# COMS3000/7003

## Week 4

### Working in InfoSec, Certifications, Biometrics, Access Control

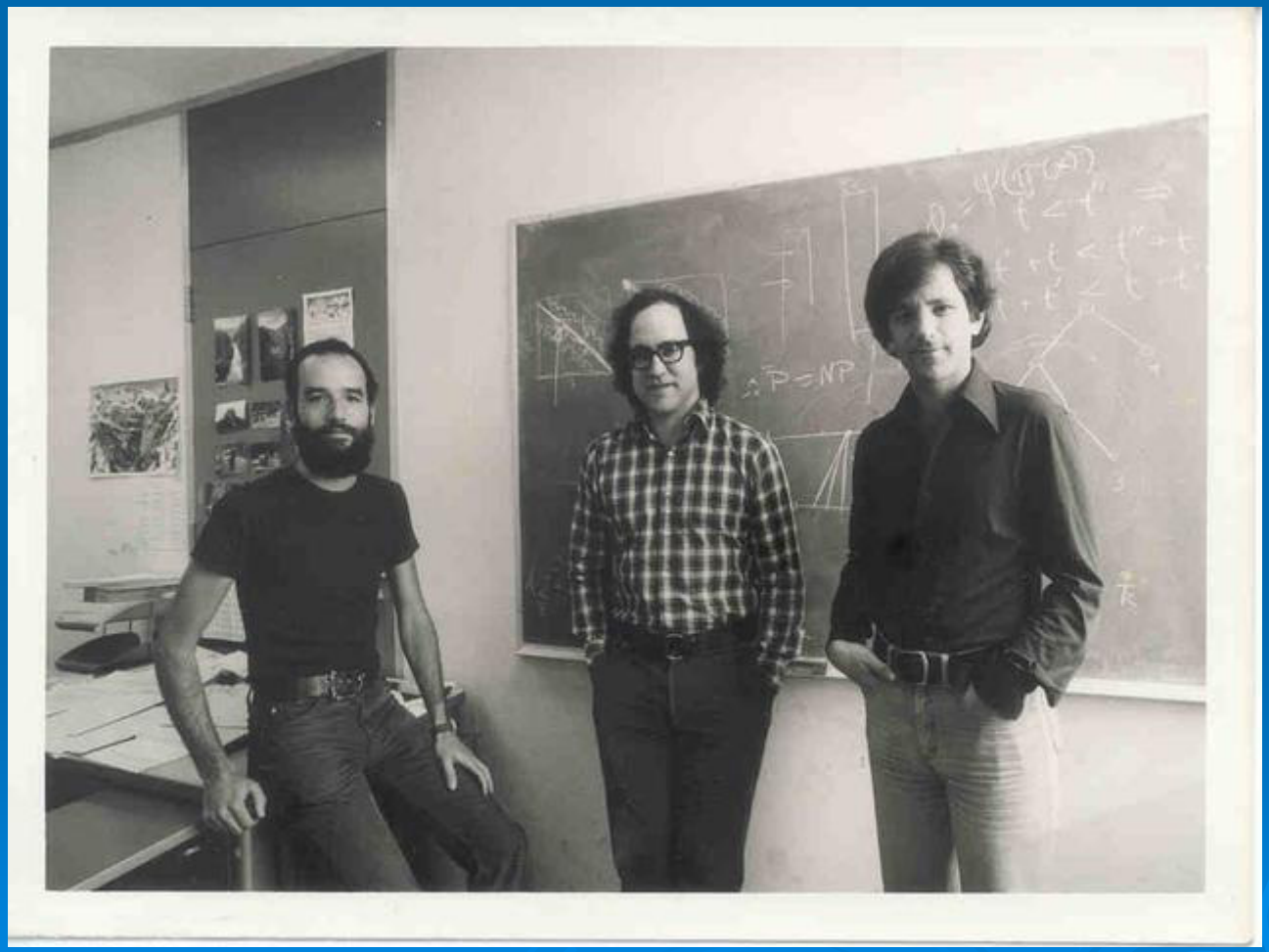
# Assignment

- The journal links only work if you add the UQ Library Ezproxy domain (pre-paid subscription by UQ):
  - http://ieeexplore.ieee.org.ezproxy.library.uq.edu.au/xpl/RecentIssue.jsp?punumber=8013 and
  - http://ieeexplore.ieee.org.ezproxy.library.uq.edu.au/xpl/RecentIssue.jsp?punumber=2

# Hash Functions - Digital Signing

- From RFC1319 *The MD2 Message-Digest Algorithm*:
  - https://tools.ietf.org/html/rfc1319
  - “The algorithm takes as input a message of arbitrary length and produces as output a 128-bit "fingerprint" or "message digest" of the input.”
  - “It is conjectured that it is computationally infeasible to produce two messages having the same message digest, or to produce any message having a given prespecified target message digest.”
  - “The MD2 algorithm is intended for digital signature applications, where a large file must be "compressed" in a secure manner before being signed with a private key under a public-key cryptosystem such as RSA.”

# Hash Functions - Digital Signing




- Adi, Ron and Len circa 1978 (RSA)

# Hash Functions - Digital Signing

- Ron, Whit, Martin, Adi & Moxie two years ago...
  - (not my photo – RSA promo shot)

# Hash Functions

| Name | Invented | By | Size | Attacks | Collision | Pre-Image |
|---|---|---|---|---|---|---|
| MD2 (RSA-MD2) | Jan 1988 | Ronald Rivest | 128 | 1997 | 2009 $2^{63.3}$ | 2004 ($2^{108}$) 2008 ($2^{73}$) |
| MD4 (NTLMv2) | Feb 1990 | Ronald Rivest | 128 | 1991 | 1995 secs 2004µSec | 2008 ($2^{102}$) |
| MD5 (SSLcerts) | Apr 1992 | Ronald Rivest | 128 | 1996 | 2004 1 hr 2006 1 m 2013 <1 s | 2009($2^{123.4}$) |

# Hash Functions

| Name | Invented | By | Size | Attacks | Collision | Pre-Image |
|---|---|---|---|---|---|---|
| MD2 (RSA-MD2) | Jan 1988 | Ronald Rivest | 128 | 1997 | 2009 $2^{63.3}$ | 2004 ($2^{108}$) 2008 ($2^{73}$) |
| MD4 (NTLMv2) | Feb 1990 | Ronald Rivest | 128 | 1991 | 1995 secs 2004µSec | 2008 ($2^{102}$) |
| MD5 (SSLcerts) | Apr 1992 | Ronald Rivest | 128 | 1996 | 2004 1 hr 2006 1 m 2013 <1 s | 2009($2^{123.4}$) |
| RIPEMD | Nov 1992 | Dobbertin, Bosselaers and Preneel | 128 | 1995 | 2004 | - |
| SHA(-0) | May 1993 | NSA (MD4) | 160 | | 1998 ($2^{61}$) 2004 ($2^{51}$) (weeks) 2004 ($2^{40}$) 2005 ($2^{39}$) 2008 $2^{33.6}$ | |

# Hash Functions

| Name | Invented | By | Size | Attacks | Collision | Pre-Image |
|---|---|---|---|---|---|---|
| MD2 | Jan 1988 | Ronald Rivest | 128 | 1997 | 2009 $2^{63.3}$ | 2008 ($2^{73}$) |
| MD4 | Feb 1990 | Ronald Rivest | 128 | 1991 | 2004µSec | 2008 ($2^{102}$) |
| MD5 | Apr 1992 | Ronald Rivest | 128 | 1996 | 2004 1 hr | 2009($2^{123.4}$) |
| RIPEMD | Nov 1992 | Dobbertin,etal | 128 | 1995 | 2004 | - |
| SHA(-0) | May 1993 | NSA (MD4) | 160 | | 2004 ($2^{51}$) | |
| SHA-1 (SSLcerts) | May 1995 | NSA | 160 | 2005<br>2015($2^{57}$) chosenIV | 2005 ($2^{69}$)<br>2005 ($2^{63}$)<br>2017 $2^{63.1}$ Google | |
| RIPEMD-160 | 1996 | Dobbertin, Bosselaers and Preneel | 128<br>160<br>256<br>320 | Reduced rounds attacks only | - | - |

# Hash Functions

| Name | Invented | By | Size | Attacks | Collision | Pre-Image |
|---|---|---|---|---|---|---|
| MD2 | Jan 1988 | Ronald Rivest | 128 | 1997 | 2009 $2^{63.3}$ | 2008 ($2^{73}$) |
| MD4 | Feb 1990 | Ronald Rivest | 128 | 1991 | 2004μSec | 2008 ($2^{102}$) |
| MD5 | Apr 1992 | Ronald Rivest | 128 | 1996 | 2004 1 hr | 2009($2^{123.4}$) |
| RIPEMD | Nov 1992 | Dobbertin,etal | 128 | 1995 | 2004 | |
| SHA(-0) | May 1993 | NSA (MD4) | 160 | | 2004 ($2^{51}$) | |
| SHA-1 | May 1995 | NSA | 160 | 2015 (IV) | 2017 $2^{63.1}$ | |
| RIPEMD-160 | 1996 | Dobbertin,etal | 128 160 256 320 | Reduced rounds | - | - |
| SHA-2 (SSLcerts) | May 2001 | NSA | 224 256 384 512 | Numerous reduced rounds attacks | - | - |
| Untruncated family subject to length extension, use SHA-512/224, SHA-512/256 | | | | | | |

# Hash Functions

| Name | Invented | By | Size | Attacks | Collision | Pre-Image |
|---|---|---|---|---|---|---|
| MD2 | Jan 1988 | Ronald Rivest | 128 | 1997 | 2009 $2^{63.3}$ | 2008 ($2^{73}$) |
| MD4 | Feb 1990 | Ronald Rivest | 128 | 1991 | 2004µSec | 2008 ($2^{102}$) |
| MD5 | Apr 1992 | Ronald Rivest | 128 | 1996 | 2013 <1 s | 2009($2^{123.4}$) |
| RIPEMD | Nov 1992 | Dobbertin,etal | 128 | 1995 | 2004 | |
| SHA(-0) | May 1993 | NSA (MD4) | 160 | | 2004 ($2^{51}$) | |
| SHA-1 | May 1995 | NSA | 160 | 2015 (IV) | 2017 $2^{63.1}$ | |
| RIPEMD-160 | 1996 | Dobbertin,etal | 128 160 256 320 | Red.Rnds | - | - |
| SHA-2 | May 2001 | NSA | 224 256 384 512 | Red.Rnds | - | - |
| MD6 | Jun 2008 | Rivest + MIT | 0-256 | - | - | - |
| SHA-3 (Keccack) (SSLcerts) | Oct 2008 Keccack May 2014 SHA-3 | Guido Bertoni Joan Daemen Michaël Peeters and Gilles Van Assche | 224 256 384 512 d(128) d(256) | Only an 8-round (out of 24) attack | - | - |

# Some Homework

- Research and expand these tables for:

| Name | Invented | By | Size | Attacks | Collision | Pre-Image |
|---|---|---|---|---|---|---|
| BLAKE | | | | | | |
| BLAKE2 | | | | | | |
| Whirlpool | | | | | | |

# Today's Lecture

- Working in IT Security
  - International Information System Security Certification Consortium $(ISC)^2$
    - Certified Information Systems Security Professional (CISSP)
  - ISACA
    - CISA, CISM, CRISK, CGEIT
  - GIAC Certifications
  - Payment Card Industry (PCI)
    - PCI Data Security Standard (PCI DSS)
- Finish off Biometrics

# What Do IT Security Professionals Actually Do?

- GRC (Governance Risk Compliance) Team
  - Enterprise Architecture
    - SABSA, Zachmann, TOGAF, QGEA
  - Information Security Management Systems (ISMS)
    - Policies, Procedures, Consulting, Audits
  - ISO 27000 Compliance
  - PCI DSS Compliance
- Security Services
  - Firewalls/Routers, Network Security, IPS/IDS, Authentication Systems, PKI, endpoint security, DLP, SIEM, secure remote access
- VPT (Vulnerability and Penetration Testing) Team

# Guest Lecturers

- Microsoft
- CUA?
- Your Digital File
- Splunk
- Telstra?

# Certifications

- International Information System Security Certification Consortium (ISC)²
  - "(ISC)² is an international nonprofit membership association focused on inspiring a safe and secure cyber world."
- 115,000 security professionals
- Certified Information Systems Security Professional (CISSP) certification
- (ISC)² offers a portfolio of credentials

# (ISC)² security credentials

# CISSP

- Need 5 years InfoSec experience
- Experience verified by another CISSP with your employers
- Exam 6 Hours
- USD $599 (AUD $800)

# (ISC)² CBK

- The (ISC)² Common Body of Knowledge – the "(ISC)² CBK".
- The CISSP domains are drawn from various information security topics within the (ISC)² CBK.
- The CISSP candidate must have at least 5 years of paid full-time experience in 2 or more of the above domains.

# CISSP® Domains

- The CISSP CBK consists of 8 domains (used to be 10):
- **Security and Risk Management**
- **Asset Security**
- **Security Engineering**
- **Communication and Network Security**
- **Identity and Access Management**
- **Security Assessment and Testing**
- **Security Operations**
- **Software Development Security**

# CISSP® Domains

- The CISSP CBK consists of 8 domains (used to be 10):
- **Security and Risk Management**
- **Asset Security**
- **Security Engineering**
- **Communication and Network Security**
- **Identity and Access Management**
- **Security Assessment and Testing**
- **Security Operations**
- **Software Development Security**

# CISSP® Domains

- The CISSP CBK consists of 8 domains (used to be 10):
- **Security and Risk Management**
- **Asset Security**
- **Security Engineering**
- **Communication and Network Security**
- **Identity and Access Management**
- **Security Assessment and Testing**
- **Security Operations**
- **Software Development Security**

# ISACA

- Previously known as the Information Systems Audit and Control Association
- Now just ISACA
  - … a nonprofit, independent association that advocates for professionals involved in information security, assurance, risk management and governance
- www.isaca.org/chapters1/brisbane/Pages/default.aspx

# ISACA Credentials

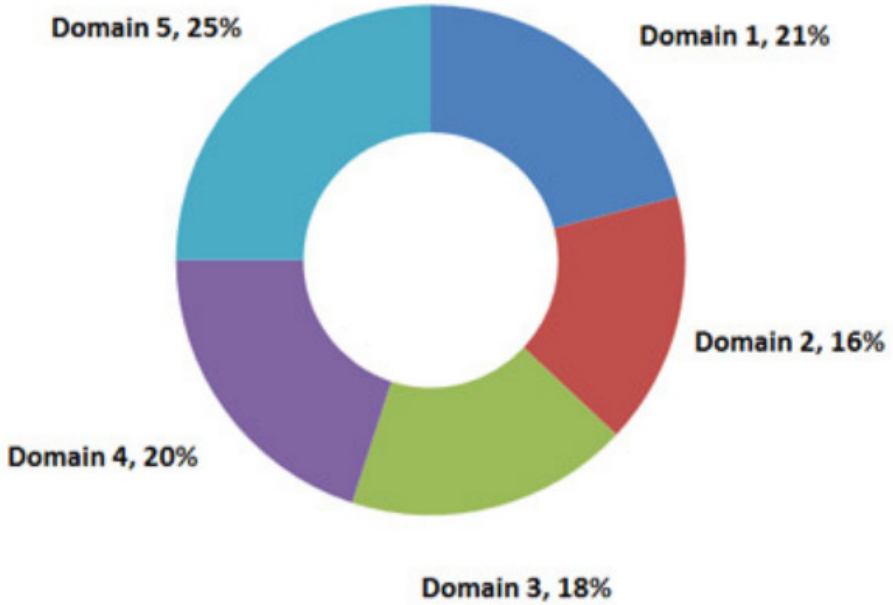
ISACA®

*Trust in, and value from, information systems*

# COBIT®

# ISACA

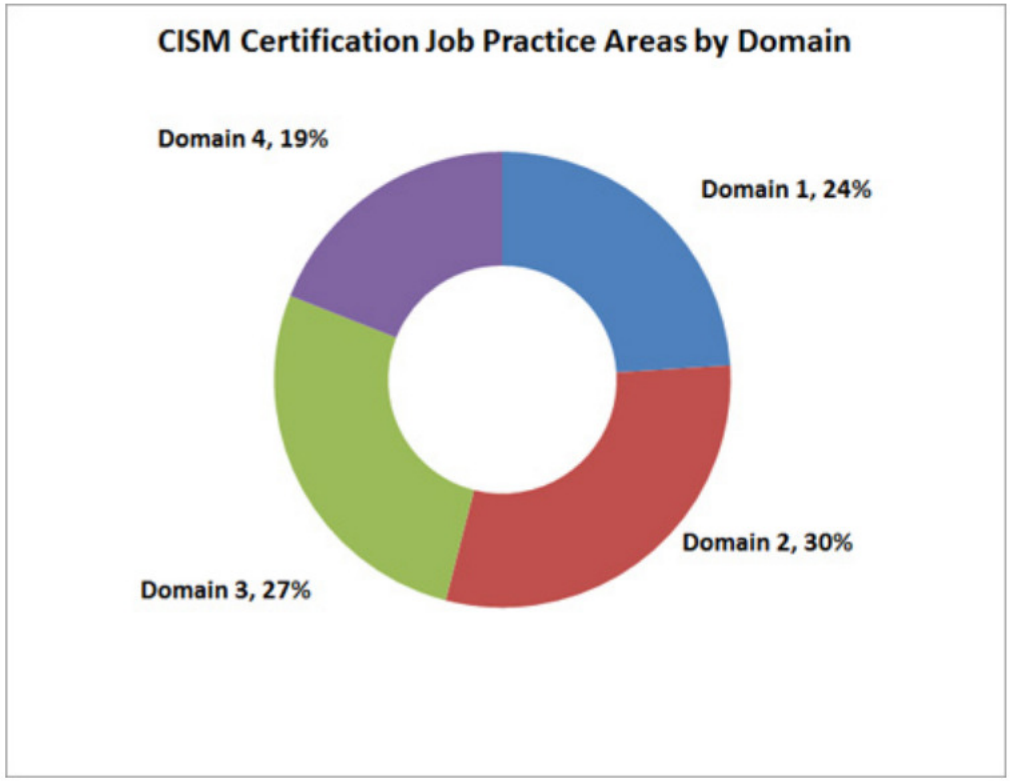

## CISA Certification Job Practice Areas by Domain




The job practice domains and task and knowledge statements are as follows:

Domain 1—The Process of Auditing Information Systems (21%)
Domain 2—Governance and Management of IT (16%)
Domain 3—Information Systems Acquisition, Development and Implementation (18%)
Domain 4—Information Systems Operations, Maintenance and Service Management (20%)
Domain 5—Protection of Information Assets (25%)

# ISACA

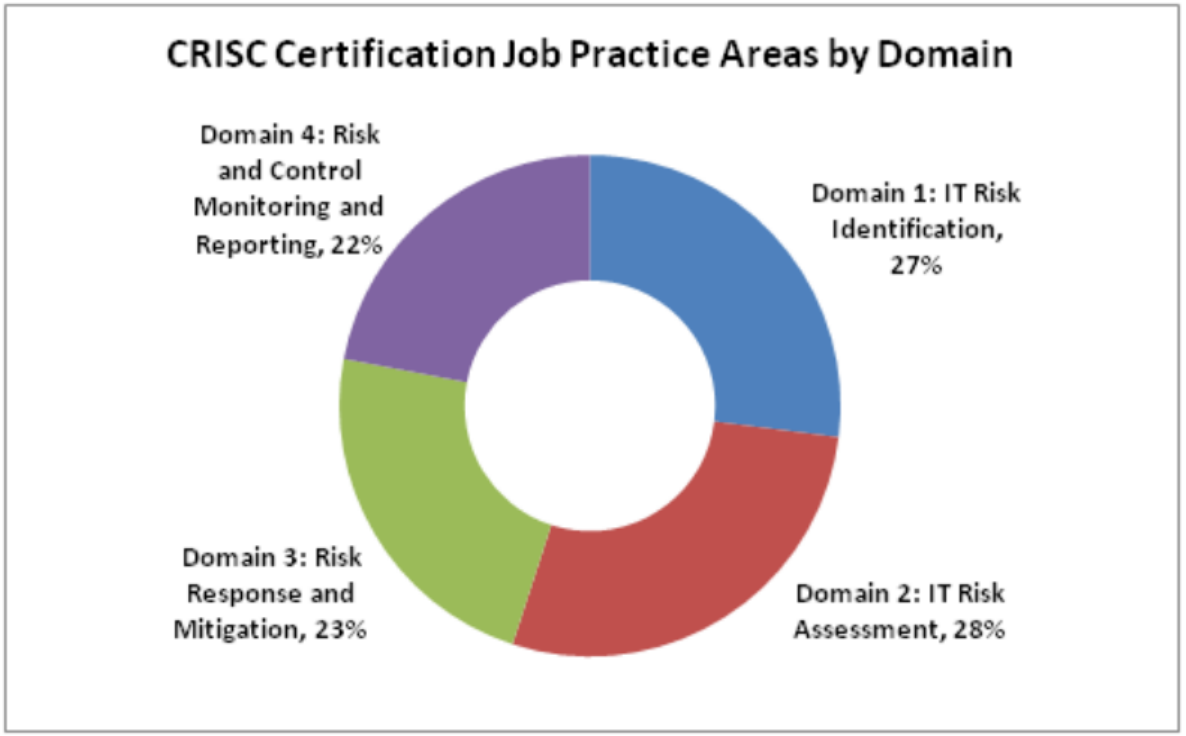



The job practice domains and task and knowledge statements are as follows:

Domain 1—Information Security Governance (24%)
Domain 2—Information Risk Management (30%)
Domain 3—Information Security Program Development and Management (27%)
Domain 4—Information Security Incident Management (19%)

# ISACA

Certified in Risk and Information Systems Control
An ISACA® Certification




The job practice domains and task and knowledge statements are as follows:

Domain 1—IT Risk Identification (27%)
Domain 2—IT Risk Assessment (28%)
Domain 3—Risk Response and Mitigation (23%)
Domain 4—Risk and Control Monitoring and Reporting (22%)

# ISACA


These statements and domains were the result of extensive research and feedback from IT governance subject matter experts from around the world. Numerous reference sources were also utilized including COBIT 5.

These statements are intended to depict the tasks performed by individuals who have a significant management, advisory, or assurance role relating to the governance of IT and the knowledge required to perform these tasks. They are also intended to serve as a definition of the roles and responsibilities of the professionals performing IT governance work.

For purposes of these statements, the terms "enterprise" and "organization" or "organizational" are considered synonymous.

The job practice domains and task and knowledge statements are as follows:

Domain 1: Framework for the Governance of Enterprise IT (25%)
Domain 2: Strategic Management (20%)
Domain 3: Benefits Realization (16%)
Domain 4: Risk Optimization (24%)
Domain 5: Resource Optimization (15%)

# GIAC

GIAC Certifications: The Highest Standard in Cyber Security Certifications

# A Multitude of GIAC certs…


# Payment Cards

# Payment Card Industry (PCI)

- PCI DSS (Data Security Standard)
- Report On Compliance
- Gap Analysis
- PCI Consulting
- Virtualisation
- Cloud
- Architecture
- Security Policy
- VPT (Vulnerability and Penetration Testing)

# Payment Card Data Is a Target

- Major payment card processor (2005) – 40 million cards lost
  - Accessed a database with direct connectivity to the Internet.
  - Company no longer in business.
- Payment processor (2009) – 160 million cards lost
  - Malware was used to capture cardholder data as it was processed.
  - Reports suggest direct costs for the breach cost 171 million USD.
- US food based retailer (2013) – 1.8 million cards lost
  - Malware installed at the POS was skimming account data at read.
  - Estimated costs exceed 80 million USD.
- Major retailer (2013) – over 100 million cards lost
  - Malware installed on POS systems to capture CHD in memory.
  - Senior staff members resigned following breach.
- Major retailer (2014) – over 50 million cards lost
  - Malware installed on POS systems to capture CHD in memory.

# Things You Need To Know

- PAN – Primary Account Number = Card number
- SAD – Sensitive Authentication Data
- CHD – Cardholder Data (next slide)
- CDE – Cardholder Data Environment
- PED – PIN Entry Device
- CVV – CVV2, CVC2,etc – Card Verification Value
- QSA – Qualified Security Assessor
- ASV – Approved Scanning Vendor

# Straight from the DSS:

***Cardholder Data includes:***

- Primary Account Number (PAN)
- Cardholder Name
- Expiration Date
- Service Code

# Straight from the DSS:

***Sensitive Authentication Data includes:***

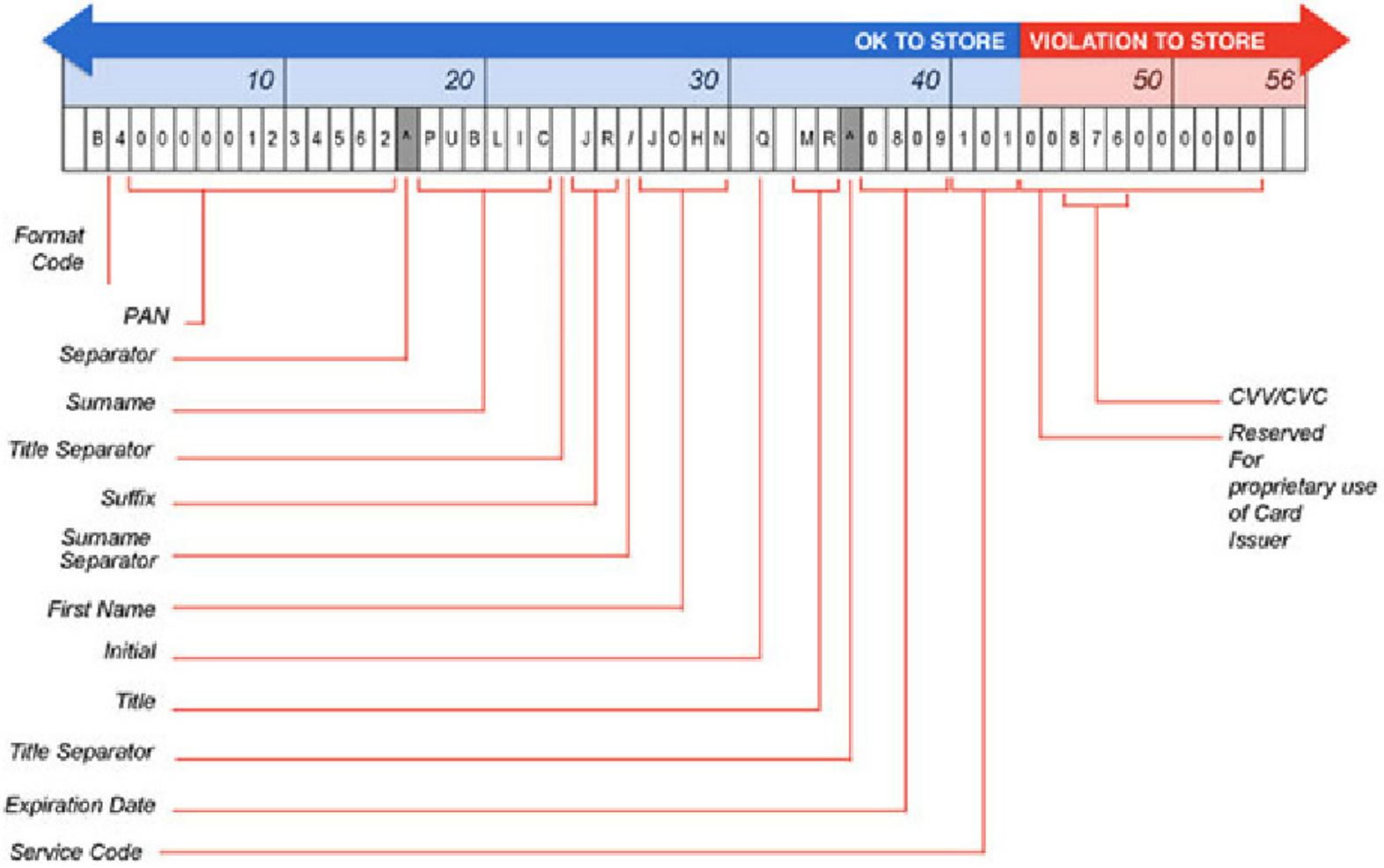
- Full magnetic stripe data or equivalent on a chip
- CAV2/CVC2/CVV2/CID
- PINs/PIN blocks

# Track Data

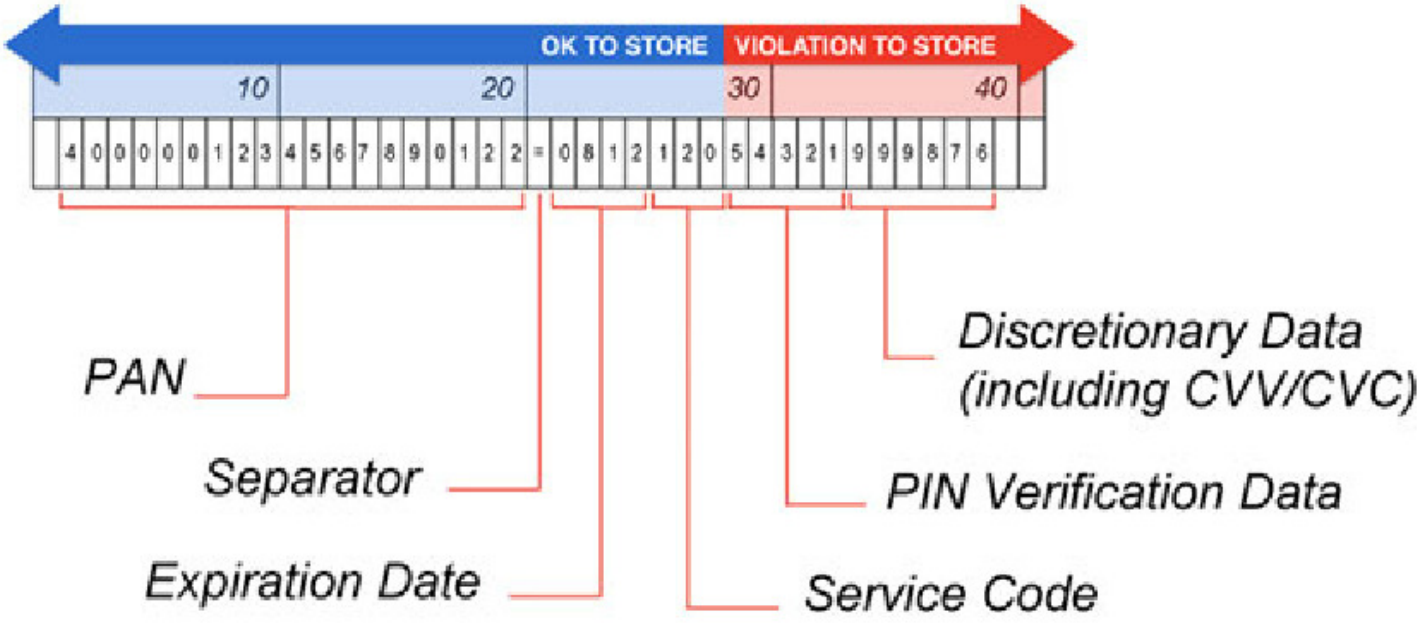
(data tracks on the magnetic stripe or in an EMV chip)

- Payment Cards typically use two tracks of data on the magnetic stripe:
  - Track 1
    - Contains all fields of both track 1 and track 2
    - Length up to 79 characters
  - Track 2
    - Provides shorter processing time for older dial-up transmissions
    - Length up to 40 characters

## Track 1 Data



## Track 2 Data



# EMV Chip Cards

- Track equivalent data found on the chip differs from the track data found on the magnetic stripe as the chip track data contains a unique Chip CVV/CVC code.
- This prevents criminals producing cloned magnetic stripe cards from a chip's track data.
- However, there is still sufficient information to allow criminals to use this data in a card-not-present fraud (such as e-commerce or mail order/telephone order).

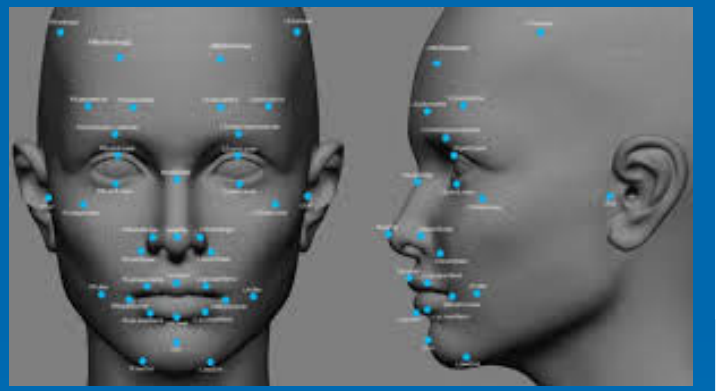
# Any questions so far?

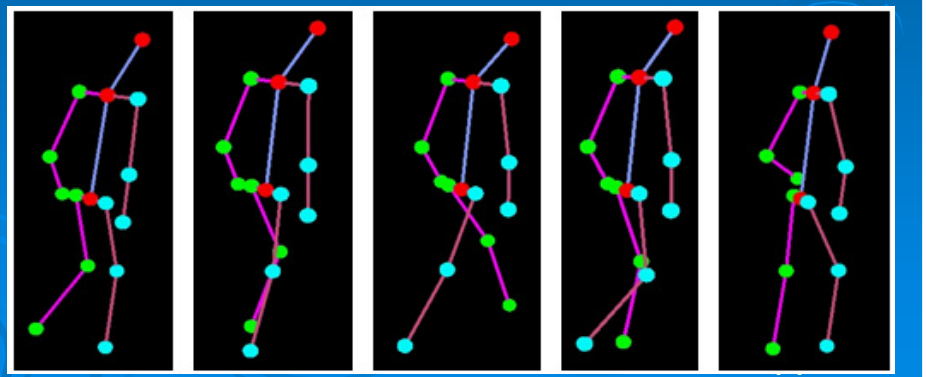
# Back to Biometrics

# Biometrics

- Authentication based on something you are
  - Characteristics of the human body, behaviour
- "Biometrics is the set of automated methods to recognize a person based on physiological or behavioural characteristics"

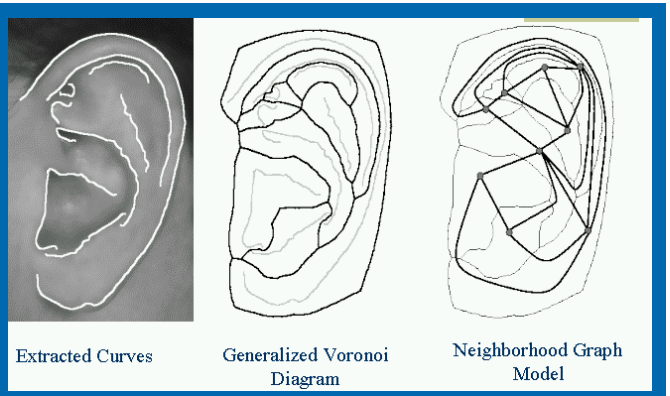
Biometric Consortium

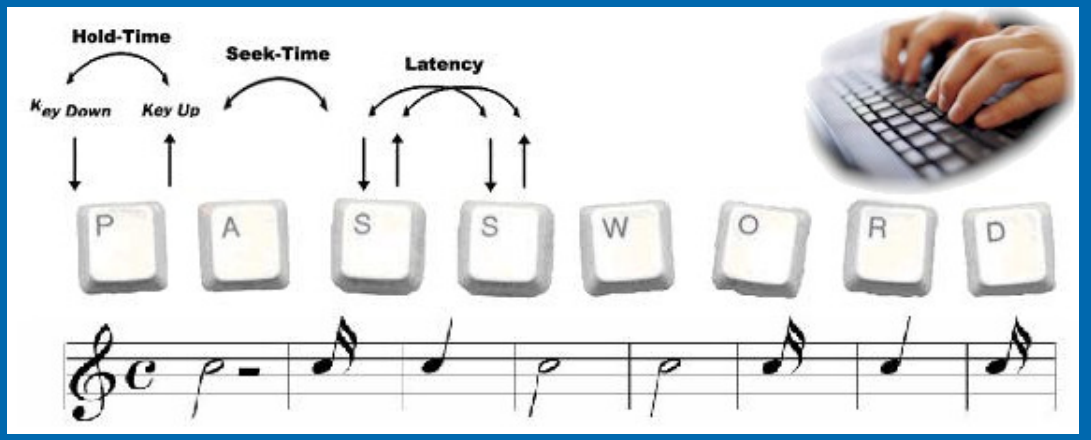




# Biometrics

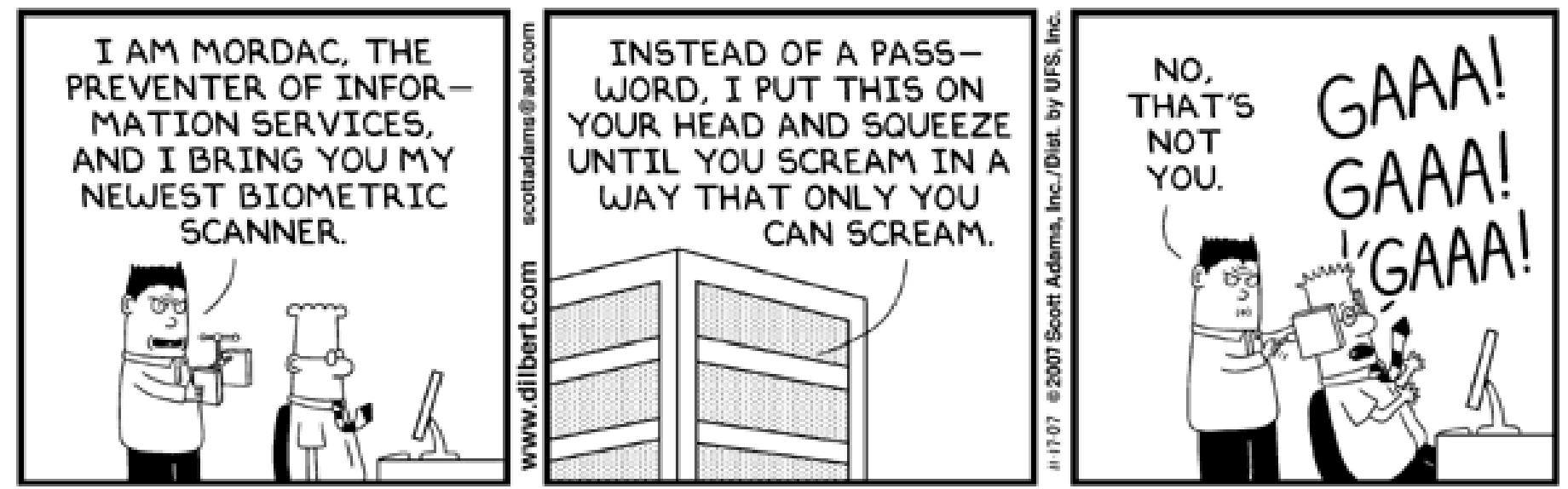
- Fingerprints
- Voice
- Iris
- Retina
- Hand-geometry
- Gait
- Signature
- Face
- DNA
- Odor
- Ear
- Hand Vein
- Keystroke dynamics
- …




# Types of Biometrics

- Examples for physiological biometrics (something you are)
  - Fingerprint
  - Retina
  - Iris
  - Face
  - …
- Examples for behavioural biometrics (something you do)
  - Signature
  - Voice
  - Gait
  - Keystroke dynamics
    - Good for ***continuous authentication***
  - And another one:



# Olfactory Biometrics

- Biometrics based on odour
- *"It turns out there are recognizable patterns of each person's body odor that remain steady, the researchers found. In addition, the accuracy rate of identifying a person by their unique odor turned out to be higher than 85%. Those numbers remain constant, the researchers say, even as body odor varies due to disease, diet change or even mood swings."*
  - http://www.zdnet.com/body-odor-passes-smell-test-as-biometric-7000026023/

http://www.seeker.com/body-odor-id-your-new-smelly-password-1768281006.html#news.discovery.com

# Criteria for a good Biometric

- Universality
  - Each person should have the characteristic
    - e.g. bald people don't have hair colour
- Distinctiveness
  - Any two persons should be sufficiently different in terms of this characteristic
    - e.g. shoe size is not very distinctive
- Permanence
  - The characteristic should be sufficiently invariant over a period of time
    - e.g. Hair colour might change frequently
- Performance
  - Recognition accuracy (and speed)
- Acceptability
  - Extent to which people are willing to accept Biometric in their daily live
    - e.g. Retinal scan might be considered intrusive (can reveal information about health)
    - e.g. hand geometry reader might be considered unhygienic
- Circumvention
  - How easily the system can be tricked

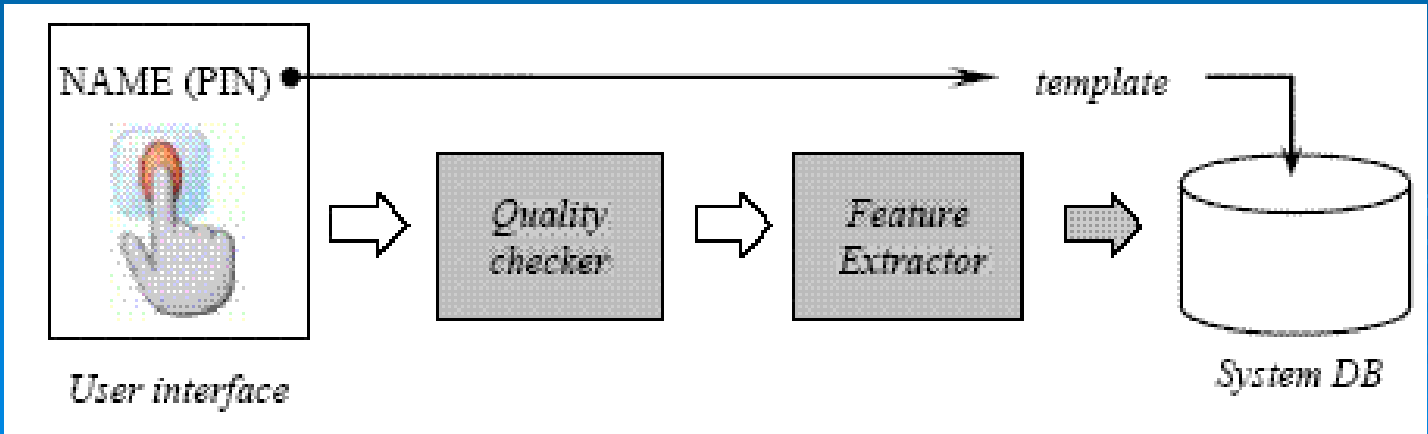
# Comparison of Biometric Systems

| Biometric identifier | Universality | Distinctiveness | Permanence | Collectability | Performance | Acceptability | Circumvention |
|---|---|---|---|---|---|---|---|
| DNA | H | H | H | L | H | L | L |
| Ear | M | M | H | M | M | H | M |
| Face | H | L | M | H | L | H | H |
| Facial thermogram | H | H | L | H | M | H | L |
| Fingerprint | M | H | H | M | H | M | M |
| Gait | M | L | L | H | L | H | M |
| Hand geometry | M | M | M | H | M | M | M |
| Hand vein | M | M | M | M | M | M | L |
| Iris | H | H | H | M | H | L | L |
| Keystroke | L | L | L | M | L | M | M |
| Odor | H | H | H | L | L | M | L |
| Palmprint | M | H | H | M | H | M | M |
| Retina | H | H | M | L | H | L | L |
| Signature | L | L | L | H | L | H | H |
| Voice | M | L | L | M | L | H | H |

Anil K. Jain et al., "An Introduction to Biometric Recognition", IEEE Transactions on Circuits and Systems for Video Technology, Special Issue on Image- and Video-Based Biometrics, Vol. 14, No. 1, January 2004.

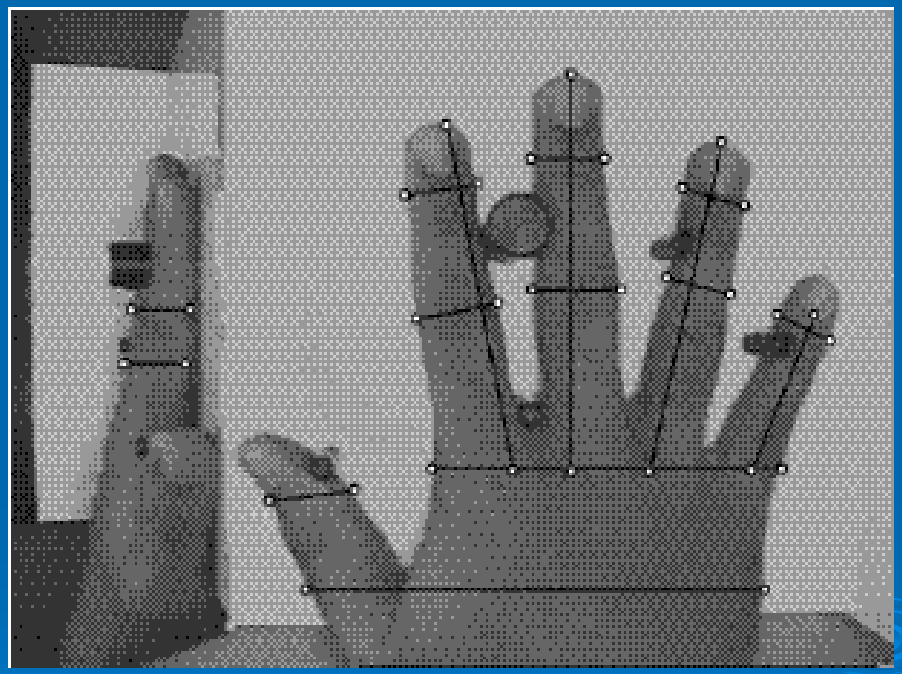
# Enrolment

- A biometric system is a pattern recognition system
- Users need to ‘enrol’
  - Biometric data is ‘scanned’
  - Features are extracted
    - Instead of storing the image of a fingerprint, only a “feature vector” describing the key characteristics is stored (highly compressed)
  - Feature Vector (‘template’) is stored in database, together with Identity of user



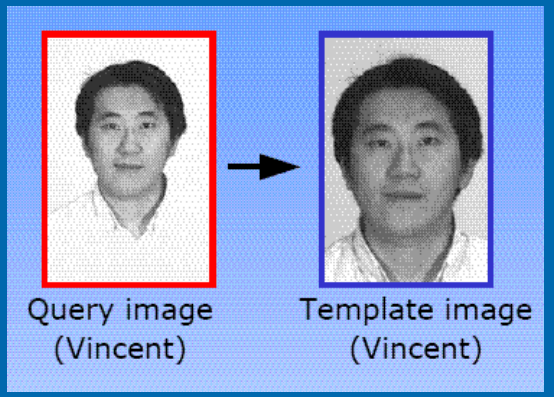
# Feature Vector - Example

- Feature Vector of hand geometry
  - Stores a few key geometrical dimensions
  - Can be compressed to as little as a few tens of bytes



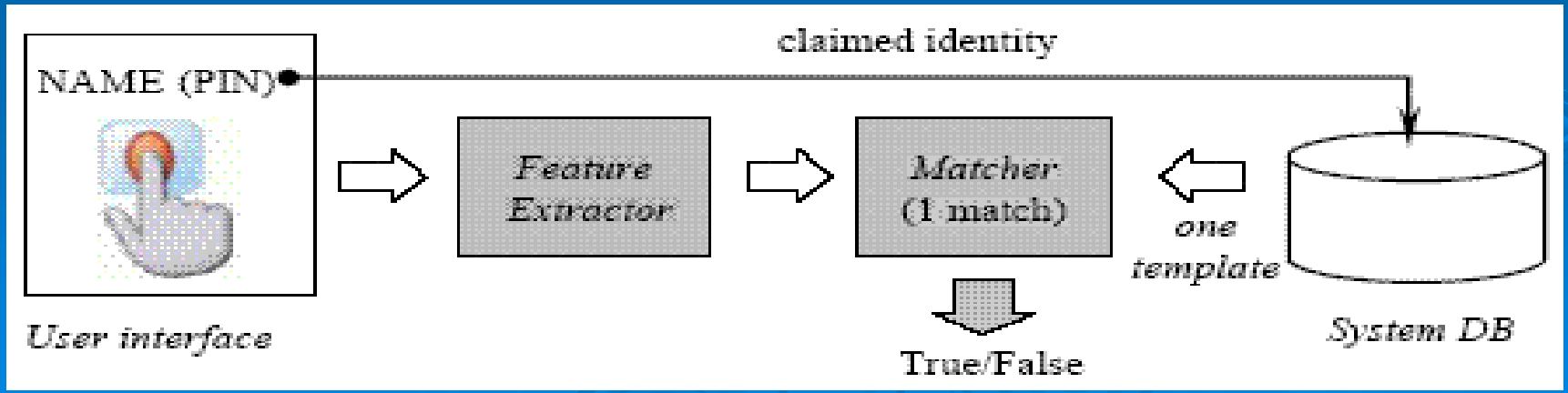
# Verification Mode

- A biometric system can operate in 2 modes
  - **Verification Mode**
    - User Bob identifies himself, e.g. via a PIN
    - Biometric is scanned and compared with Bob's template in data base
    - System answers the question: **"Does this Biometric belong to Bob?"**
    - One-to-one match




Images from "Biometrics a grand challenge", A. K. Jain et al., biometrics.cse.msu.edu

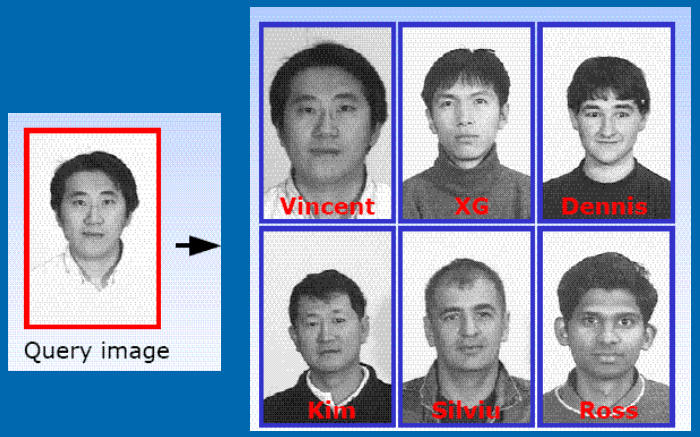
Verification

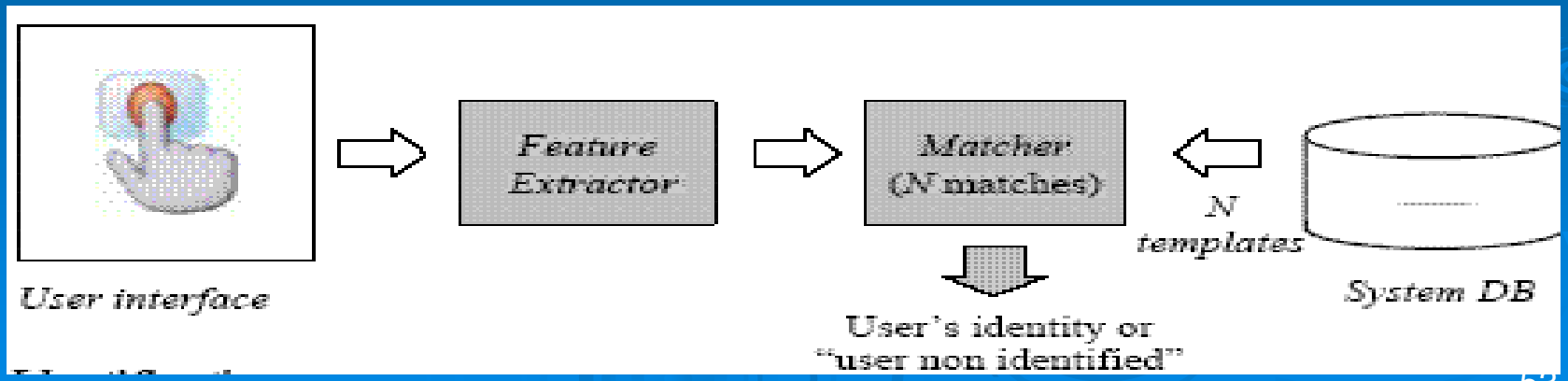



Images from: Anil K. Jain et al., "An Introduction to Biometric Recognition", IEEE Transactions on Circuits and Systems for Video Technology, Special Issue on Image- and Video-Based Biometrics, Vol. 14, No. 1, January 2004.

# Identification Mode

- User is not required to claim identity
- System tries to answer the following question: **"Whose biometric is this?"**
- One-to-N match
- Identification is harder, more error prone.
  - The larger N, the higher the probability of an error




Identification

# Formal Description of the Verification Problem

- $\mathbf{X_Q}$: Input feature vector (extracted from scanned data)
- **I**: Claimed identity
- Problem: determine if ($X_Q$,I) belongs to class w1 or w2
  - w1: genuine user
  - w2: imposter
- $\mathbf{X_Q}$ is matched against $\mathbf{X_I}$, the biometric template of user **I**.
- $S(X_Q,X_I)$ is the function that measures the similarity between feature vectors $\mathbf{X_Q}$ and $\mathbf{X_I}$
- S() is called the **matching score**, typically a single value that indicates the level of match. Larger *S()* indicates better match.
- How can we make an accept/reject decision?
  - Use simple threshold ***t***

$$(I, X_Q) \in \begin{cases} w1 & \text{if } S(X_Q, X_I) \geq t \\ w2 & \text{otherwise} \end{cases}$$

# Formal Description of Identification Problem

- Given an input feature vector $X_Q$, determine the corresponding identity $I_k$ in the template database
  - k ϵ {1,2,3…N, N+1}.
- $I_1$, $I_2$, … $I_N$: enroled users
- $I_{N+1}$: indicates no match → reject

$$X_Q \in \begin{cases} I_k & \text{if } \max_k \left( \{ S(X_Q, X_{I_k}) \} \right) \geq t, k = 1,2,...N \\ I_{N+1} & otherwise \end{cases}$$

$X_{Ik}$ is the biometric template corresponding to identity $I_k$, and *t* is a predefined threshold.

# Biometrics – What can go wrong?

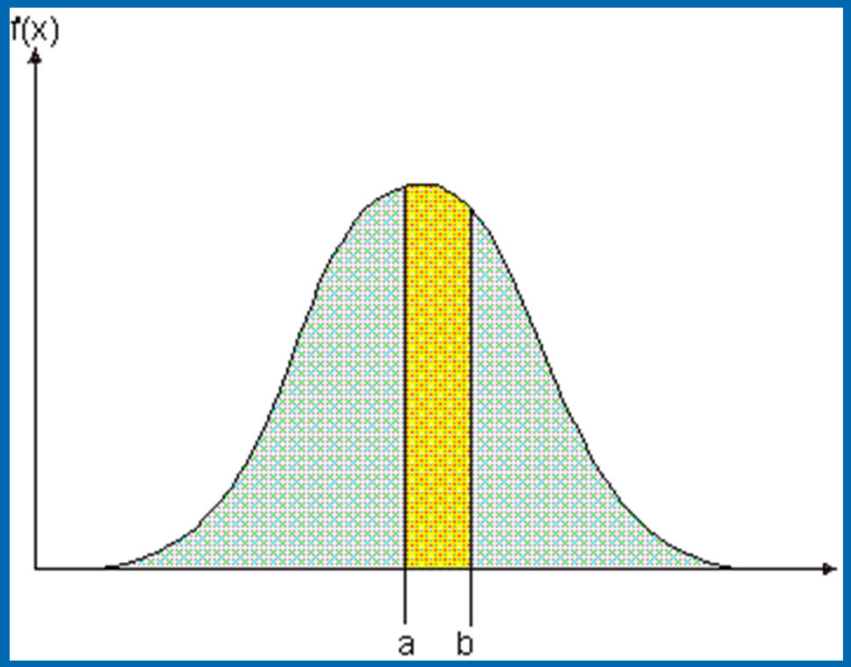
- Two Main Types of Errors:
  - False Accept (False Match)
    - e.g. Alice's biometric is wrongly matched to Bob's template and she gets access to the bank vault.
    - FAR: False Acceptance Rate, (or probability)
    - or FMR: False Match Rate (or probability)
      - Proportion of Imposters accepted
  - False Reject (False Non-Match)
    - e.g. Bob's biometric is not matched to his template in the database and he is wrongly denied access.
    - FRR: False Rejection Rate (or probability)
    - or False Non-Match Rate (FNMR)
      - Proportion of genuine users rejected
- In addition: Failure to Enrol (FTE)
  - Low quality input, which does not allow the creation of a valid template.

# Errors in Biometric Systems

- Why can errors happen (e.g. fingerprints)?
  - Sensor noise
  - Different characteristics of sensors
    - e.g. enrolment vs. verification/identification
  - Dry fingers
  - Changes in user's physiology, bruises, cuts…
  - Ambient conditions, temperature, humidity
  - User interaction, finger placement..

# Matching Score

- Scanned data and feature vector for the same person vary due to
  - Sensor noise, ambient conditions, user interaction …
  - These factors are to a large degree random
- → The matching score S() for a particular measured feature vector and a given template can be modeled as a **random variable**
- (Continuous) Random variables are defined through?
  - their probability density function (pdf)
  - Can be determined through measurements

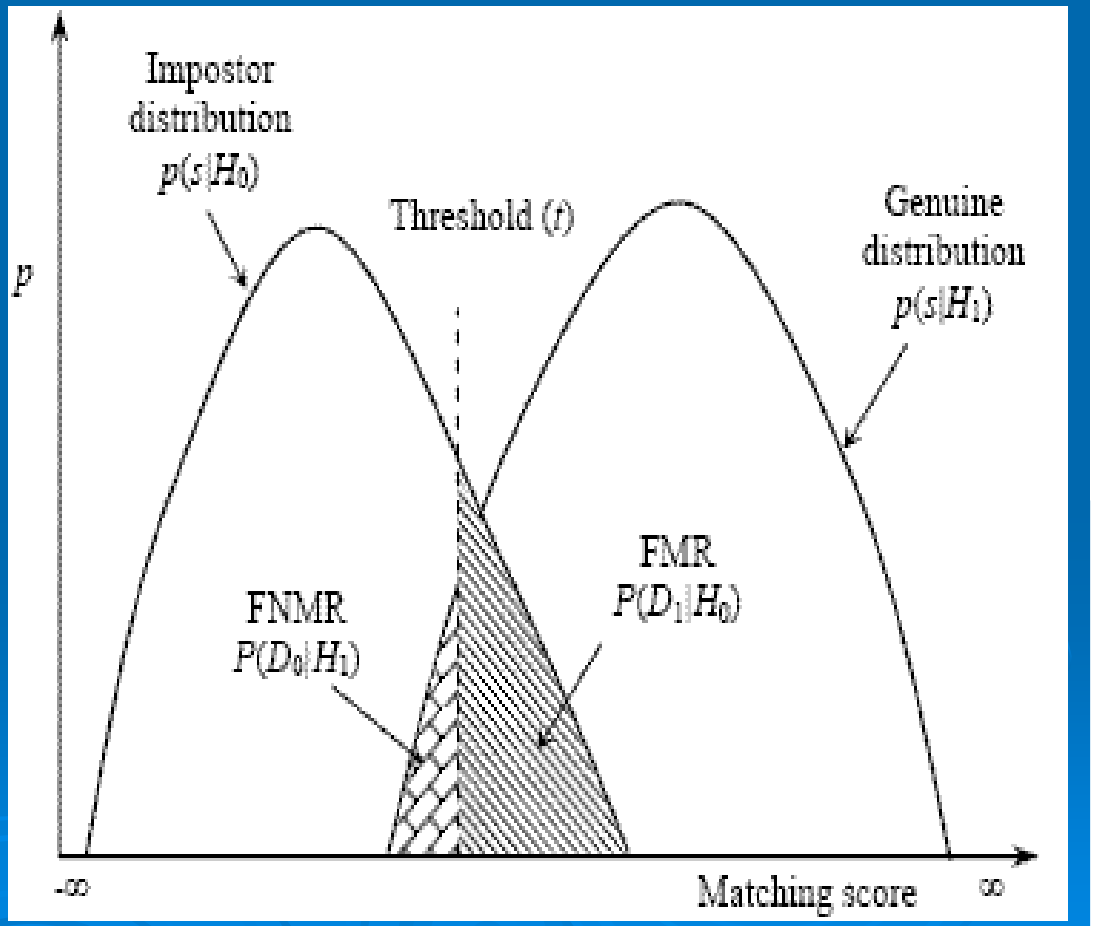



$$P(a \leq X \leq b) = \int_a^b f(x)dx$$

# Whiteboard

# Matching Score pdf

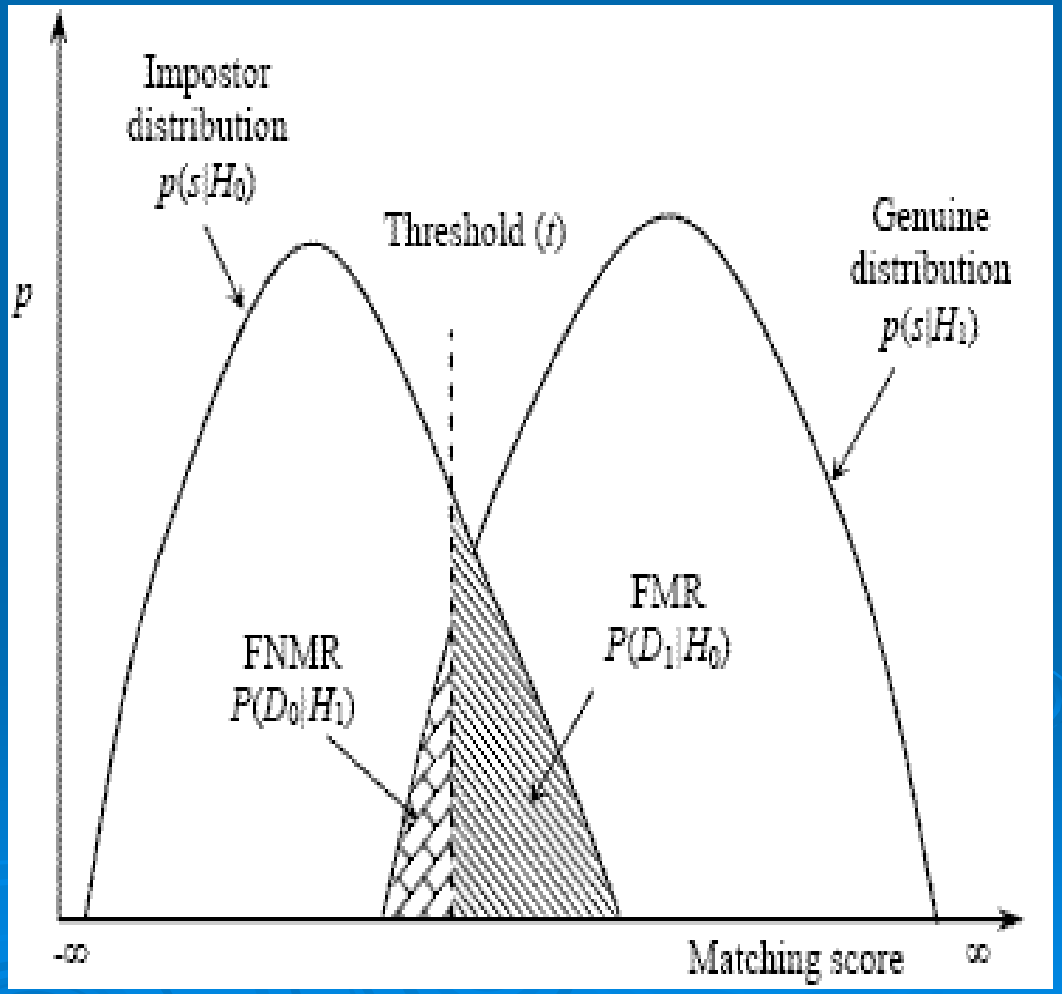
- In Biometrics, random effects such as sensor noise, ambient conditions, user interaction etc. influence scanned feature vector
- → The matching score S() can be modeled as a **random variable X** and a corresponding *pdf*
- The pdf can be determined through measurements
- The pdf of the matching score differs for genuine users and imposters
- Conditional pdf
  - p(s| genuine user)
  - p(s| imposter)



# Performance of Biometric Systems

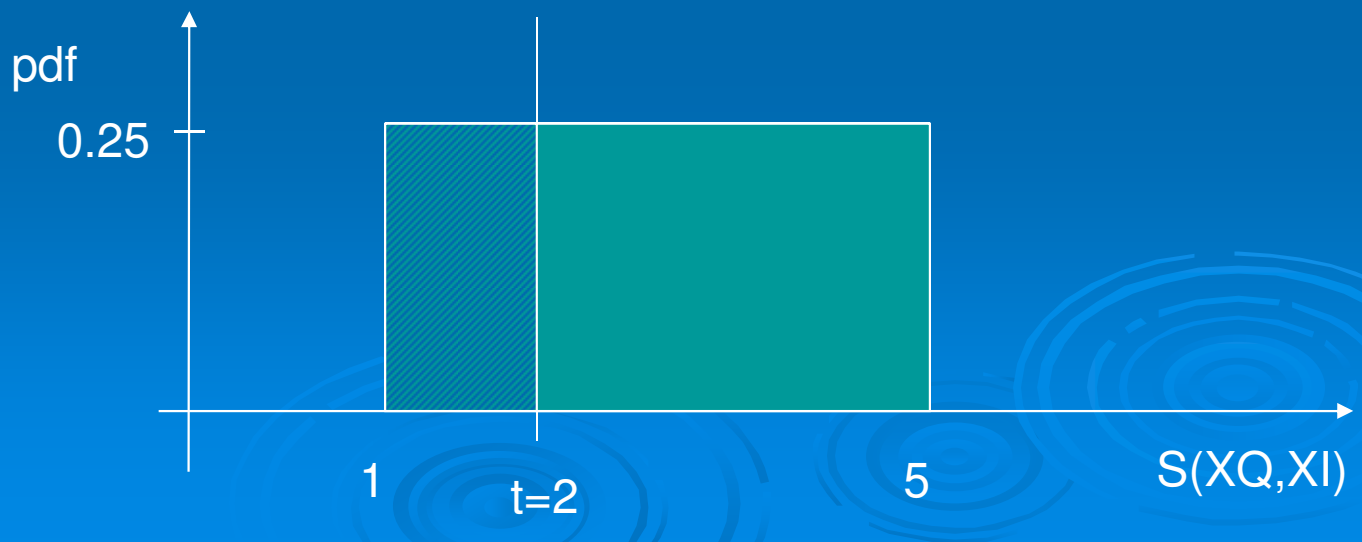
- **False Match:**
  - S() of imposter can get over threshold
- **False Non Match:**
  - S() of genuine user can drop below threshold

- We can tune the system by adjusting the threshold *t*
  - What's the effect of lowering t?
    - FMR increases
    - FNMR decreases
  - What's the effect of increasing t?
    - FMR decreases
    - FNMR increases



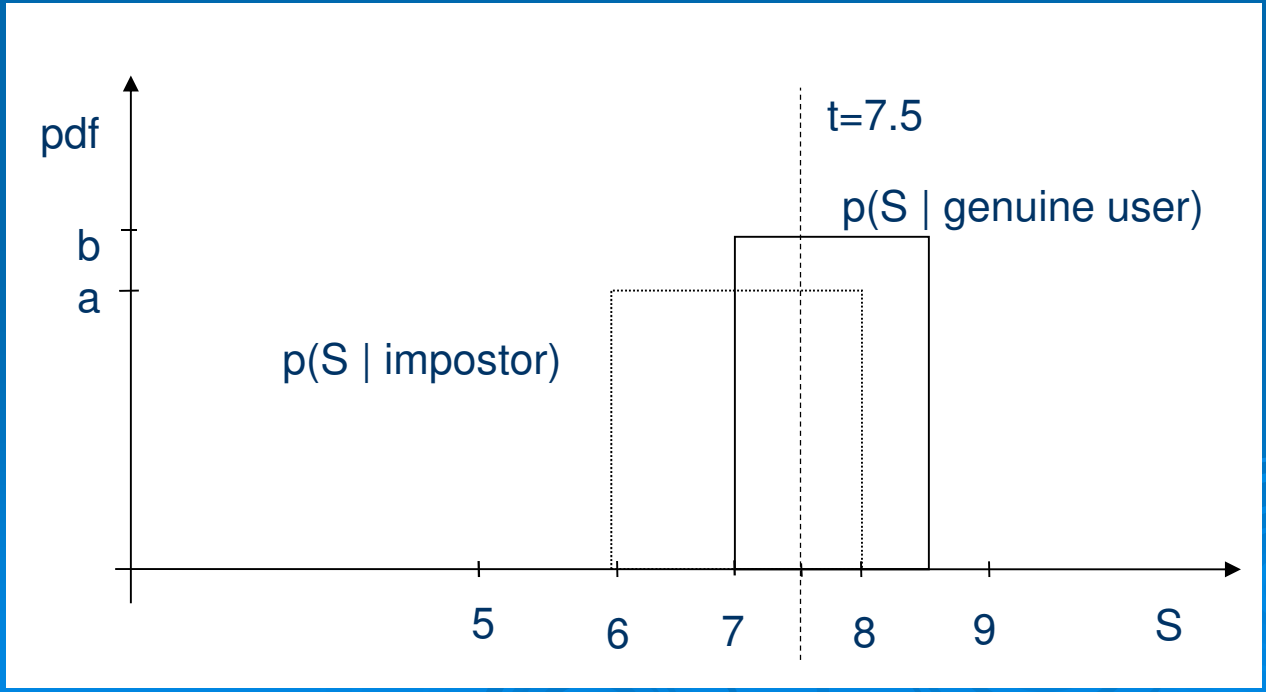
# Example

- Assume the matching score $S(X_Q, X_I)$ of a biometric system in verification mode for a genuine user has the (somewhat unrealistic) conditional pdf shown below.
  - $t = 2$ is the chosen threshold
- What is the probability that the user gets rejected?
  - Area under the curve for $S(X_Q, X_I) < t \quad = ?$
  - $= 0.25 * 1 = 0.25$
  - What is this parameter?
    - → FRR (FNMR)
- What is the probability that the user gets accepted?
  - Area under the curve for $S(X_Q, X_I) \geq t$
  - $= 0.25 * 3 = 1 - 0.25 = 0.75$



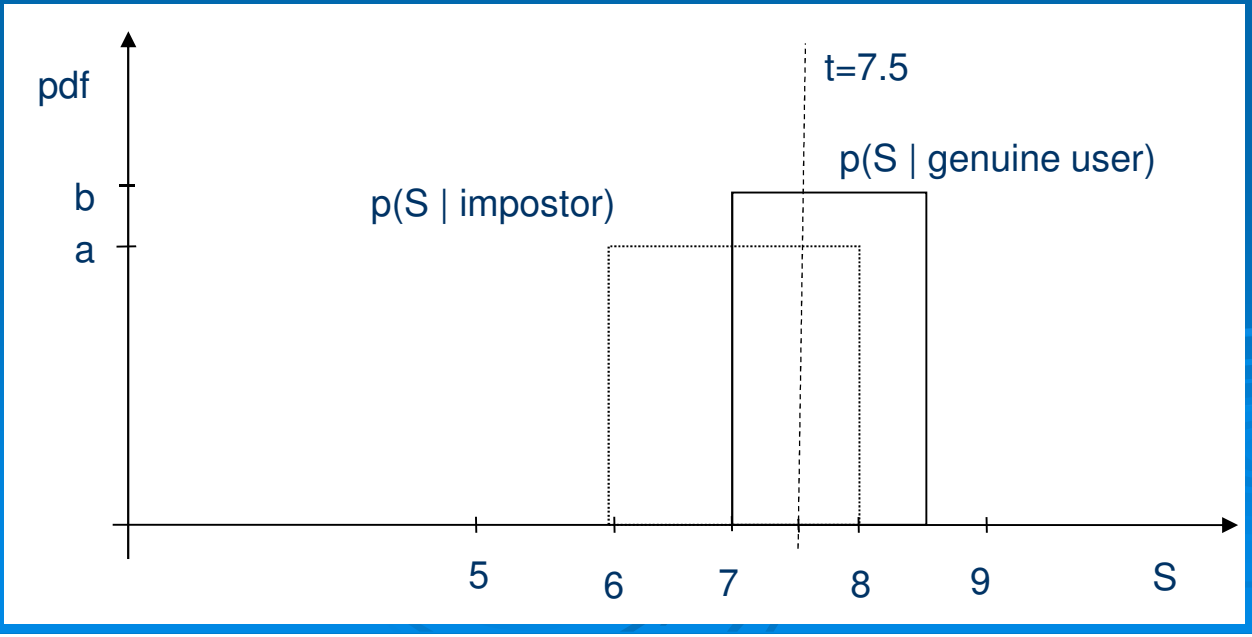
# Class Exercise

- Consider a biometric system with the following conditional probability density functions for the matching score *S* for an impostor and a genuine user.
  - Threshold t = 7.5
- What are the values of the parameters FAR (FMR) and FRR (FNMR)?



# Class Exercise - Solution

- FAR (FMR):
  - Probability of an impostor being accepted
  - Area under the curve p(S|impostor) for S ≥ t
  - FMR = 0.5 * a
  - a=?
  - We know that all probabilities must add up to 1
    - 2*a = 1 → a = 0.5
  - FMR = 0.5 * 0.5 = 0.25
- FRR (FNMR):
  - Probability of a genuine user being rejected
  - Area under the curve p(S | genuine user) for S< t
  - FNMR = 0.5 * b
    - b * 1.5 = 1 → b =2/3
  - FNMR = 0.5 * 2/3 = 1/3

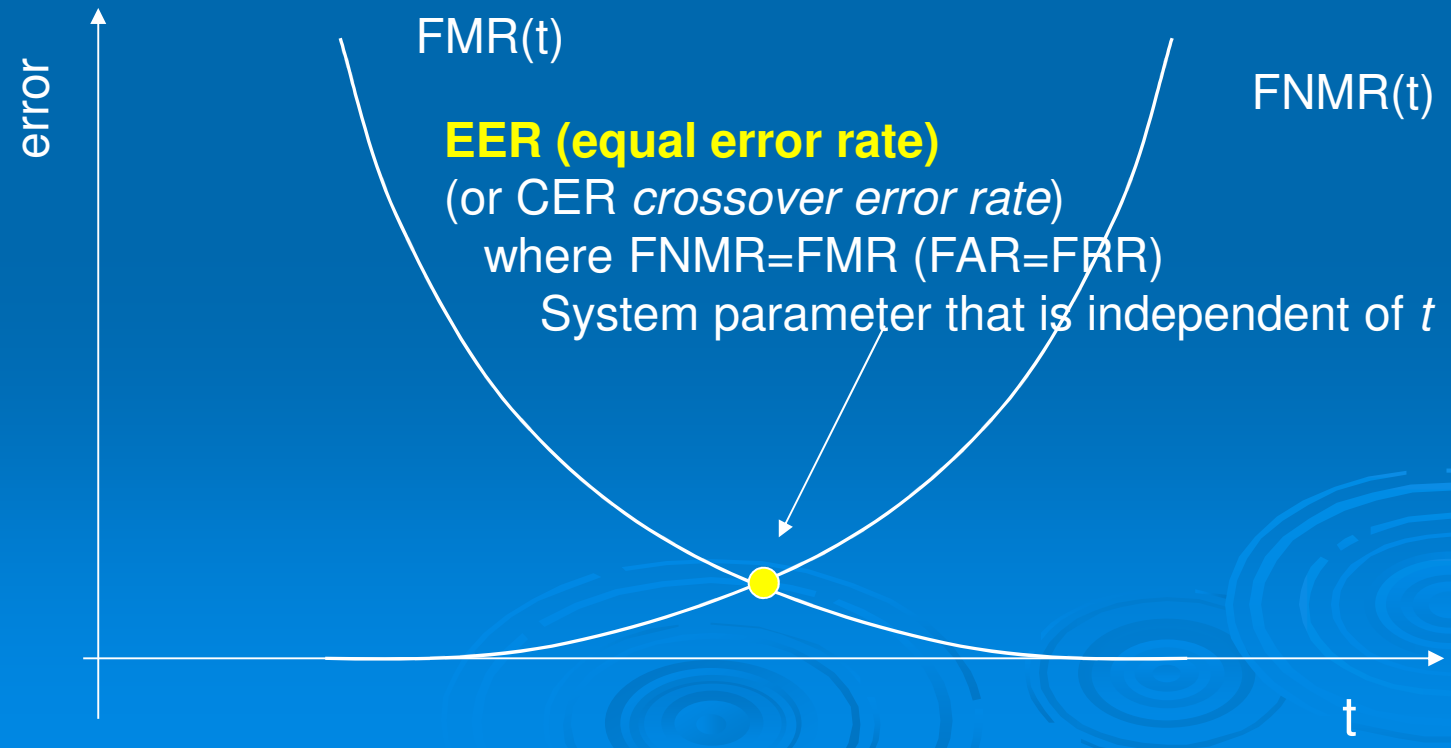


# FMR-FNMR Trade-off

- Different Applications choose different operating points *t*, i.e. different FMR-FNMR trade-off levels
- How would you choose threshold *t* for the following applications?
- High security applications, e.g. access control for highly sensitive information?
  - False Match would be a disaster
  - We can accept a few False Non Matches
  - → high threshold *t*
- Forensic Applications, e.g. matching fingerprints from crime scene with fingerprint database
  - Low FNMR is important.
  - Here, it is important to 'cast the net wide', and not let a potential criminal go undetected.
  - A relatively high FMR can be dealt with by considering other evidence
  - → low threshold *t*

# FMR vs. FNMR Trade-off

- By adjusting *t* we can trade off FMR for FNMR
  - Low *t* means high FMR and low FNMR
    - Easier for imposters to gain access, fewer genuine users rejected
  - High *t* means low FMR and high FNMR
    - Fewer imposters accepted, more genuine users rejected



# Example

- A manufacturer of a Face Recognition system claims that their product has a FMR of < 1%
- How good is the system?
  - We don't know
  - FMR or FNMR alone do not give any information about the performance of the system. You need both values, or the crossover accuracy.

# Performance Progress
# Example of Face Recognition

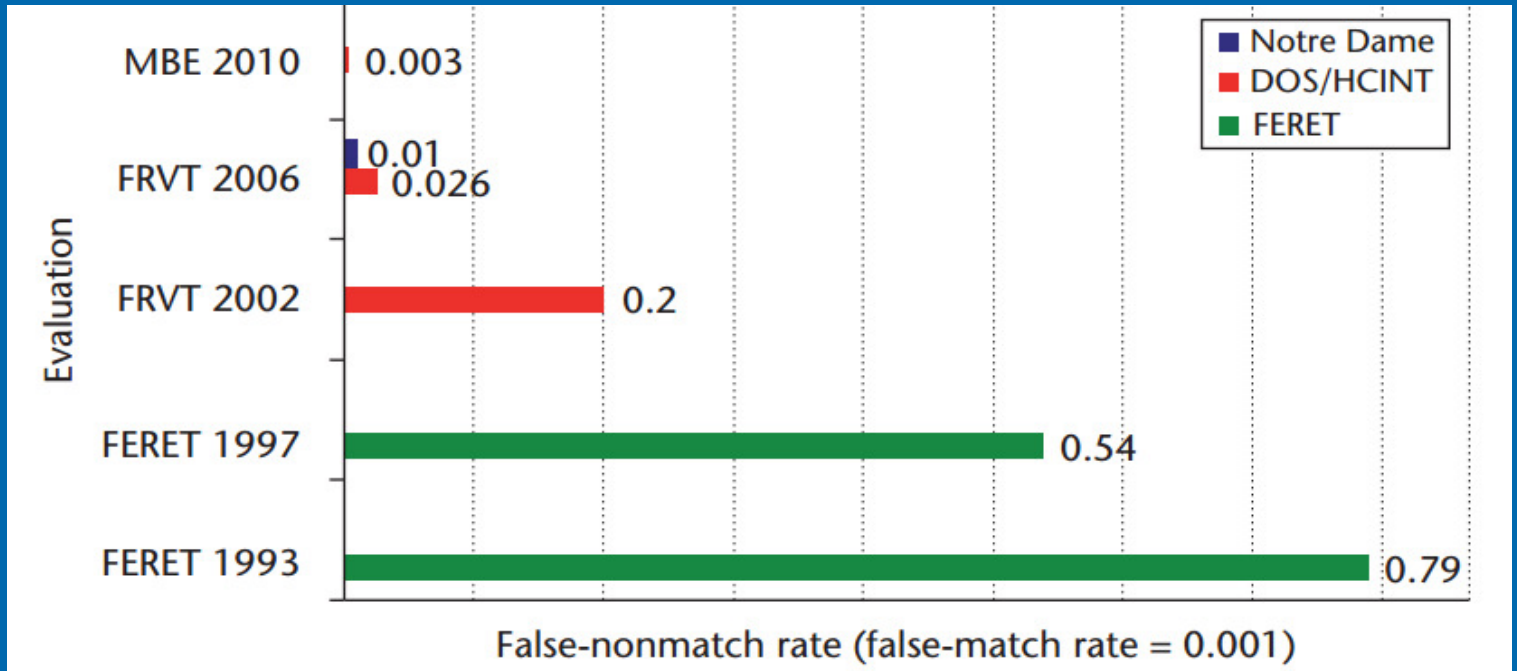



***Figure 2. The reduction in error rate for state-of-the-art face-recognition algorithms as documented through the FERET, FRVT 2002, FRVT 2006, and MBE 2010 face evaluations conducted by NIST. Performance is shown separately for the FERET, DOS/HCINT, and the Notre Dame FRVT 2006 datasets.[3]***

Jain, Anil K., Brendan Klare, and Unsang Park. "Face matching and retrieval in forensics applications." *iEEE MultiMedia* 1 (2012): 20-28.

http://www.cse.msu.edu/rgroups/biometrics/Publications/Face/JainKlarePark_FaceMatchingRetrieval_ApplicationsForensics_IEEEMultimedia11.pdf

# Commercial Biometric Systems

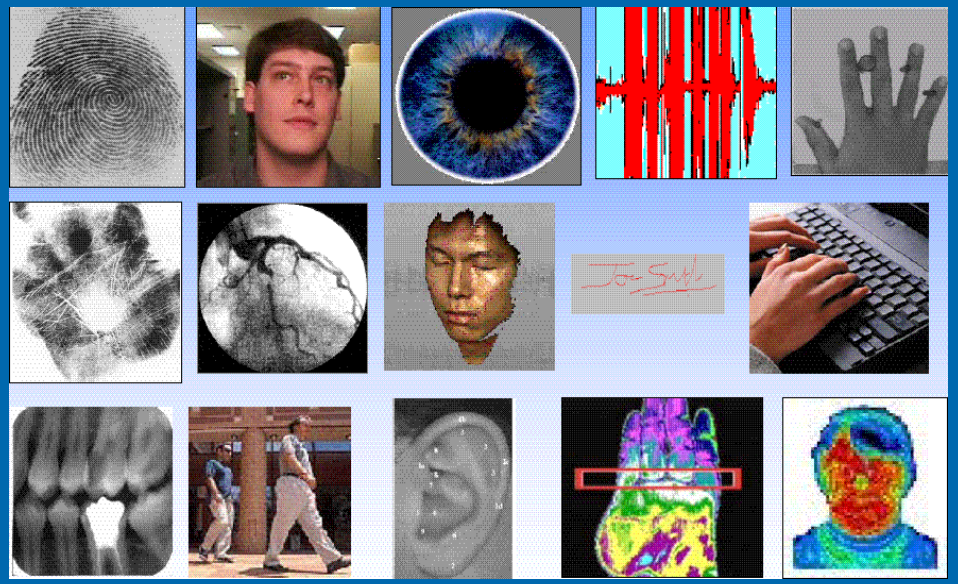
- There are a lot, in particular for fingerprints
- A randomly chosen example: Door Lock
  - Good example in terms of providing key performance figures
  - http://www.kaba.com.au/Products-Solutions/Access-Control/E-Flash/32380/digital-door-locks-e-flash-ef220-biometric-fingerprint-rim-lock.html
- Other important security criterion that is not quantified
  - circumvention

## Fingerprint Access Control

- Up to 40 fingerprints per lock
- Award winning accurate Thermal Sweep scanner (EER:0.38% FAR:0.0001% FRR:2.53%)
- Fastest fingerprint reader in the market (< ½ second)
- Individual registration and deletion with Standard or Security modes

# Choice of Systems

- No Biometric System is perfect
- Trade off between characteristics:
  - Universality, Distinctiveness, Performance, Accuracy…
- Future:
  - *Multimodal Biometrics (?)*
    - Example: Combine fingerprint reader with face recognition
    - Supported in Windows 10



# Attacks on Biometric Authentication

- Possible attacks on face recognition based authentication
- Spoofing attack
  - e.g. hold up picture in front of camera
- Replay attack
  - Record image, and the replay it
- Solution
  - *liveness test*
  - *How?*
    - *Depth detection*
    - *Temperature*


Image courtesy of Danny Smith, UQ

# Liveness Test

- This is hard, ongoing research topic
- Any other ideas?
  - e.g. check if person is blinking regularly
  - Works for spoofing attack, but not replay attack
- Example research idea:
  - Check if reflection of phone screen in eye matches image on screen
    - PhD research, Danny Smith, UQ

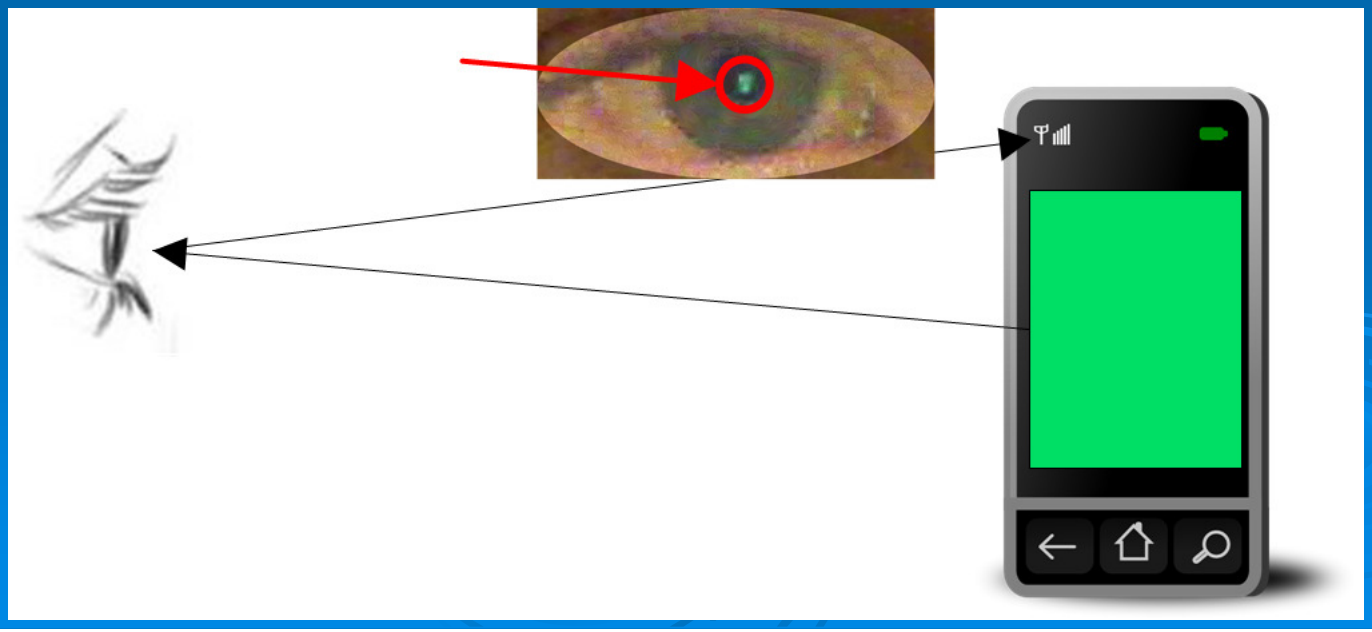


Image courtesy of Danny Smith, UQ

# Biometrics - Limitations

- Biometrics can improve security of Authentication
- But, the technology has limitations
  - Error rates
  - Circumvention
  - Revocation
    - What if biometric information is leaked, e.g. fingerprint, DNA, etc.
    - Cannot easily be revoked or 'reset', such as a passwords
- Biometrics is unlikely to replace passwords in the near future, but rather complement them
  - Multi-factor authentication
- An then there are also Privacy concerns …

# Reading

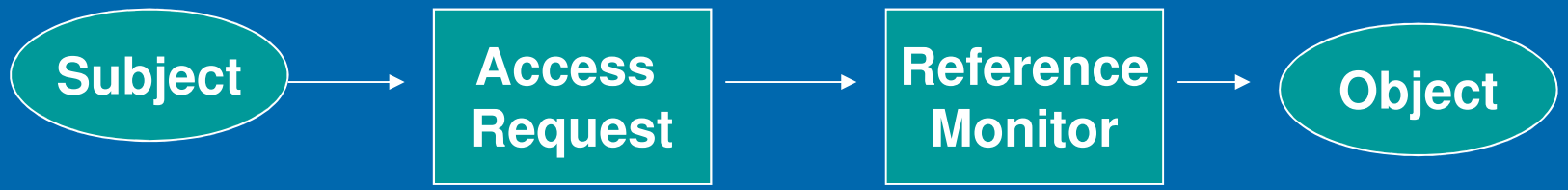
- A. K. Jain et al., "An introduction to biometric recognition." *Circuits and Systems for Video Technology, IEEE Transactions on* 14.1 (2004): 4-20.
  - http://www.cse.msu.edu/~rossarun/BiometricsTextBook/Papers/Introduction/JainRossPrabhakar_BiometricIntro_CSVT04.pdf
- A. K. Jain et al., "Biometrics: A Grand Challenge", Proc. of ICPR (2004)
  - http://biometrics.cse.msu.edu/Publications/GeneralBiometrics/JainetalBiometricsGrandChallenge_ICPR04.pdf

# Any questions?

# COMPUTER BASED ACCESS CONTROL

# Computer Based Access Control (Authorisation)

- We assume user has been authenticated
- How does an Operating System control access to resources (files, printer, memory, database record, network etc.)?
- Fundamental access control model:
  - Subject: active party
    - e.g. user, process
  - Object: passive party
    - e.g. file
    - Roles of object and subject depend on situation, can be reversed
      - Subject can become object and vice versa
  - Reference Monitor: grants or denies access



# Access Control (Authorisation) Policy

- Access Control Policy specifies what subjects can do with objects
- What are the basic operations that can be applied to objects (e.g. files)?
  - Read
  - Write
  - Execute
  - Append (excludes Read access)
    - Example where *Append* is granted, without *Read* access:
    - → Log file
  - Delete
  - …

# Access Control Policy

- How can we specify an access control policy, i.e. *who can do what, with which objects*?
- We define the following:
  - set *S* of *subjects*
  - set *O* of objects
  - set *A* of *access operations*
- Access Rights can be defined as a **Access Control Matrix**
  - Entry $M_{SO}$ specifies the set of access operations subject **s** can perform on object **o**

$$M = (M_{SO})_{s \in S, o \in O} \text{ with } M_{SO} \subset A$$

- Example:

| | Bill.doc | Edit.exe | Fun.exe |
|---|---|---|---|
| Alice | - | {execute} | {execute, read} |
| Bob | {read, write} | {execute} | {execute, read, write} |

# Access Control Matrix

- Access Control Policies are rarely implemented directly as Access Control Matrices
- Why?
  - Hard to maintain for large number of objects and subjects, especially in a dynamic environment
    - e.g. for 10,000 objects and 1,000 subjects, we have a matrix with 10 Million entries
- Alternatives?
  - Store the access rights with the objects
    - → Access Control Lists (ACL)
  - Store access rights with the subjects
    - → Capabilities

# Access Control Lists (ACL)

- Access rights are stored with objects
- Columns of Access Control Matrix (including user names in first column)

- Advantage:
  - Easy to see who has access to specific objects
- How about getting an overview of access rights of an individual users?
- How can access rights of an individual users be revoked?
  - Need to search through all ACLs → expensive operation

| | Bill.doc | Edit.exe | Fun.com |
|---|---|---|---|
| Alice | - | {execute} | {execute, read} |
| Bob | {read, write} | {execute} | {execute, read, write} |

# Access Control Lists

- Managing access rights of a large number of individual users (subjects) via ACLs can be tedious
- Solution?
- Groups (or Roles)
  - Users (subjects) with similar access rights are aggregated in groups and access permissions are given to groups
  - Some policies allow membership to multiple groups, others not
  - Groups can be defined according to roles
    - e.g. in a Bank: teller, branch manager, branch accountant, …
  - Access rights can be revoked by removing a user from a group