Current Issues in Biometrics

US Department of Homeland Security

December 11, 2003
S&T Research Agenda

- Bio-Countermeasures
- Chemical Countermeasures
- Radiological and Nuclear Countermeasures
- Standards
- SAFECOM
- Threat and Vulnerability, Testing and Assessment
- Critical Infrastructure Protection
Initial S&T Emphasis: High Consequence Threats

- Cutaneous Anthrax
- Salmonella Food Poisoning
- Smallpox
- Engineered organisms
- Bulk food Contam
- FMD
- Anthrax

Increasing Sophistication

Increasing Consequence
Differentiating Document and Person Verification

- USVISIT focuses on verification of traveler identity.

- There is currently no effective lost, stolen, fraudulent document process.

- Enhanced International Travel Security (EITS) was conceived to address this and other functions.
  - Concept developed in international workshop sponsored by OECD and ICAO.
  - Privacy advocates played a central role.
  - A number of functions were considered and compared.
  - Lost, stolen, and fraudulent documents are a potential first win.
EITS Sample Application

1. Travel Leg
2. Scan Document #
3. Validation Request
4. Policy Filter
5. Query
6. Red/Green Light

Registry
Travel-Related Biometrics Issues

- **Modality Standard**
  - Face – the legacy biometric for travel documents
  - Fingerprints – huge amount of law enforcement data; fingerprint latency
  - Iris – claimed accuracy
  - Challenge: How to effectively fuse multimodal biometrics?

- **Format Standard**
  - Image
  - Template
  - Challenge: How to develop vendor-neutral templates?

- **Vulnerabilities**
  - Modality spoofing – disguises, etc.
  - Process – insider threat, etc.
  - System – hacking into biometric databases, etc.
  - Challenge: How to design hardened biometric systems?
Exhibit C
Authentication technology

While authentication technologies are improving, no single approach can provide high assurance on its own. There are no smart cards or tokens that cannot be cracked, biometrics are not 100 percent reliable, and high-quality passwords are difficult to remember, manage, and enforce. With all of these technologies there are also people and process issues (such as enrollment procedures and audit trails) that can undermine their integrity. Therefore, a multifactored system is a preferable approach. Multifactor authentication typically combines a password with a token or smart card and can include other forms of authentication including biometrics, challenge codes and questions, and profile access matching. Authentication is strongest when part of the information resides with the user, a part with the token or smart card, and a part in the network. Credit card companies, good users of multifactor authentication, rely on tokens (credit cards), passwords (PIN), challenge questions (“What’s your mother’s maiden name?”), and profile matching (“Is this a typical charge for this individual?”).
Travel-Related Biometrics Issues

- **Modality Standard**
  - Face – the legacy biometric for travel documents
  - Fingerprints – huge amount of law enforcement data; fingerprint latency
  - Iris – claimed accuracy
  - Challenge: How to effectively fuse multimodal biometrics?

- **Format Standard**
  - Image
  - Template
  - Challenge: How to develop vendor-neutral templates?

- **Vulnerabilities**
  - Modality spoofing – disguises, etc.
  - Process – insider threat, etc.
  - System – hacking into biometric databases, etc.
  - Challenge: How to design hardened biometric systems?
Each of the above state-of-play situations with respect to face, fingerprint and iris biometrics all point to storage of the image as being the only reliable globally interoperable method for guaranteeing that a receiving State can process the data provided by the Issuing State against the image of the MRTD holder they capture at their border.

**Recommendation:**

For each biometric type stored in the MRTD, storage of the image is mandatory, and storage of an associated template be optional at the discretion of the Issuing State.
Travel-Related Biometrics Issues

- Modality Standard
  - Face – the legacy biometric for travel documents
  - Fingerprints – huge amount of law enforcement data; fingerprint latency
  - Iris – claimed accuracy
  - Challenge: How to effectively fuse multimodal biometrics?

- Format Standard
  - Image
  - Template
  - Challenge: How to develop vendor-neutral templates?

- Vulnerabilities
  - Modality spoofing – disguises, etc.
  - Process – insider threat, etc.
  - System – hacking into biometric databases, etc.
  - Challenge: How to design hardened biometric systems?
'Operation Tarmac' airport sweep widens

Ashcroft: "A wake-up call for every airport in America"

April 24, 2002 Posted: 3:34 PM EDT (1934 GMT)

From Kelli Arena and Terry Frieden
CNN

WASHINGTON (CNN) -- Federal authorities Wednesday sought to
arrest more workers at Washington
area airports wanted on a variety of
charges, ranging from immigration
violations to fraudulently obtaining
security credentials.

As of Wednesday morning, 96 workers
had been arrested. The United States
Justice Department had said it was
seeking a total 138 people.

None of the workers arrested is suspected of any connection to terrorism,
officials said.

Tuesday, Attorney General John Ashcroft called the arrests "a wake-up call for
every airport in America."

"These individuals are charged with gaining access to secure areas of our
airports by lying on security applications, using false or fictitious Social Security
numbers or committing various immigration frauds," Ashcroft said.
Human Behavior ID for Security

- Measurements of human activity beyond “traditional” biometrics

- Law Enforcement
  - Countering identity theft.
  - Unifying criminal aliases.

- Signatures of hostile intent
  - Casing behavior
  - Deception during screening of travelers, visitors, employees
  - Unusual patterns of activity in secure areas
  - Insider threat
Identity Theft Continues To Increase

NEW YORK, May 15, 2001

(CBS) The FBI calls it "the fastest growing white-collar crime in America."

It's identity theft and it can happen to anyone, even celebrities. Oprah Winfrey, Steven Spielberg, and Tiger Woods, all of whom have had their identities stolen.

When she first reported on the story for 60 Minutes, CBS News Correspondent Lesley Stahl interviewed Mary Zupanc, then a staff doctor at the Mayo Clinic in Rochester, Minn. Zupanc's identity was stolen by a ring of thieves in New York.

Mary Zupanc in 1998: Victim of

Criminal used the DMV for aliases

IDENTITY: Felon repeatedly altered his appearance and thumbprint to obtain 83 driver's licenses.

November 14, 2000

By KIMBERLY KINDY
The Orange County Register

It took the Department of Motor Vehicles over eight years to catch up with the many facets of Ronald Clifton King.

The convicted felon managed to hoodwink the DMV 83 times, securing a driver's license for each of his numerous aliases and using the licenses to bolster his life of crime, according to department and court records.

He was brazen, visiting as many as 10 DMV offices in one day, the 44-year-old repeatedly posed for the department's cameras, using plastic surgery and hair dye to alter his appearance over the years, according to DMV documents, police and interviews with victims.

Each time he'd alter his thumbprint into the DMV computer. Then, law enforcement officials say, he'd wait for DMV to send the license to one of his 20 addresses that spread from Orange County to Riverside County in Northern California.

"It was a shocker. The fact that you can get that many licenses... it was unbelievable to me," said U.S. Postal Inspector Ben Costello, who helped investigate the King case for his agency. "I'm sure it will be a wake-up call for DMV to tighten their policies for getting licenses."
Human Behavior ID for Security

- Measurements of human activity beyond “traditional” biometrics
- Law Enforcement
  - Countering identity theft.
  - Unifying criminal aliases.
- Signatures of hostile intent
  - Casing behavior
  - Deception during screening of travelers, visitors, employees
  - Unusual patterns of activity in secure areas
  - Insider threat
When reporting suspicious activities, the information provided below is pretty much common sense. However, what may not be so obvious are your skills to notice those items. How often have you seen a car drive down the street and you were sure it was a Toyota instead of a Honda? A lot of the car manufacturers produce cars that look very similar to other best selling nameplates.

Reporting suspicious activities are one thing, reporting suspicious activities with detail is another. It takes practice to be come really good at noticing detail. For example: if you were to see a suspicious activity, did you take notice of what time it was? Just noting the time of an event can be extremely helpful to our law enforcement personnel.

Have some fun the next time you’re out and about walking around the neighborhood, try practicing your observation skills. When a car passes you by as your walking down the street, look at you watch (if you happen to be wearing one) to see what time it is, see if you can determine the manufacture of the car, this might not be as easy as you think!

Check out the license plate, what state is it from, is the license plate “personalized”? Does the car have any unique features like chrome rims, or raised letters on the sidwalls of the tires? What dealer did the owner buy the car from? With a little practice you’ll be surprised how much of the little details that you can pick up. And it is the little details that can make the big difference.

Facial Appearance

Write specific facial details below - only what you definitely remember.

Hair color and style
Eye color

Shape
Mustache

Shape and size of nose
Cheek (full or hollow)

Brow

Mouth

Cheekbones

Neck

Adam’s apple

Life-Threatening Emergencies
9-1-1 • Stay on the Telephone • Don’t Hang Up

Gary W. Strong
December 11, 2003
Summary

- **Modality Standard Challenge**: How to effectively fuse multimodal biometrics?

- **Format Standard Challenge**: How to develop vendor-neutral templates?

- **Vulnerabilities Challenge**: How to design hardened biometric systems?

- Measurements of human activity beyond “traditional” biometrics

- **Law Enforcement identity management**

- Detecting signatures of hostile intent