



**CESG**

# ***CESG Biometric Security Capabilities Programme:***

## ***Method, Results and Research Challenges***

Matthew Lewis - Biometric Vulnerability Assessment

Philip Statham - Biometrics Programme Manager

[matthew.lewis@cesg.gsi.gov.uk](mailto:matthew.lewis@cesg.gsi.gov.uk)

[philip.statham@cesg.gsi.gov.uk](mailto:philip.statham@cesg.gsi.gov.uk)

# Outline

- Programme Overview
- Existing Security Investigations
- CESG's Approach / Method
- Initial Investigations and Results
- Security Issues and Possible Countermeasures
- Research Challenges (for Biometric Security)

# Vulnerabilities Programme Overview

- Develop vulnerabilities evaluation methodology *(specifically to support Common Criteria evaluations of biometric systems)*
- Assess the security capabilities of current biometric products
- Improve security capabilities of future products
- Provide advice to CESG policy

*Practical investigations are feeding the methodology*

# Published Ad-hoc “Evaluations”

- Six biometric devices point their finger at security
  - *Network computing – Jun 1998 (Fingerprint)*
- Biometrics security
  - *PC magazine – Feb 1999 (Fingerprint / Face / Voice)*
- Fingerprint recognition—don’t get your fingers burned
  - *Van der Putte, Keuning, Jan 2000*
- Impact of artificial “gummy” fingers
  - *Matsumoto, Jan 2002*
- Biometric access devices & programs put to the test
  - *c’t magazine, may 2002 (Fingerprint / Face / Iris)*

# spoofing Biometric Systems



# Approach

- Contact vendors to participate in the programme
- Perform security investigation of product
- Issue report to vendors on investigation results (encourage feedback)
- Investigation results inform the methodology for biometric security evaluation

# Method

- Split system into component parts
- Identify vulnerabilities for each part and interfaces
- Relate to modes of attack
  - *Zero Effort / Casual Impostor Techniques*
  - *Weak / Easy Template Generation*
  - *Access to Template / Data Store*
  - *Spoofing - Artificial Attempts, Mimicry and Fakes*
  - *Wire Capture / Replay*

3 Investigation Levels: Generic, Technological and Application

# Image Quality Control

## *What is a fingerprint?*

Portion of  
finger on  
sensor



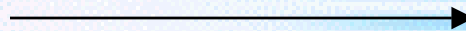
Template with few features

Lifting  
finger on/off  
sensor



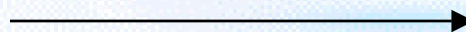
Null image / template

Multiple  
fingers on  
sensor






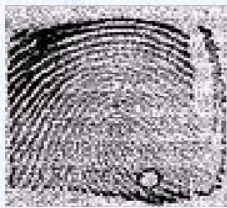

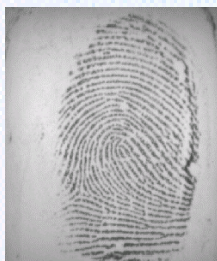


Either finger can be used at  
authentication

Non-  
fingerprint  
images



Drawing on a thin piece of  
tissue paper can be enrolled  
and used at authentication

# SpooF Fingertips

	Real	SpooF
CCD 1		
CCD 2		
Optical 1		
Optical 2		

- Successful enrolment and authentication with spooF fingertips

- Liveness detection can be satisfied with live finger behind artefact

- Note: This is a cooperative effort

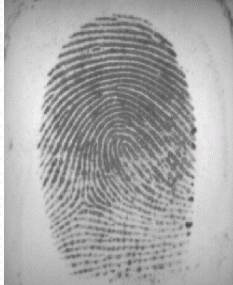
# Access to Template / Data Store

## *Reconstructing Enrolment Images*

**Original**



**Reconstruction**



Templates / Data are often not protected

# Access to Template / Data Store

## *Reverse Engineering Template Data: Example*

- View fingerprint template in hexadecimal format –  
Observe **3 byte triplets** separated by null (00) values
- Trailing **un-used bytes** padded with null values (00)
- Byte triplets likely to represent minutiae (x,y) coordinates and angle
- Possible to remove / add minutiae points

```
dc cc cc 00 cd ff ff 00 4b f6 3b 00 ab f1 2f 00  
cb 3a 60 00 09 b0 1d 00 bc 6f 3e 00 36 bf 01 00  
c4 53 03 00 74 5f a0 00 74 b9 08 00 4e 50 ff 00  
cc cc cc 00 ce ef fe 00 20 7f 27 00 00 00 00 00  
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

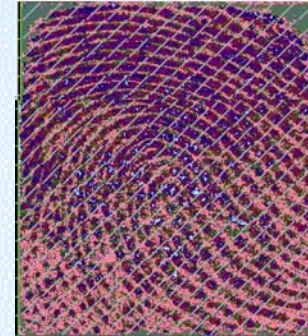
# Wire Snooping

*Intercepting and Reconstructing Biometric Data*

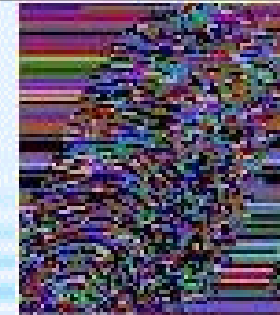
**Real**

**Reconstruction**

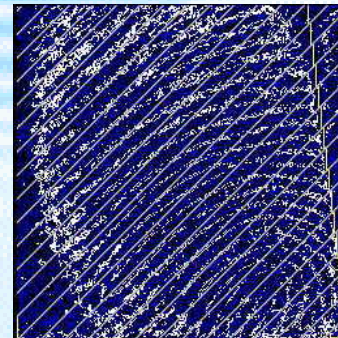
**CCD 1 (USB)**



**CCD 2 (Ethernet)**



**Optical (USB)**



# Facial Recognition Tests

- Enrolment, identification, verification of  
*live subjects*  
*printed cartoon images*  
*(printed) photo images*
- Identification, verification against stored images
- Effect of disguise on performance

# Face Recognition Tests

## *Image Acquisition Criteria*

Enrolling Simple / Easy Images



Success:

No

No

Yes

**A**

**B**

**Paper print of A**

**(A&B Morphed)**

Authenticating against enrolled user with photographs and morphed images



Livecheck off - Yes

Livecheck on – Yes but with difficulty

# Face Recognition Tests

## *Effect of Disguise*



Enrolment / Reference Image



Normal ID: 0.767342



0.762008 0.76242 0.736215 0.707423 0.723648 0.66777

# Face Recognition Tests

## *Effect of Disguise*



Enrolment / Reference Image

Normal ID: 0.788537

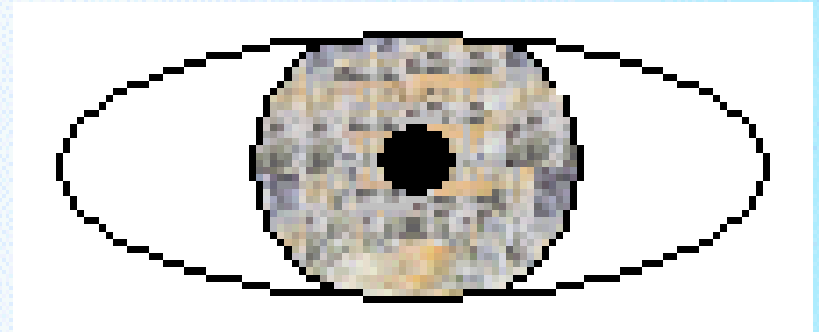


0.75622 0.713133 0.73317 0.72323 0.71426 0.716726

# Iris Recognition Tests

## *Enrolling 2D Images*

Constructing fake irises (used at enrolment and authentication)



Enrolling and authenticating with printed images of irises



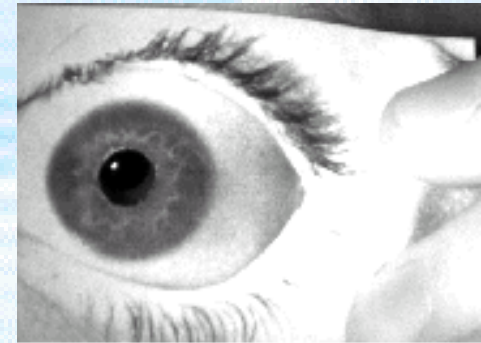
Satisfy liveness checking with:

- Live eye behind pierced hole in pupil
- Soft contact lens placed over iris

# Spooing Iris Recognition

- Iris camera stores images taken at enrolment (greyscale under IR illumination)
- Image printed in greyscale on high dpi LaserJet printer
- liveness detection satisfied with live eye behind pierced hole at pupil

Enrollment	Authentication	Positive Match?
2D Image	2D Image	Yes
Real Iris	2D Image	Under Investigation
2D Image	Real Iris	Under Investigation



# Future Work

- Continued practical investigation
- Continued development of methodology
- Investigation of voice recognition
  - Preliminary investigation conducted by CESG
  - Successful enrolment and authentication of random sounds and playback of human recordings
  - National Physical Laboratory (NPL) to assist in testing

# Security Issues & Possible Countermeasures

- **Quality Control**
  - *Software awareness of **good** sample quality and expected input*
- **Data / Template Protection**
  - *Integrity checks and cryptographic protection on user records and templates*
- **Spoofing**
  - *Liveness checking and anti-spoofing techniques*
- **Wire Data Protection**
  - *Integrity checks and cryptographic protection of wire data*
  - *Device authentication*
  - *Synchronisation / time-stamping / unique session keys*

**Supervision can be a good countermeasure!**

# Research Challenges

## *for Biometric Security*

### **Can biometric security systems answer these questions?**

- *Is the sample presented to the sensor alive and real?*
  - Challenge: Effective methods for liveness detection
  - Challenge: Effective anti-spoofing techniques
- *Is the sample correctly presented?*
  - Challenge: Identify the same sample from positional and rotational variances
- *Is image quality sufficient for good image capture?*
  - Challenge: Software methods to determine sample is of sufficient quality and corresponds to expected input
- *Is there any assurance of template integrity?*
  - Challenge: Make templates secure

**Thank you for your  
attention**



**Further Information**

**[www.cesg.gov.uk](http://www.cesg.gov.uk)**

**– click on biometrics link**

**Questions?**



**CESG**