Ensuring Test Integrity and Security with Biometric Verification
Welcome and introductions

Daniel Eyob, CFE, CPP
Director, GMAT Test Security
Graduate Management Admission Council®

Wayne Bailey
Enterprise Architect
Pearson VUE
Agenda

- Pearson, GMAC® and the GMAT®
- Exam identity fraud case study
- The search for an identity management solution
- Initial palm vein implementation project
- Biometrics, privacy regulation and compliance
- 1:N system design and implementation
- Questions
Pearson, GMAC® and the GMAT®
World’s largest education business

- $9 billion revenue
- 70 countries
- 36,000 employees
Pearson VUE

• Global leader in computerized testing
  – Clients in the licensure, certification, academic admissions, regulatory, and government testing service markets
  – World's leading network of over 5,000 test centers in 165 countries
  – Innovative technology offers unparalleled levels of security and program control

• First patented test center design

• First to use biometric verification
Graduate Management Admission Council® (GMAC)

- Opens doors for graduate management programs, professionals & prospective students around the world
- Leading source of research and information about quality graduate management education
- Owner and administrator of the Graduate Management Admission Test® (GMAT)
The GMAT® exam

• Premier standardized test specifically designed for graduate business and management programs
  – 4 hour, computerized exam
  – Available in 110 countries

• Most widely used assessment for graduate management admissions

• A high score can enable admission to the top business schools worldwide
Exam identity fraud case study
GMAT fraud ring discovered in 2003

• Proxy testing ring in US northeast
  – At least 590 exams (GMAT and others) taken over five years
  – Impersonators used fake IDs and forged passports
  – Typical price for the service – $3,000 per attempt

• Three year investigation
  – Ringleader (Lu Xu) served more than 2 years in prison

• Fraudulent GMAT scores sent to business schools worldwide
  – 145 schools were impacted
  – 185 scores canceled
Study confirms widespread cheating on job exams

Secret investigation discovers ‘proxy test takers’ prevalent

By Kevin Gleason and Anne Wenzel
Global Correspondents | July 27, 2011

WASHINGTON - A secret international investigation into job certification test fraud conducted by a major US technology company has confirmed long-held suspicions that thousands of people worldwide are cheating on certification exams for coveted jobs.

Cisco Systems Inc., the Silicon Valley firm behind some of the world’s biggest computer networks, and Pearson Vue, one of the world’s largest test administrators, recently conducted a trial run of an anticheating system intended to identify and crack down on “proxy test takers,” people who impersonate others to take exams for them.

Officials at Cisco and Pearson Vue told The Boston Globe this week that during an eight-month span ended in June 2008, they monitored hundreds of thousands of exams given in eight countries in Asia, Europe, the Middle East, and North America. Cisco said it had confirmed that one in 10 of those exams was taken by a proxy, and not the actual enrollee.

The tests were held at LaM Hong University and Dong A foreign language center in the southern province. The TOEIC and TOEFL exams in question are the local versions only recognized by Vietnamese organizations.

During ongoing investigation into proxy testing in Dong Nai, police found out that the officials had spent VND4-7 million ($US192-336) each to hire many LaM Hong high-performing students to either impersonate them or help them.

The tests have only collected statistics from 3 out of 8 exams that have taken place at LaM Hong University.

Trade management levels at the province’s state departments in order to publish their CVs for promotion purposes, Tuoi said.

Old LaM Hong alumnus Do Tran Le Son, who was found to have a 27-year-old Tran Quang Hung on charges of impersonating him to take the test.

GMAC
A recent survey of MBA candidates in China found...

One in eight considered proxy testing to be acceptable behavior.
Meanwhile, in Long Island...
The next step

• Early realization of issues with fingerprint verification
  – Technology unable to detect/prevent all impersonation
  – ‘Trace’ technology
  – Cultural concerns
  – Legal restrictions in some parts of the world
  – Unlikely to achieve world-wide implementation

• Goals for next generation test taker identification
  – Fairness to honest test takers
  – Help schools admit correct people
  – Eliminate test cheating
  – Global implementation
  – Cultural sensitivity
The search for an identity management solution
Pearson’s approach

• Goals for identity management
  – Migrate from outdated fingerprinting technology
  – Address privacy challenges and concerns
  – Support phased introduction of reliable 1:N matching
  – Differentiate from competition

• Product strategy
  – Define short term needs vs. long term capabilities
  – Understand operational, contractual and legal requirements
  – Engage independent experts to assist with technology evaluation, solution design and integration
  – Consult with outside experts (International Biometrics Group)
Core functional requirements

• Capabilities
  – Candidate enrollment
  – Local verification (1:1)
  – Watch list checks (“No Test List”)
  – Global duplicate/impostor detection (1:N)
  – Enhanced privacy features

• Large scale, fault-tolerant identification
  – Multiple client programs
  – Integration with existing candidate processing systems
  – Enrolled N per client: 10K to millions
  – Exception processing
Initial 3 year roadmap

• Planning
  – Initial technology and operational analysis
  – Technology testing, evaluation and vendor negotiations
  – Technology selection and acquisition for pilot

• 1:1 Verification
  – Software development, documentation and training
  – Pilot planning, rollout, analysis and general deployment
  – Fingerprint retirement

• 1:N Matching
  – Technology selection and acquisition
  – Identification system development
  – General deployment
Initial solution recommendations

• **Fujitsu PalmSecure™ (palm vein) for 1:1 verification and watch list searches**

  ![Fujitsu Logo]

• Hybrid, **multi-modal** solution for duplicate detection (1:N)
  - Use facial recognition to reduce search set
  - Apply palm vein matching to identify candidate
Palm vein implementation project
Palm vein quick primer

① The PalmSecure scanner emits near-infrared light, which is reflected from the palm back toward the sensor.

① The deoxidized hemoglobin in the veins of the palm absorbs some of this light—thereby reducing the reflection rate and causing the veins to appear as a dark pattern in the image captured by the sensor.

② The unique characteristics of the vein patterns are then extracted by the Fujitsu algorithm.

① These are converted to an encrypted template to be used for enrollment and matching.
## Trade-offs involved

<table>
<thead>
<tr>
<th>Biometric</th>
<th>Benefits</th>
<th>Trade-offs</th>
</tr>
</thead>
</table>
| **Fingerprint** | • Accuracy  
• Performance and scalability  
• Inexpensive, interoperable sensors  
• Existing process for Pearson  
• Multiple matching technologies available | • Negative privacy impacts  
• Perceived as invasive  
• Not cutting-edge  
• Cost of high end 1:N matching technologies  
• Enrollment failures unavoidable |
| **Palm vein**  | • Accuracy  
• Contactless operations  
• Positive privacy advantages  
• Cutting-edge perception  
• Tamper-proof | • Performance and scalability  
• One primary solution vendor in market  
• Development needed for 1:N architecture  
• Possible client resistance |
Initial 1:1 implementation

Enrollment & Verification
same/different day

High quality photo capture

Fingerprint as a ‘bridge’

GMAC pilot 2008
Full GMAC deployment 2009
Client migration 2009-2011
System enhancements 2011-2012
Biometrics, privacy regulation and compliance
Biometric privacy and regulation

• General privacy concerns about biometrics
  – Intrusive
  – Permanent – biometric identities are usually not revocable
  – Loss or theft
  – Human rights – surveillance society

• European perspective on biometric data
  – Biometric data is sensitive and requires special handling
  – Processing requires prior authorization in some jurisdictions
  – Transfer outside the EU poses specific challenges
Regulatory compliance strategy

- Appropriate engagement with
  - Internal counsel (Pearson & GMAC)
  - Outside counsel (experts in privacy and biometrics)
  - Current and former privacy regulators

- Phased approach to regulatory approvals
  - Initial discussions with numerous regulators
  - Response to inquiries from Germany, Australia, etc
  - Early EU approvals – Portugal, Poland, Lithuania (2009)
  - French authorization request and approval (2009)
  - Subsequent regulator approvals (2009-2012)
Lessons learned

• Biometrics require ‘strict scrutiny’ compared to other data

• Inconsistent standards/requirements
  – Differences among EU member states
  – Differences within a country (e.g. Germany, United States)
  – Regulatory requirements can change

• Time required to file/receive authorization or respond to an inquiry
  – Sometimes months or years

• Need for proactive investment in relationship and follow-up with regulatory authorities
  – Especially where authorization is needed or there is a risk of complaints/investigations
1:N system design and implementation
Candidate Management

Client Policies & Blocks

Site Management

ID Policies

Signature & Photo Capture

Fingerprint Verification

Exception Management

PalmSecure Verification

Forensic Matching

Image Quality Processing

Existing Identification System

Palm Vein Implementation & Image Ready

ALWAYS LEARNING
1:N solution options

• Original recommendation - multimodal hybrid approach
  – Facial recognition + palm vein
  – Leverage the current candidate data collection process
  – Use face recognition technology to reduce search set
  – Apply palm vein matching to results to identify candidate

• New option – native Fujitsu 1:N
  – Fujitsu released an authentication library with true 1:N support
  – Larger N sets, faster than previous version
  – Possibility of leveraging emerging third-party integrations for scalability and performance
    • M2SYS
    • Sensometrix
<table>
<thead>
<tr>
<th>Solution</th>
<th>Benefits</th>
<th>Trade-offs</th>
</tr>
</thead>
</table>
| Multimodal fusion (Face + Palm) | • Facial recognition: many matchers, faster and more accurate  
• Results can be generated quickly  
• Proven technology: many systems exist  
• Multimodality is a common approach | • Dependent on two technologies  
• Extra integration, testing, points of failure  
• Issues with facial capture reliability  
• Significant privacy risks with facial recognition |
| Native Fujitsu 1:N (Palm) | • Palm vein proven to one of the most accurate technologies  
• Less system complexity  
• No further hardware/training investment required | • Locked into one vendor  
• New technology, may have scalability hurdles to overcome  
• No performance benchmarking available |
Updated product strategy – 2010-2012

- Rejected dual-mode hybrid approach
  - Fujitsu ecosystem had sufficiently matured
  - Concerns about dual-mode privacy, complexity, cost

- Native Fujitsu (PalmSecure)
  - Capture and 1:1 verification
  - Short-term watch list (“NTL”) solution

- Sensometrix solution (SensoBrain)
  - Acceleration/management layer
  - Handles all 1:N functions
  - Long term watch list (“NTL”) solution
High level 1:N architecture

Test Centers
- Test Center Check In
- Testing Server

Operations
- Forensic Matching

Pearson Hub Systems
- Real-Time Web Service
- Biometric Repository
- Authentication Service
- Palm Vein Identification (SensoBrain)

Identity Management System
- Forensic Matching Service

Forensic Matching

GMAC
GRADUATE MANAGEMENT ADMISSION COUNCIL
How it works – No Test List (NTL)

• Small scale 1:N (N = hundreds)
  – Individual compared to biometric identifiers of people on the No Test List
  – Performed locally via a real-time connection to the central matching system

• Blocks individuals on the NTL from being admitted
  – Even if they schedule using a different name and identity
  – Flags records for administrative intervention

• Ensures testers are not
  – Known fraudsters – e.g. proxy testers
  – Other candidates under a ban
How it works – Global duplicate detection

• Large scale 1:N (N = up to 10 million)
  – Individual compared to entire candidate population
  – Queued and performed centrally by matching system

• Ensures individual has one and only one record in the system
  – Identifies any testing event where the candidate matches another candidate’s biometric identifier
  – Flags records for administrative intervention

• Detects and prevents
  – Accidental or intentional duplication of candidate records
  – Proxy testing
Results

• An early pilot (conducted through IBG) detected multiple small scale proxy/duplicate events

• Full SensoBrain 1:N enabled since September 2011
  – Real-time NTL matches have thwarted known offenders
  – Additional proxy attempts detected

• Successful implementation with other Pearson clients
Results

• Proxy Test Takers Identified:
  • 2009 - 56
  • 2010 - 60
  • 2011 - 85
  • 2012 - 37
  • 2013(YTD) - 2

• Duplicate Profiles Identified:
  • 2009 - 23
  • 2010 - 83
  • 2011 - 264
  • 2012 - 619
  • 2013(YTD) - 265
Thank you!

Daniel Eyob
Director, GMAT Test Security
Graduate Management Admission Council®
deyob@gmac.com
www.linkedin.com/pub/daniel-eyob/11/b88/987

Wayne Bailey
Enterprise Architect
Pearson VUE
Wayne.bailey@pearson.com
www.linkedin.com/in/waynebailey