; Excluding Seaport

Badges per month: 900
Total time to enroll: 35 minutes
Biometric enrollment: 30 secs
Deteriorated biometrics: 2 / mo*
Approximately 500+ readers

* Smart card program < 3 years old