

# **Software Countermeasures for Biometric Systems**

**Biometric Consortium Conference  
September 21, 2005**

**Conor White, Chief Technology Officer, Daon**

- **Biometrics are NOT a “security solution”**
  
- **Biometrics are part of a security solution**
  - Can provide highest levels of identity assurance
  - Can also be the weakest link if not implemented correctly
  
- **This presentation focuses on some of the key issues associated with the software environment in which biometric technology (readers & algorithms) get deployed**

# On the Internet, nobody knows you're a Dog!!!



- And a Pawprint reader alone is insufficient to make the determination!

- **Security is all about risk management**
- **Nothing is 100% secure**
  - Not biometrics
  - Not smart cards
  - Not RFID
  - Not encryption
- **Security is an analysis of risk and an implementation of appropriate measures to lower risk to an acceptable level**



# What threats are present

## ■ Assume a hostile network

- Eavesdropping on sensitive traffic
- Injection/deletion of messages

## ■ Assume a hostile environment

- Database may be compromised
- Machines may be physically attacked
- Attacks launched against operating system, identity management software or biometric matchers

## ■ Biometric data must be transmitted & stored securely

- Privacy concerns (legislation)
- Risk of legal challenges if stolen

- **In terms of biometrics, we must provide an identity assurance framework that:**
  1. Securely manages sensitive biometric data
  2. Ensures the privacy of users' biometric data
  3. Resists attacks launched by insiders/outsideers
  4. Provides for non-repudiation of activities
  5. Implements Holistic environment/platform security
  6. Offers security independent of network
  
- **Some issues:**
  - Data – In Motion and at Rest
  - Authentication of Participants
  - System Security
  - Anti-spoofing/Liveness detection

## ■ Considerations

- First point of attack is the network
- Encryption is not necessarily the answer
  - Encryption is easy
  - Key management is hard!
- Insertion of rogue messages
- Man-in-the-middle attacks
- Replay Attacks
- Non-repudiation of participants (people and systems/end points)



## ■ Digital Signatures

## ■ Proven Encryption

## ■ Message liveness – e.g. nonces

## ■ Standard network/transport security standards

## ■ Industry embracing Service-Oriented Architectures

- Security standards for message security (WS-Security)

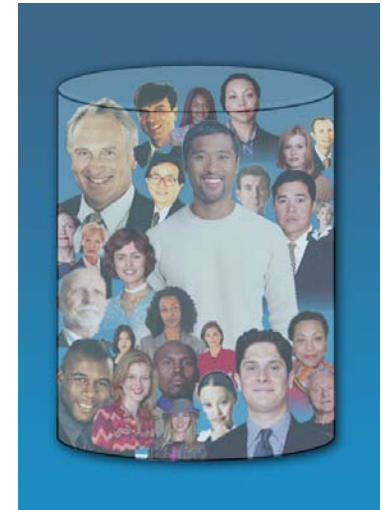
## ■ Considerations:

- Store biometric data securely
- Database theft
- Privacy of data – risk of compromise
- Digital Identity Integrity

## ■ Encrypting data is not sufficient

## ■ Key Management

- Hardware based key stores
- Different theft “channel” - can’t be “logically” stolen



- **Consider**
  - People accessing the system
  - Systems accessing the system
  - Integration with higher-level security schemes
  - External CA infrastructure
  - Remote Authentication
  - Single Sign-On
  
- **Integrate with industry standard protocols and architectures**
  
- **Federated Trust Infrastructures**
  - E.g. SAML, Liberty
  
- **Biometric Trust Infrastructures**

## ■ Enterprise Security Safeguards

- Firewalls
- Intrusion Detection
- AV Tools

## ■ Software component integrity

## ■ Audit trail

- Secure audit trails are necessary for non-repudiation



C:\program files\<<vendor>\Activity\_20050921.log

This is NOT  
an audit trail

## ■ Is it really a credible threat

- Yes
- It must be solved for mainstream (non-attended) access

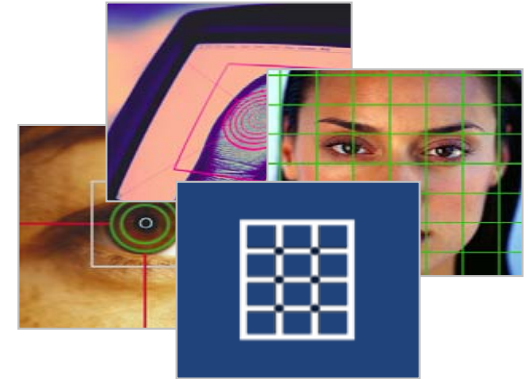
## ■ Can it only be solved through new devices

- No - it can't be solved by devices alone
- Device detection of liveness is important – but as attacks get more sophisticated, cannot be relied on alone.
- Combining device and software techniques provides the best results



## ■ Multi-biometrics

- Use of different biometric types
- Use of multiple captures of the same type
- Biometric Fusion
  - E.g. finger and face, iris and face



## ■ Multi-factor

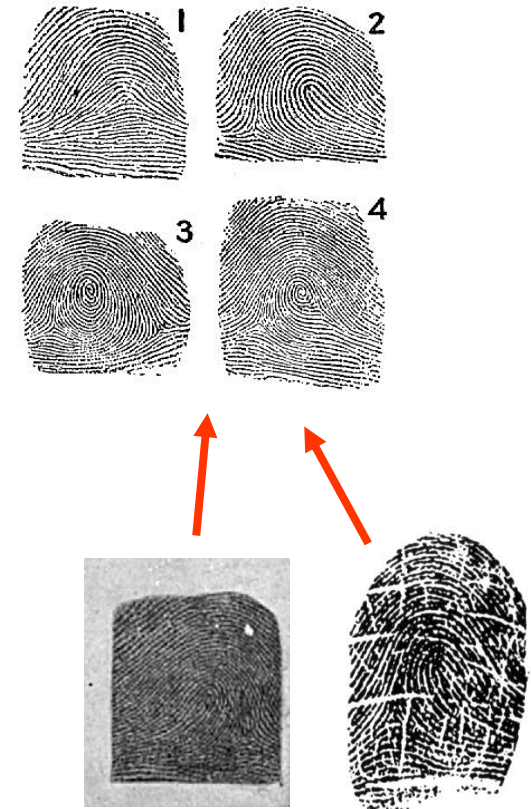
- Biometric (something you are)
- Token (something you have)
- PIN/Passphrase (something you know)

## ■ Biometric Quality Assessment

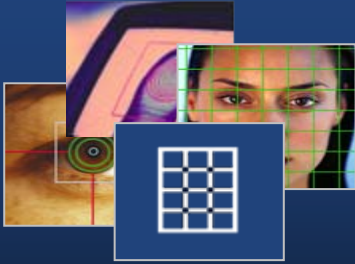
- Consistency of quality scores
- Person-centric management of biometric thresholds

# Countermeasures to Spoofing

- **Out of channel challenges**
  - E.g. Phone call
- **Directed Sample Challenge**
  - Randomly ask for different fingers
  - Use multiple samples
- **Multi-sample Imaging**
  - Enrolment from nail to nail
  - Ask for movement of finger (rolling)
  - Latents generally just a subset of finger
- **3D technologies**
- **Pressure variances – spoof vs live fingers**



## Flexibility



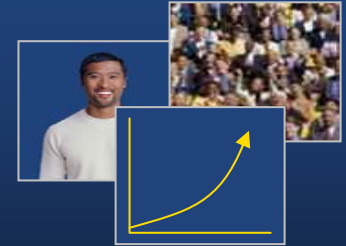
Any form of  
identity



Using any  
token or credential



In any  
environment



For any  
population

## And Enterprise Capabilities



Availability



Security

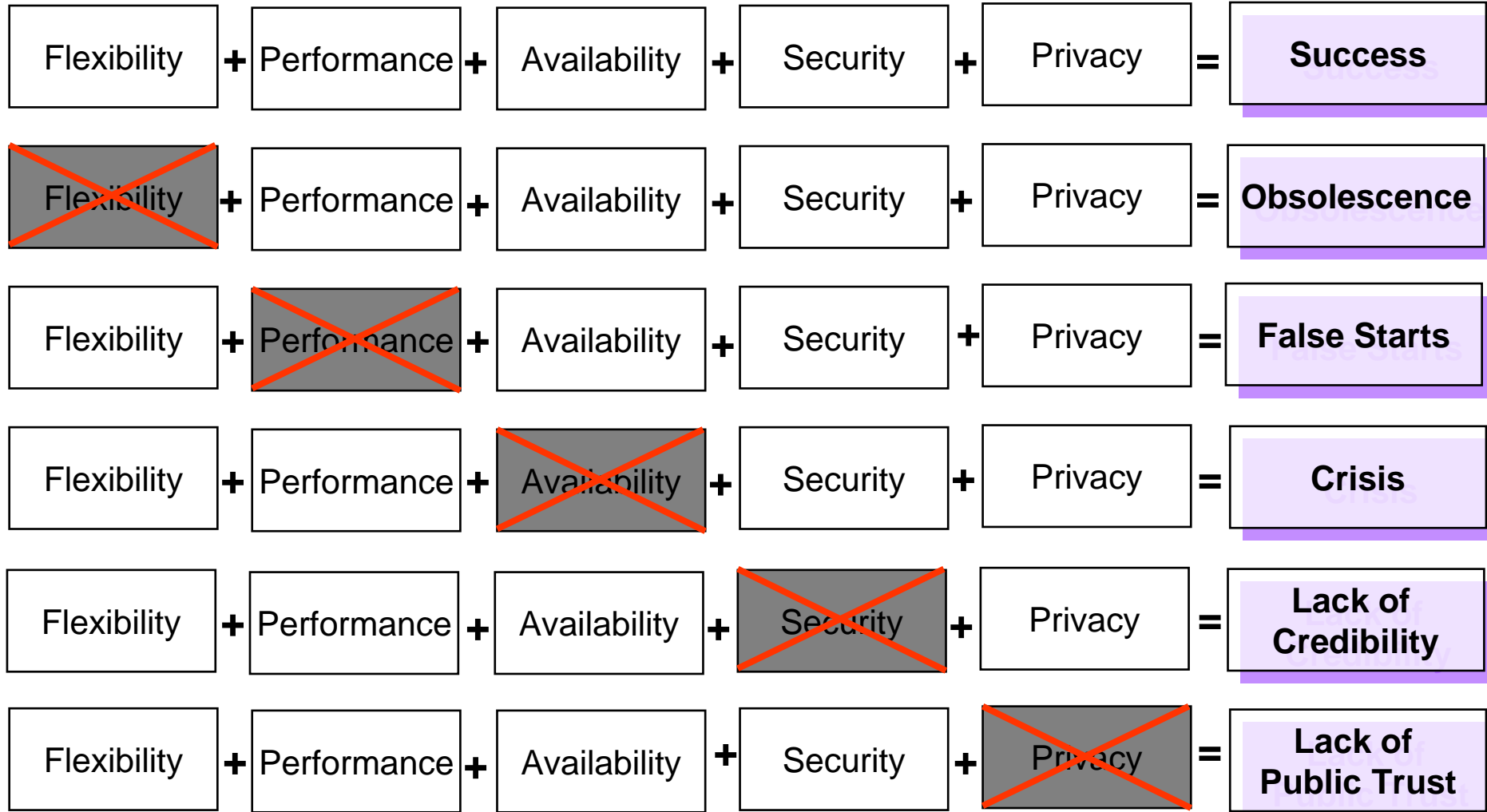


Privacy



Performance

# Formula For Success



**Thank You**

**Questions?**