# COMP 2410 – Networked Information Systems

## 6. Key Security Safeguards

**Roger Clarke**
**Xamax Consultancy, Canberra**
**Visiting Professor, A.N.U. and U.N.S.W.**

**http://www.rogerclarke.com/II/NIS2410.html#L6**
**http://www.rogerclarke.com/II/NIS2410-6 {.ppt, .pdf}**

**ANU RSCS, 24 March 2016**

Copyright 2013-16 XAMAX Consultancy Pty Ltd
SOME RIGHTS RESERVED
FREE FOR EDUCATION www.aesharenet.com.au/FfE2/



## Networked Information Systems
## This Series of Six Lectures

**Network Infrastructure and Architecture**

1. Network Infrastructure
2. The Architectures of Networked Applications

**Information Assurance and Security**

3. Security of Information and IT
4. Malware and Other Attacks
5. Data Protection and Privacy
6. Key Security Safeguards

Copyright 2013-16 XAMAX Consultancy Pty Ltd



## Key Security Safeguards
## Agenda

1. Minimum Safeguards
2. Service Continuity and Recovery
3. Incident Management
4. Access Control
5. Authentication of Assertions Generally
6. Authentication of (Id)Entity

Copyright 2013-16 XAMAX Consultancy Pty Ltd



## 1. The Absolute-Minimum Security Safeguards

1. Physical Safeuguards
2. Access Control
3. Malware Detection and Eradication
4. Patching Procedures
5. Firewalls
6. Incident Management Processes
7. Logging
8. Backup and Recovery Plans, Procedures
9. Training
10. Responsibility

Copyright 2013-16 XAMAX Consultancy Pty Ltd

http://www.xamax.com.au/EC/ISInfo.pdf

## Beyond the Absolute-Minimum Safeguards

**Risk Asssessment**, leading to at least some of:

11. Data Communications Encryption
12. Data Storage Encryption
13. Vulnerability Testing
14. Standard Operating Environments
15. Application Whitelisting
16. Device Authentication and Authorisation
17. Use of Virtual Private Networks
18. Intrusion Detection and Prevention
19. User Authentication
20. Firewall Configurations, Outbound

Copyright 2013-16 XAMAX Consultancy Pty Ltd
http://www.xamax.com.au/EC/ISInfo.pdf


## 2. Natural and Non-Natural Disasters as Threats to Business Continuity

- **Earthquake** Newcastle 1989, Christchurch 2011
- **Tsunami** Fukushima 2011
- **Cyclone** Darwin 1974 (Tracy), Nth Qld 2011 (Yasi)
- **Flood** Brisbane 2010-11
- **Bushfire** Canberra 2003, Victoria 2009
- **Terrorism** World Trade Center 2001 ('9/11')

Some corporations went bankrupt
Yet some survived despite losing 70% of their staff

Copyright 2013-16 XAMAX Consultancy Pty Ltd
http://www.australia.gov.au/about-australia/australian-story/natural-disasters


## Business Continuity Planning

How an organisation sustains and recovers its business operations after a major security incident

- Identify Priority Business Processes
  (Use Risk Assessment techniques to do that)
- Implement Protections for People, and Other Assets
- Identify Measures to Re-Acquire Key Assets
- Specify Interim and Recovery Processes
- Rehearse Those Processes
- Review and update the Business Continuity Plan

Copyright 2013-16 XAMAX Consultancy Pty Ltd
Boyle & Panko 'Corporate Computer Security'
Pearson 2013, p. 581-585


## IT Disaster Recovery Planning

How an organisation sustains and recovers its IT infrastructure after a major security incident

- Identify Priority IT Infrastructure
  (Use Risk Assessment techniques to do that)
- Imagine Disaster Scenarios
- Imagine Recovery Scenarios
- Specify Processes
- Rehearse Processes
- Review and update the IT Disaster Recovery Plan

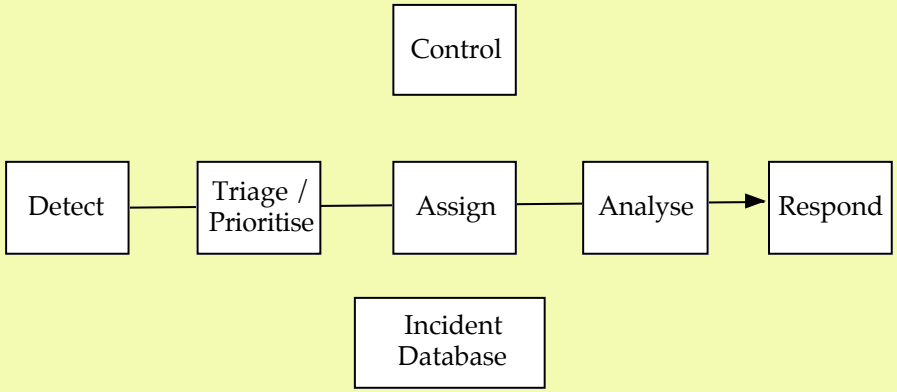
Copyright 2013-16 XAMAX Consultancy Pty Ltd
Boyle & Panko 'Corporate Computer Security'
Pearson 2013, p. 585-590

# Key IT Infrastructure Issues

- **Data**
  - Backup / Replication
  - Dispersal
  - Recovery Procedures
    - Specified
    - Rehearsed
- **People**
  - Cross-Training
  - Dispersion
- **Facilities**
  - Duplication – Hot / Warm / Cold-Site
- **Processing**
  - Interim and Fallback (Manual) Procedures

Copyright 2013-16 XAMAX Consultancy Pty Ltd


# 3. Incident Management



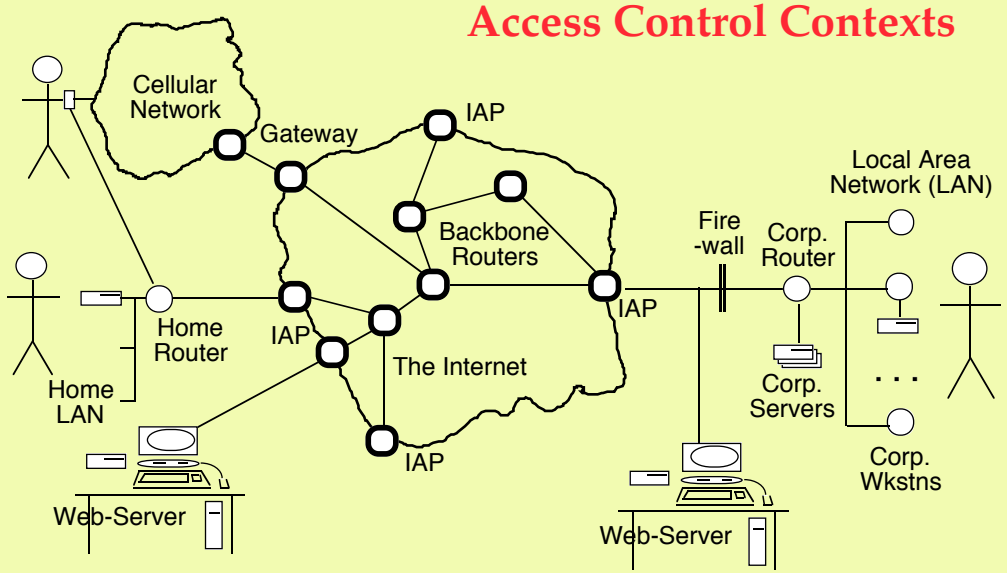

Copyright 2013-16 XAMAX Consultancy Pty Ltd
http://www.rogerclarke/SOS/ChgeCtl90.html#IR


# 4. Access Control

- Protect System Resources against Unauthorised Access
- **Provide convenient access** to the right people, to relevant data and software capabilities, by providing User Accounts with Privileges and Restrictions
- **Prevent access** by the wrong people to data and software capabilities
- Person-Based, or Role-Based (RBAC)

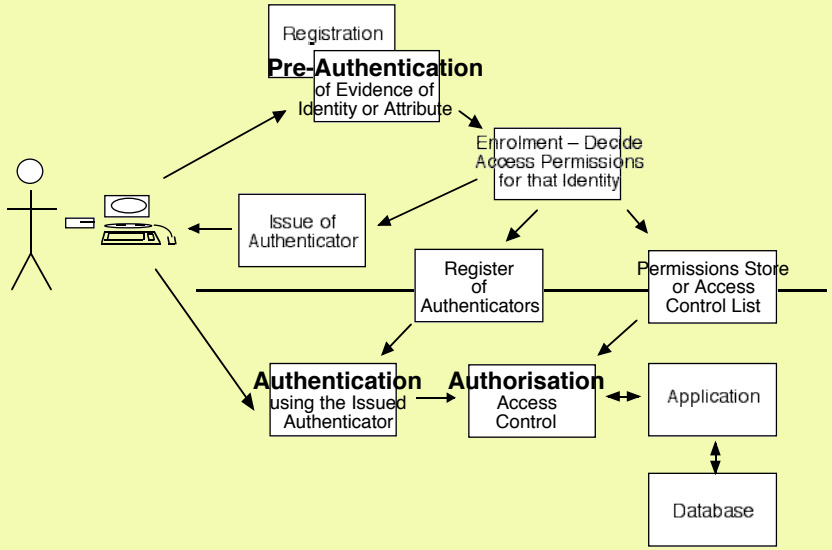
Copyright 2013-16 XAMAX Consultancy Pty Ltd


# Access Control Contexts




Copyright 2013-16 XAMAX Consultancy Pty Ltd

# Access Control Processes




Copyright 2013-16 XAMAX Consultancy Pty Ltd



# Threats to Passwords

1. Guessing
2. 'Brute Force' Guessing
3. Visual Observation
4. Electronic Observation
5. Interception
6. Phishing
7. Use of One Password for Multiple Accounts
8. Discovery of a Password Database
9. Compromise of the Password-Reset Process
10. Continued Use of a Compromised Password
11. Compromise of a Password Stored by a Service-Provider
12. Acquisition and Hacking of the Password-Hash File

Copyright 2013-16 XAMAX Consultancy Pty Ltd

http://www.rogerclarke.com/II/Passwords.html



# Ways of Strengthening Access Control

- Channel Encryption, e.g. SSL/TLS, so that even if the password is intercepted, it is not 'in clear'
- Transmission of only a hash of the password
- Server-Side Storage of only a hash of the password
- One-Time Passwords

Copyright 2013-16 XAMAX Consultancy Pty Ltd



# 5. Authentication of Assertions

- **Authentication**: A process that establishes a level of confidence in an Assertion
- **Assertion**: A declaration made by some party
- **Authenticator**: Evidence relevant to an Assertion
- **Credential**: A physical or digital Authenticator
- **Evidence of Identity (EOI)**
  *[[ Proof of Identity (POI) ]]*
  An Authenticator for Identity Assertions

Copyright 2013-16 XAMAX Consultancy Pty Ltd

## Categories of Assertions

- About Real-World Facts
- About Data Quality (accuracy, timeliness, ...)
- About Value
- About Location
- About Documents

- About Attributes
- About Principal-Agent Relationships

---

- About Identities
- About Entities

Copyright 2013-16 XAMAX Consultancy Pty Ltd


## Value Assertion

**Value is transferred to/from an (Id)entity or Nym**

## Authentication of Value Assertions

**For Goods**

- Inspect them
- Get them put into Escrow, for release by the Agent only when all conditions have been fulfilled

**For Cash**

Release the Goods only:

- For Cash On Delivery
- After Clearing the Cheque
- Against a Credit-Card Authorisation
- After a Debit-Card Transaction

Copyright 2013-16 XAMAX Consultancy Pty Ltd


## Attribute Assertion

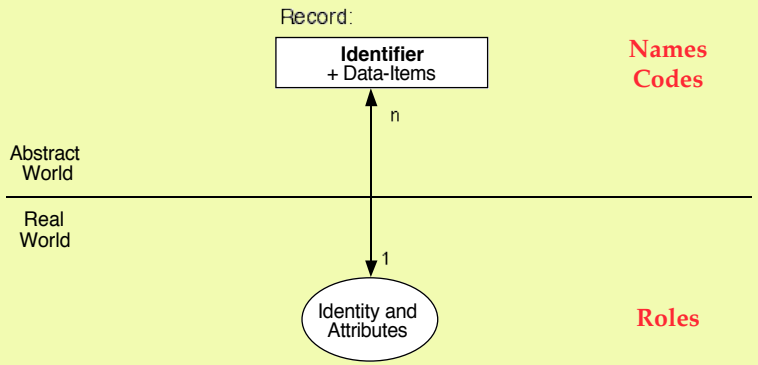
- **An Identity or Nym has a particular Attribute**:
  - Age / DoB before or after some Threshhold
  - Disability, Health Condition, War Service
  - Professional or Trade Qualification

## Authentication of Attribute Assertions

- ID-Card and DoB (may or may not record ID)
- Bearer Credential (ticket, disabled-driver sticker)
- Attribute Certificates (with or without ID)

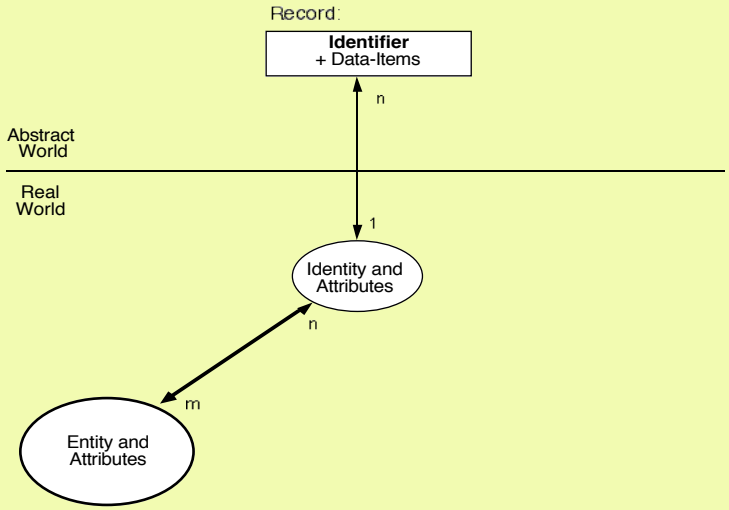
Copyright 2013-16 XAMAX Consultancy Pty Ltd


## 6. Identity and Identifier




Copyright 2013-16 XAMAX Consultancy Pty Ltd

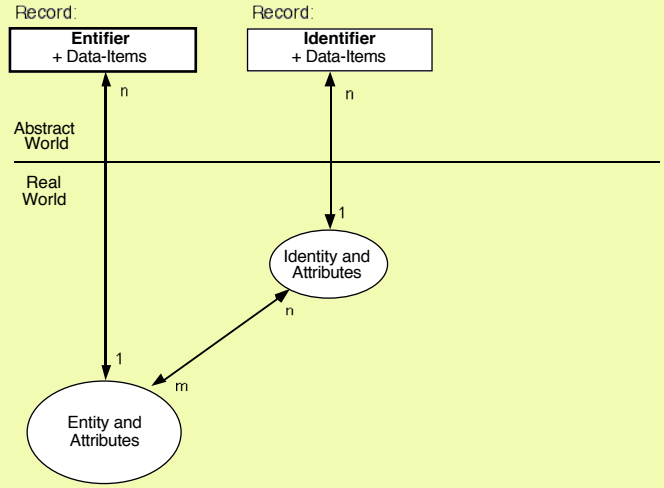
# The Entity/ies underlying an Identity




Copyright
2013-16
XAMAX Consultancy Pty Ltd



# Entity and Entifier




Copyright
2013-16
XAMAX Consultancy Pty Ltd



# The Digital Persona

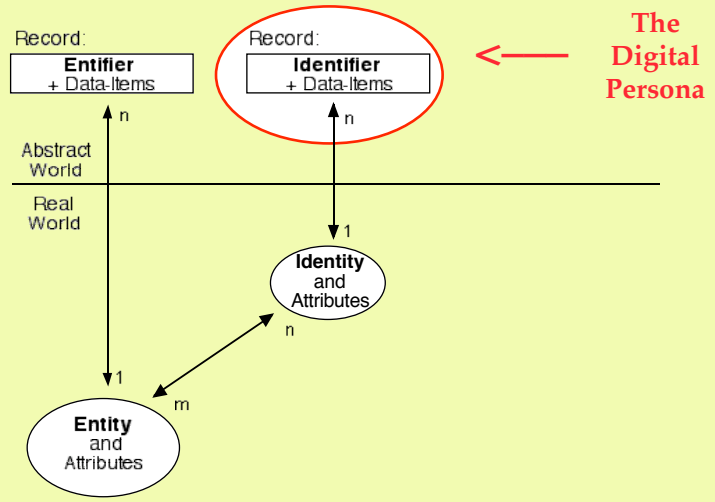
A model of an individual's public personality
based on data and maintained by transactions
and intended for use as a proxy for the individual

**A group of data items that together**
**form a simplified representation of an identity**

http://www.rogerclarke.com/DV/CFP93.html (Feb 1993)
http://www.rogerclarke.com/DV/DigPersona.html (Jun 1994)
http://www.rogerclarke.com/DV/HumanID.html (Dec 1994)
http://www.rogerclarke.com/ID/DP12.html (Sep 2014)

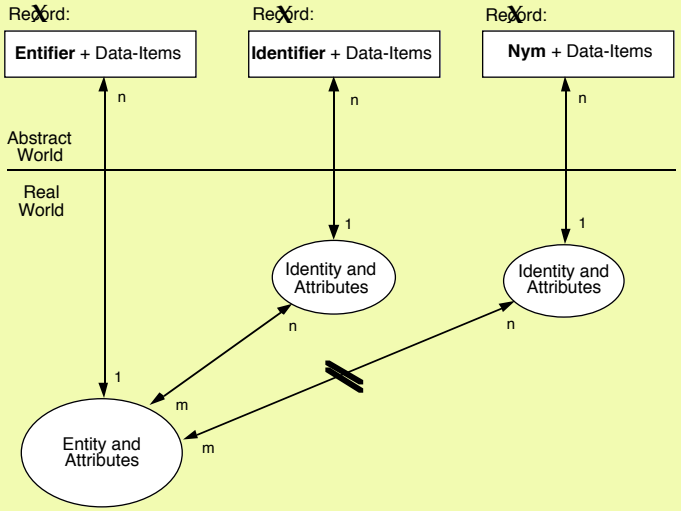
Copyright
2013-16
XAMAX Consultancy Pty Ltd






Copyright
2013-16
XAMAX Consultancy Pty Ltd

# Nymity




The Digital Persona

Copyright 2013-16 XAMAX Consultancy Pty Ltd



# Nym

## A Digital Persona

i.e. a set of attributes of an Identity

that is sufficient to distinguish that Identity from other instances of its class

but

**that is not sufficient to enable association with a specific Entity**

**Pseudonym** – association is not made, but is possible

**Anonym** – association is not possible

Copyright 2013-16 XAMAX Consultancy Pty Ltd



# Nymality is Normality

aka ('also-known-as'), alias, avatar, character, nickname, *nom de guerre*, *nom de plume*, manifestation, moniker, personality, profile, pseudonym, pseudo-identifier, sobriquet, stage-name

Cyberpace has adopted those and spawned more:

account, avatar, handle, nick, persona, ...

Copyright 2013-16 XAMAX Consultancy Pty Ltd



# Common Nymous Transactions

- Barter transactions
- Visits to Enquiry Counters in government agencies
- Telephone Enquiries
- Inspection of publications on library premises
- Access to Public Documents by electronic means, at a kiosk or over the Internet
- Cash Transactions, incl. the myriad daily payments for inexpensive goods and services, gambling, road-tolls
- Voting in secret ballots
- Treatment at discreet clinics, e.g. for sexually transmitted diseases

Copyright 2013-16 XAMAX Consultancy Pty Ltd

## (Id)Entification

- **Identification**
  The **process** of associating a Digital Persona with a particular Identity, by acquiring an Identifier for the Identity
- **Entification**
  The **process** of associating a Digital Persona with a particular Entity, by acquiring an Entifier for the Entity
- **Token**
  A recording medium for an (Id)entifier
- **Identity Silo**
  A restricted-purpose Identity, and associated Identifier(s)

Copyright 2013-16 XAMAX Consultancy Pty Ltd


## Human Identification

- **Identification Generally**
  The process of associating a Digital Persona with a particular Identity, by acquiring an Identifier for the Identity
  Applies to natural objects, artefacts, animals, ...
- **Human Identification in Particular**
  - Acquisition of a Human Identifier (Commonly a Name or a Code)
  - High-Reliability Lookup in a Database (1-with-many comparison, a single confident result)

Copyright 2013-16 XAMAX Consultancy Pty Ltd


## Human Identity Authentication

- **What the Person Knows**
  e.g. mother's maiden name, Password, PIN
- **What the Person Has ('Credentials')**
  e.g. a Token, such as an 'ID-Card', a Ticket
  e.g. a Digital Token such as
  "a Digital Signature consistent with the Public Key attested to by a Digital Certificate"

Copyright 2013-16 XAMAX Consultancy Pty Ltd


## A Sample Personal Device – The Mobile Phone

- **Entifier for the Product** – model-name, model-number
- **Entifier for the Handset** – Serial-Number of the device
  - Mobile Equipment Identity (**IMEI**) – GSM / UMTS
  - Electronic Serial Number (ESN) or Mobile Equipment Identifier (MEID) – CDMA
- **Identifier for the Persona** – Serial-Number of a chip, the International Mobile Subscriber Identity (**IMSI**)
  - Subscriber Identity Module (SIM) – GSM / UMTS
  - Removable User Identity Module (R-UIM) or CDMA Subscriber Identity Module (CSIM) – CDMA
  - Universal Subscriber Identity Module (USIM) – 3G
- **Proxy-(Id)entifier** – MAC Address / NICId, or IP-Address

Copyright 2013-16 XAMAX Consultancy Pty Ltd

## Human Identity Authentication

- **What the Person Knows**
  e.g. mother's maiden name, Password, PIN
- **What the Person Has ('Credentials')**
  e.g. a Token, such as an 'ID-Card', a Ticket
  e.g. a Digital Token such as
  "a Digital Signature consistent with the
  Public Key attested to by a Digital Certificate"

## Human Entity Authentication

- **What the Person Does** (Dynamic Biometrics)
- **What the Person Is** (Static Biometrics)
- **What the Person Is Now** (Imposed Biometrics)

Copyright 2013-16 XAMAX Consultancy Pty Ltd


## Quality Challenges in Biometric Applications

**Dimensions of Quality**

- Reference-Measure
- Association
- Test-Measure
- Comparison
- Result-Computation

**Other Aspects of Quality**

- Vulnerabilities
- Quality Measures
- Counter-Measures
- Spiralling Complexity
- Consequences

Copyright 2013-16 XAMAX Consultancy Pty Ltd


## Ways of Strengthening Access Control

- Channel Encryption, e.g. SSL/TLS, so that even if the password intercepted, it is not 'in clear'
- Transmission of only a hash of the password
- Server-Side Storage of only a hash of the password
- One-Time Passwords
- Multi-Factor Use Authentication:
  - **What You Know**
    password, 'shared secrets'
  - **What You Have**
    one-time password gadget, a digital signing key
  - **Where You Are**
    your IP-address, device-ID
  - **What You Are**
    a biometric, e.g. fingerprint
  - **What You Do**
    time-signature of password-typing key-strikes
  - **Who You Are Known to Be**
    reputation, 'vouching'

Copyright 2013-16 XAMAX Consultancy Pty Ltd


## Key Security Safeguards Agenda

1. Minimum Safeguards
2. Service Continuity and Recovery
3. Incident Management
4. Access Control
5. Authentication of Assertions Generally
6. Authentication of (Id)Entity

Copyright 2013-16 XAMAX Consultancy Pty Ltd

# COMP 2410 – Networked Information Systems

## 6. Key Security Safeguards


**Roger Clarke**
**Xamax Consultancy, Canberra**
**Visiting Professor, A.N.U. and U.N.S.W.**


**http://www.rogerclarke.com/II/NIS2410.html#L6**
**http://www.rogerclarke.com/II/NIS2410-6 {.ppt, .pdf}**

**ANU RSCS, 24 March 2016**


Copyright 2013-16 XAMAX Consultancy Pty Ltd
SOME RIGHTS RESERVED
FREE FOR EDUCATION www.aesharenet.com.au/FfE2/

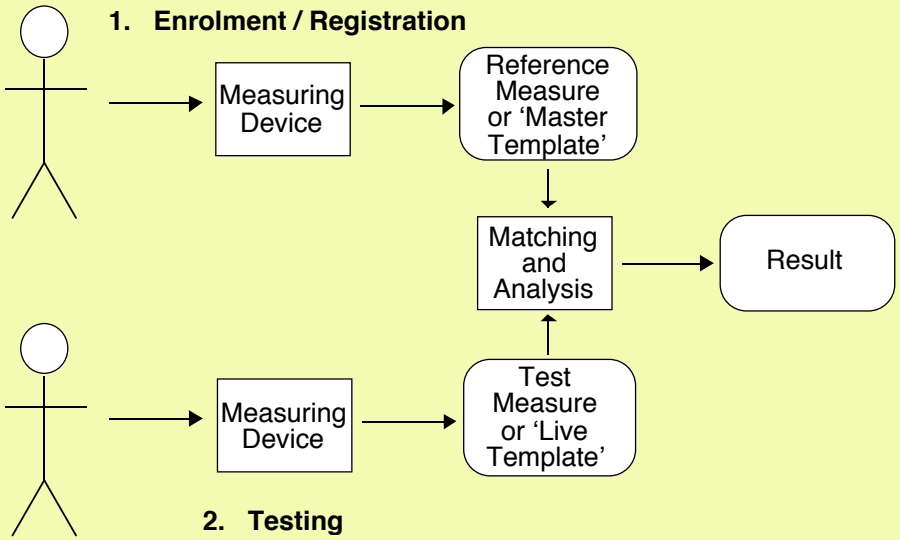



# Drill-Down Slides

Copyright 2013-16 XAMAX Consultancy Pty Ltd



# The Biometric Process




Copyright 2013-16 XAMAX Consultancy Pty Ltd



# Quality Challenges in Biometric Applications

**Dimensions of Quality**

- Reference-Measure
- Association
- Test-Measure
- Comparison
- Result-Computation

**Other Aspects of Quality**

- Vulnerabilities
- Quality Measures
- Counter-Measures
- Spiralling Complexity
- Consequences

Copyright 2013-16 XAMAX Consultancy Pty Ltd

## Biometrics
## Reference-Measure Quality

- The Person's Feature ('Enrolment')
- The Acquisition Device
- The Environmental Conditions
- The Manual Procedures
- The Interaction between Subject and Device
- The Automated Processes

Copyright 2013-16 XAMAX Consultancy Pty Ltd


## Biometrics
## Association Quality

- Depends on a Pre-Authentication Process
- Subject to the Entry-Point Paradox
- Associates data with the 'Person Presenting' and hence entrenches criminal IDs
- Risk of an Artefact Substituted for, or Interpolated over, the Feature

Copyright 2013-16 XAMAX Consultancy Pty Ltd


## Biometrics
## Test-Measure Quality

- The Person's Feature ('Acquisition')
- The Acquisition Device
- The Environmental Conditions
- The Manual Procedures
- The Interaction between Subject and Device
- The Automated Processes

Copyright 2013-16 XAMAX Consultancy Pty Ltd


## Biometrics
## Comparison Quality

- **Feature Uniqueness**
- **Feature Change**:
  - Permanent
  - Temporary
- **Ethnic/Cultural Bias**

  "Our understanding of the demographic factors affecting biometric system performance is ... poor" (Mansfield & Wayman, 2002)
- **Material Differences** in:
  - the Processes
  - the Devices
  - the Environment
  - the Interactions
- **An Artefact**:
  - Substituted
  - Interpolated

Copyright 2013-16 XAMAX Consultancy Pty Ltd

## 'Factors Affecting Biometrics Performance'
### (Mansfield & Wayman, 2002)

- **Demographics** (youth, aged, ethnic origin, gender, occupation)
- **Template Age**
- **Physiology** (hair, disability, illness, injury, height, features, time of day)
- **Appearance** (clothing, cosmetics, tattoos, adornments, hair-style, glasses, contact lenses, bandages)
- **Behaviour** (language, accent, intonation, expression, concentration, movement, pose, positioning, motivation, nervousness, distractions)
- **Environment** (background, stability, sound, lighting, temperature, humidity, rain)
- **Device** (wear, damage, dirt)
- **Use** (interface design, training, familiarity, supervision, assistance)

Copyright 2013-16 XAMAX Consultancy Pty Ltd


## Biometrics
## Result-Computation Quality

- Print Filtering and Compression:
  - Arbitrary cf. Purpose-Built
- The Result-Generation Process
- The Threshhold Setting:
  - Arbitrary? Rational? Empirical? Pragmatic?
- Exception-Handling Procedures:
  - Non-Enrolment
  - Non-Acquisition
  - 'Hits'

Copyright 2013-16 XAMAX Consultancy Pty Ltd


## Biometrics
## Consequences of Quality Problems

- A Tolerance Range has to be allowed
- 'False Positives' / 'False Acceptances' arise
- 'False Negatives' / 'False Rejections' arise
- Tighter Tolerances (to reduce False Negatives) increase the rate of False Positives; and vice versa
- The Scheme Sponsor sets (and re-sets) the Tolerances
- Frequent exceptions are mostly processed cursorily
- Occasional 'scares' slow everything, annoy everyone

Copyright 2013-16 XAMAX Consultancy Pty Ltd


## Design Factors Using Biometrics
## Privacy-Sensitive and Cost-Effective

**Technologies and Products**

- A Privacy Strategy
- Privacy-Protective Architecture
- Open Information
- Independent Testing using Published Guidelines
- Publication of Test Results

**Application Design Features**

- No Central Storage
- Reference Measures only on Each Person's Own Device
- No Storage of Test-Measures
- No Transmission of Test-Measures
- Devices Closed and Secure, with Design Standards and Certification
- Two-Way Device Authentication

**Application Design Processes**

- Consultation with the Affected Public from project commencement onwards
- Explicit Public Justification for privacy-invasive features
- PIAs conducted openly, and published
- Metricated pilot schemes

**Laws**, to require compliance with the above

**Laws**, to preclude:

- Retention of biometric data
- Secondary use of biometric data
- Application of biometrics absent strong and clear justification
- Manufacture, import, installation, use of non-compliant biometric devices
- Creation, maintenance, use of a database of biometrics

Copyright 2013-16 XAMAX Consultancy Pty Ltd