

# **Recent Developments in Biometric Vulnerability Assessment by the Biometrics Institute**

**Dr Geoff Poulton and Dr. Ted Dunstone**

# The Story So Far

- BI has developed a methodology for assessing biometric vulnerability
  - Partly supported by PM&C
- Successfully completed: **Face, Finger**
- Current: **Voice**
  
- Problem:
  - We can use the methodology...
  - **But can't publish or use the results - yet!**
- Solution
  - Carry out independent studies

## Speaker Verification Project - Current Status

- Lab established at University of Canberra
- Literature review complete
- One voice system being tested
  - Selected Threats: T.Mimic, T.Replay and T.Lambtemplate
  - Completion expected by end of May 2009

# Test Laboratory at University of Canberra



- Speaker Verification Measurement setup

# Results

- What we can say:
  - Project has met all its goals so far
  - Some preliminary tests have been carried out
    - Results consistent with previously reported results from other researchers
  - We believe the methodology will work well for voice recognition

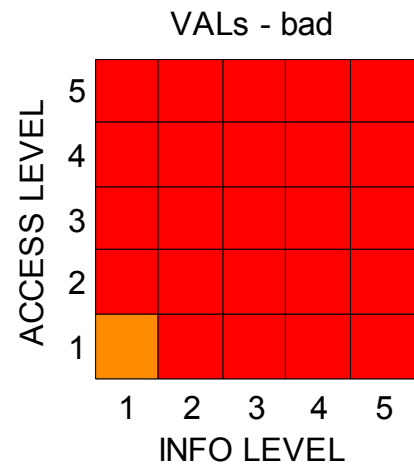
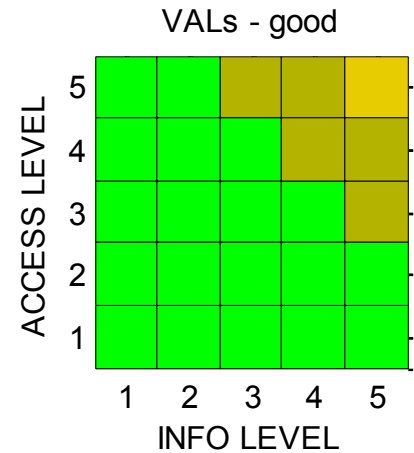
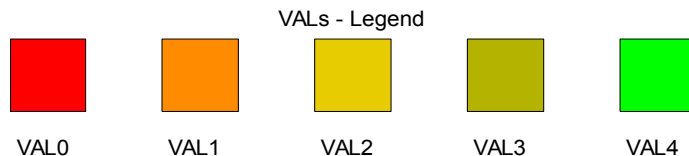
## BI Independent Study\*

- Apply the methodology to a fingerprint system
- Aims:
  - Results we can publish and talk about
  - A set of resources for testing other systems
    - Hardware
    - Software
    - Usable fingerprint database
  - Everything we need to rapidly test other systems

\* Carried out by Geoff Poulton Research for the Biometrics Institute

# Key Concept – VAL

- A VAL (Vulnerability Assurance Level) is a **GUARANTEE\***
  - Max. % of successful spoofing attacks
- VAL4: <1 in 100 attacks succeed
- VAL3: <1 in 30       "       "
- VAL2: <1 in 10       "       "
- VAL1: <1 in 3       "       "
- VAL0: essentially no guarantee



\* At a 95% confidence level

# System and Attacks

## System

- Hardware:
  - digitalPersona U are U 400B
- Software:
  - Neurometrics Verifinger

## Spoofing Attack Methods

- Artefact
  - (fake finger)
- “Lamb” template
  - (enrolled template which can admit multiple attackers)



# First Attack Method - Artefact

- Types of Artefact
- Chopped off real finger
  - Extreme, but might work
    - (may fail a liveness check)
- Simple copies on paper or transparency
  - Won't work with most scanners
    - (including the one under test)
- Moulded artificial finger pad
  - Silicone, gelatine or other material
  - Most common choice
    - Selected for this study (silicone)

# Conclusions

- The system is extremely vulnerable to an Artefact attack
- Highly vulnerable to a Lambtemplate attack
  - For up to four attackers
- All resources necessary to test other fingerprint systems have been generated by the project
  - A proven methodology
  - A set of artefacts
  - A test database with required permissions
- This is a good basis for the Biometric Vulnerability Assessment Service (BVAS) offered by the BI

## **Concluding Remarks**

If your organisation is interested in having a system tested please contact the Biometrics Institute

Request a copy of the “Biometric Vulnerability: A Principled Assessment Methodology” White Paper by email.

Isabelle Moeller (+61 2 9431 8686)

Email: **[manager@biometricsinstitute.org](mailto:manager@biometricsinstitute.org)**

**Feel free to speak to me or Isabelle if you would like more information.**