22nd NISS Conference

Submission:	Tutorial
Topic:	BIOMETRICS - DEVELOPING THE ARCHITECTURE, API, ENCRYPTION AND SECURITY. INSTALLING & INTEGRATING BIOMETRIC SYSTEMS INTO YOUR EXISTING SYSTEMS
Keywords:	Biometric(s), security, encryption, API, computer
Author:	William H. Saito, President/CEO
Organization:	I/O Software, Inc. 1533 Spruce Street Riverside, CA 92507
Phone:	(909) 222-7600
Email:	william@iosoftware.com

ABSTRACT

DEVELOPING THE ARCHITECTURE, API, ENCRYPTION AND SECURITY
INSTALLING & INTEGRATING BIOMETRIC SYSTEMS INTO YOUR EXISTING SYSTEMS

As the technology behind biometrics become cheaper and more reliable, many companies have begun to integrate various biometrics into their existing security system. This workshop will explain how to implement and build biometric technology to augment current security systems while explaining specific issues that need to be addressed.

Designed to benefit both technical and non-technical professionals, this real world information will enable developers to develop biometric solutions without compromising the intended security enhancement.

Seamlessly developing biometrics to enhance your existing security

- Template storage and management issues
- Template encryption issues
- Security and integrity of biometric data from source to output
- Potential security threats and solutions to them
- Export restrictions regarding certain biometric implementations

Developing API's (Application Programming Interface)

- Current status of the biometric API's
- How to use and which is best for you?
- API's and implementing a secure system
- API's and non-PC platforms
- Exploring template compatibility

Developing a common methodology for software developers looking to integrate biometrics into their applications

- End user education
- Making applications easier to use via biometrics
- Common UI (User Interface) issues regarding biometrics
- User enrollment problems and solutions
- Client/Server programming issues to consider
- Frequent error conditions and how to handle them
- Audit and event logs issues while addressing privacy

Biometrics

Installing and Integrating Biometric Systems into your Existing Systems

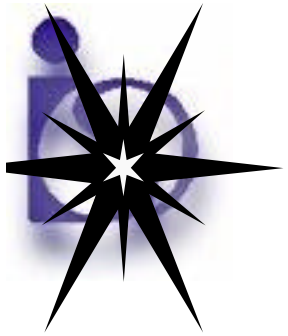
NISS Conference, October 18-21

William Saito

President/CEO

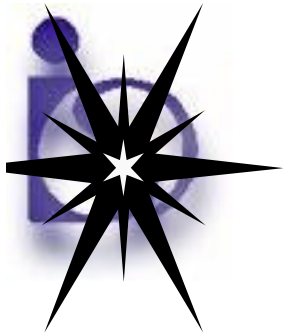
Company

- Founded in 1991
- Core Products & Technology
  - Device driver development & hardware integration
  - Commercial biometric application development
  - Biometric solution provider
- Original developer of BAPI
- BioAPI member
  - DWG (Device Working Group) Chair
- UAS Working Group member



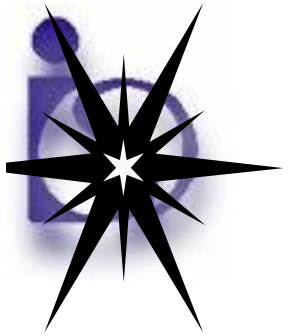
Biometrics 101

Choosing your biometric technology



Why is biometrics important?

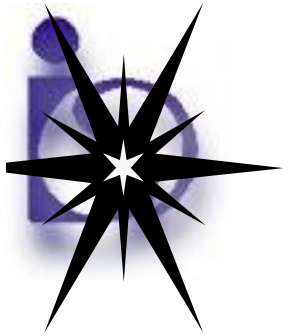
- What you know (i.e., password or PIN)
  - Insecure, can be forgotten, needs to be changed, can easily be copied or given to others
- What you have (i.e., ID card or key)
  - Can be lost or copied (without your knowledge), replacement costs are high
- What you are (i.e., fingerprints)
  - Only non-reputable authentication method. Conclusively proves you are who you say you are



Types of biometrics

- Fingerprint/Finger length
- Hand geometry
- Iris/Retina
- Facial image/Facial thermograms

- Voice
- Signature
- Keystroke

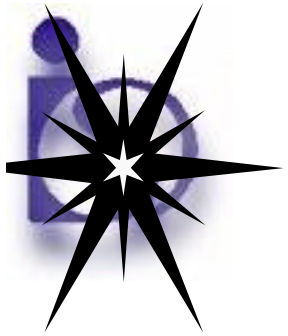


Types of biometrics

- Physiological vs. behavioral characteristics
  - Physiological: Don’t change over time

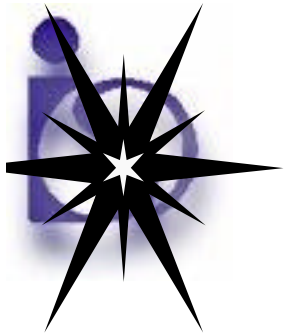
    (Fingerprint, hand, iris, etc..)
  - Behavior: Change over time

    (Voice, signature)
- Interactive vs. Passive biometrics
  - Passive: Facial



Trade offs

- Cost
- Security
- Size
- Convenience
- Speed
- Accuracy
- Connectivity & compatibility (ports/OS/CPU)
- *Intrusiveness*



Selecting criteria

- Level of accuracy (A)
- Ease of use (B)
- Barrier to attack (C)
- Public acceptability (D)
- Long-term stability (E)
- Cost (F)
- Size (G)

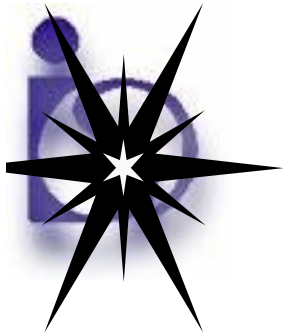
Biometrics technologies

(Comparison)

• Finger	A8	B8	C8	D7	E8	*F5*	*G5*
• Signature	A4	B9	C4	D9	E4	*F3*	*G3*
• Hand	A7	B7	C7	D7	E4	*F7*	*G7*
• Iris /Retina	A9	B3	C8	D4	E7	*F9*	*G9*
• Facial	A4	B5	C4	D8	E4	*F4*	*G8*
• Voice	A7	B8	C4	D8	E5	*F2*	*G2*

(0=Very Low 5=Average 9=Very High)

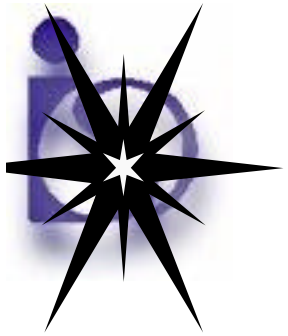
(Black = Higher value is better / *Red* = Lower value is better)



Biometric taxonomy

- Cooperative vs. Non-cooperative
- Overt vs. Covert
- Habituated vs. Non-habituated
- Supervised vs. Unsupervised
- Stable Environment vs. Unstable
- Optional vs. Mandatory

Biometrics do best in conditions of left column



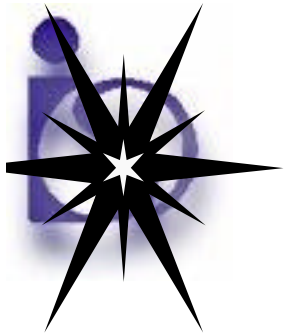
Types of applications

- Physical access
- Computer logon/logoff
- File encryption
- Client/Server
- Dumb terminals
- Internet / e-Commerce
- Smart cards
- PKI - Public Key Infrastructure

How biometric devices work

How biometrics work

- User enrollment
- Image capture
- Image processing
- Feature extraction
- Comparison
  - Verification
  - Identification



Templates

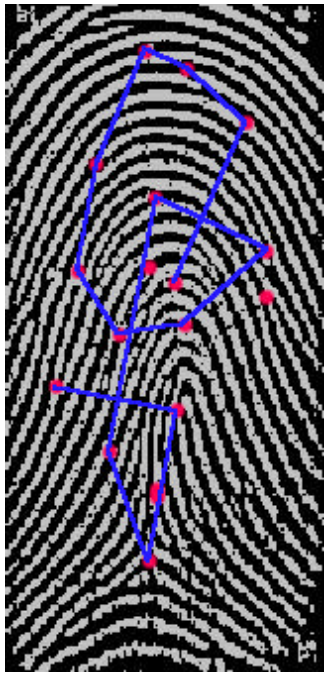
- Templates are usually not compatible between vendors
- Template size/type varies
  - 50 - 8000+ bytes
  - Speed vs. accuracy vs. size
- Template types include:
  - Vectors
  - Minutiae

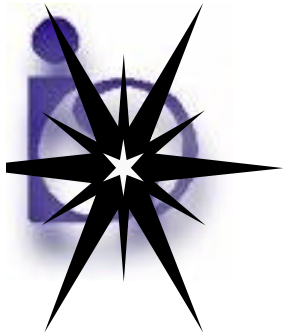
Image conversion

"Raw" Data

Processed Data

Template Data

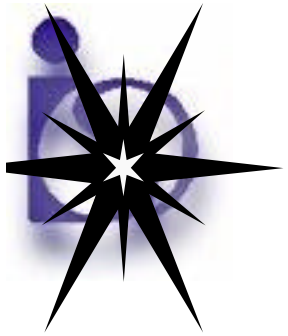




Comparison methods

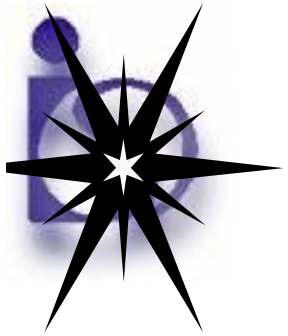
- Verification
  - 1:1 matching
  - To verify that the person is who he says he is
- Identification
  - 1:n search
  - To find a person out of many in a database

Evolution of devices



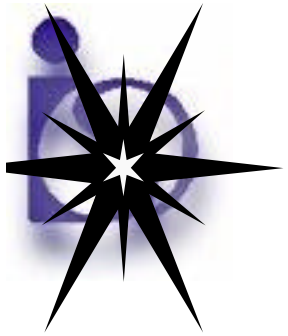
Fingerprint devices : Three Generations

- First Generation
  - Supervised
  - Slow
  - Bulky devices / heavy!
  - Required calibration
  - Not PC based
  - Very expensive! (>$5K)
  - Application: Criminal Enforcement



Fingerprint devices : Three Generations

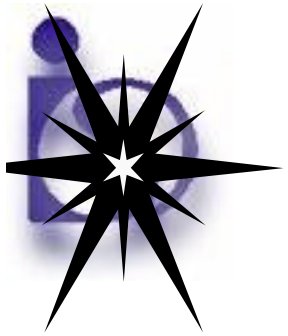
- Second Generation
  - Optical only devices
  - High FRR and/or FAR
  - Required some finger preparation
  - Somewhat PC friendly development environment
  - Expensive (>$1K)
  - Applications:
    - Building access control
    - High security computing in vertical applications



Fingerprint devices : Three Generations

- Third Generation
  - Non optical based sensor
  - First mass produced devices
  - Fast, self-calibrating, encryption support, dead/fake finger detection
  - SDK’s available for PC’s
  - Inexpensive (<$300)
  - Applications:
    - General Purpose Computing
      - Windows NT/95, UNIX

Types of devices



Device interfaces

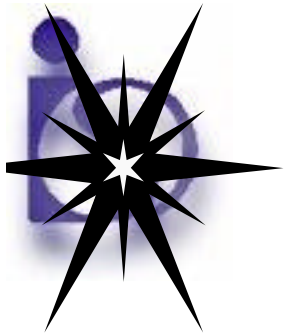
- Various port types (and issues)
  - Composite video signal
  - Parallel port (Pass through & ECP/EPP modes)
  - Serial port (RS-232, RS-422, RS-485, etc..)
  - USB port (NT support)
  - PCMCIA port
  - Weigand
- Transfer time / ease of integration
- Encryption

Image capture component

- Resolution
  - 350 - 500+ dpi
- Sensor types & materials
  - Optical
  - Capacitance
  - Resistance
  - Thermal
  - Polymer

Sensor comparisons

- Optical
  - Most bulky
  - Distortion issues
  - Dry finger problems
- Capacitance
  - ESD issues
  - Surface strength issues
  - Surface area limitations
- Thermal
  - Lowest surface area required

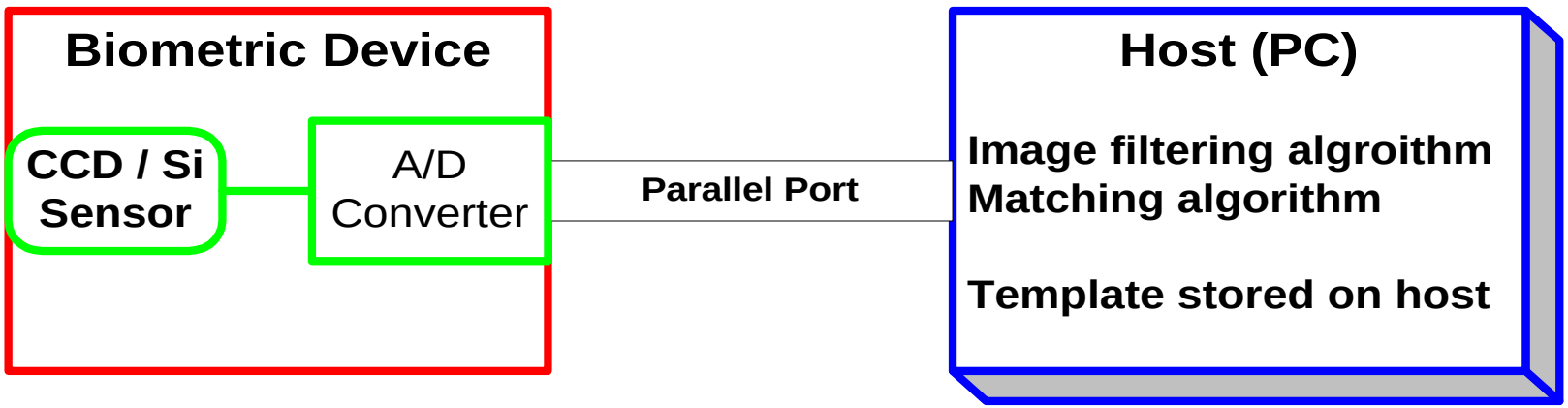


Device sophistication

- Simple
  - Scanner (only)
  - Scanner with encryption
- Processing (self-contained)
  - Scanner with CPU and/or LSI for fingerprint processing
  - Scanner with CPU and memory for storage of fingerprint (optional encryption)
- Complex
  - Scanner + CPU + protected storage for PKI type use

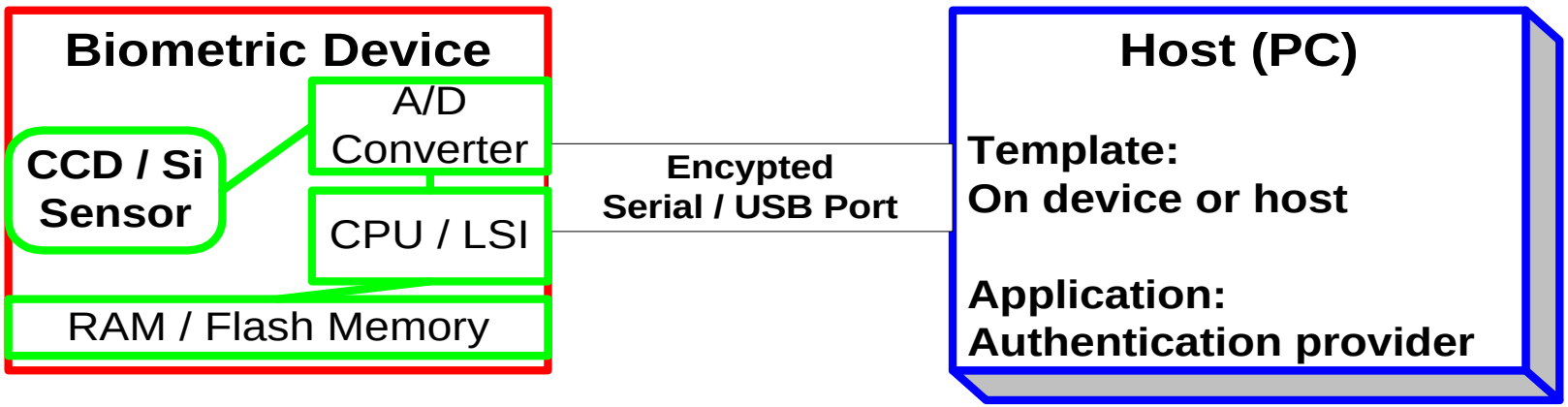
Simple biometric devices

- Simple design / low-cost device
- No security
- All processing done on host PC
- Ideal for simple low security applications



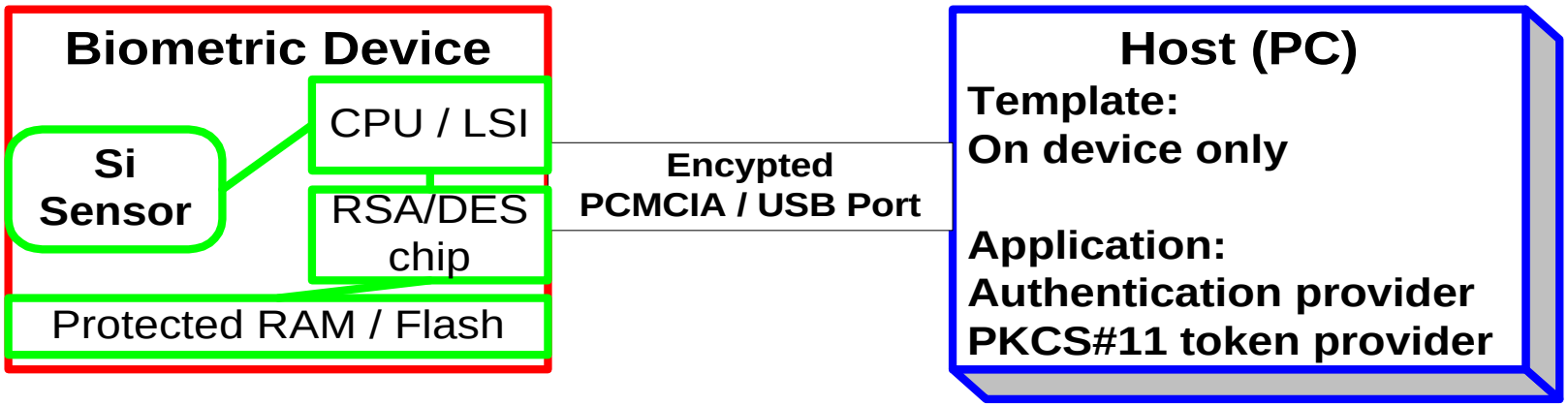
Self-contained devices

- Device contains a lot of intelligence
- Communications encrypted to host
- Some or all processing done in device
- Ideal for physical access, smart cards and terminals



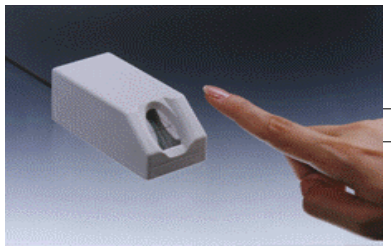
Complex devices

- Devices are small and portable
- Templates and private keys (PKI) never leave device (storage is protected)
- Tamperproof (FIPS 140-1)
- Ideal for PKI (PKCS#11 - cryptoki) applications



Application suitability

Client/Server



Fingerprint Reader

1. Finger scanned

2. Image converted A/D

Raw image

Client PC

3. Image processing algorithm

4. Template generation

Client PC

Template

Server

5. Template matched with enrolled image

6. If template matches, access is granted

Server

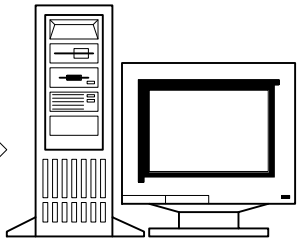
Smart card

Smart card with fingerprint template

Card

Card Terminal

Card Info.



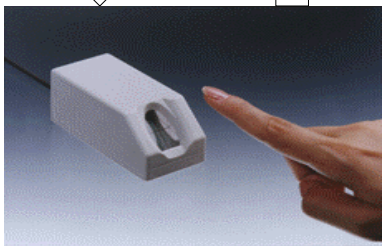
Data Center

Terminal

1. Card is inserted
2. Template is read from card
3. Template(PIN) sent to fingerprint reader

Template

Matches



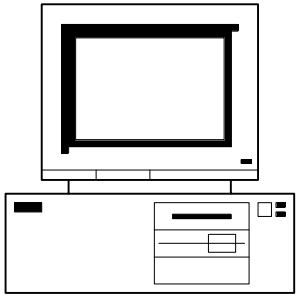
Fingerprint Reader

4. Finger scanned
5. Finger checked with uploaded template
6. Sends PIN back to terminal

Server

7. Card data updated
8. Updated information sent to data center
9. Transaction complete

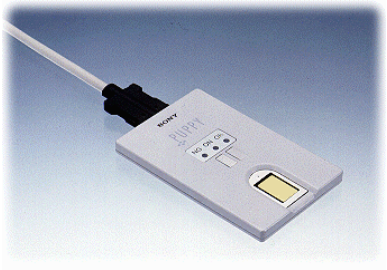
PKI



Workstation

Requests Authentication

Requests Cryptographic Services

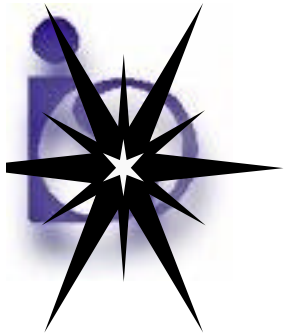


PKI based fingerprint device

Workstation	**PKCS#11 Module**	**Fingerprint Reader**
Certificate based web site requests certificate - or - E-mail application requests private key	1. User authentication requested 4. Cryptographic services requested -or- certificate requested	2. Finger scanned 3. Authentication token returned to workstation 5. Cryptographic provided to data -or- certificate returned

Other device features

- Keypads & LED’s
- “Live finger” sensor
- Smart card integration
- Ergonomics
- Size
- Water resistance



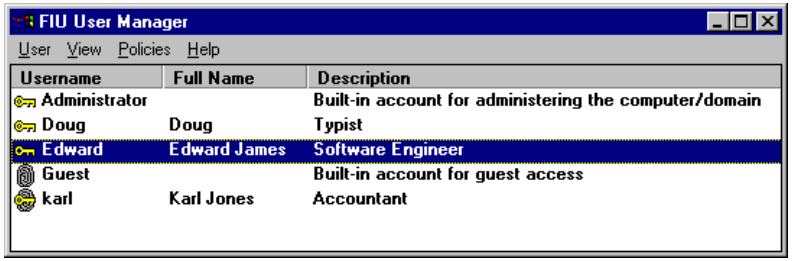
Other issues

- FCC, CE, UL certification
- Microsoft WHCL compatibility
- NS1 export approval
- CC1 export approval
- Federal Information Processing Standard
  - FIPS 140-1
- AFIS compatibility

Biometric applications

Biometric applications

- SecureSuite
  - Biometrically authenticated Windows 95/98/NT Logon
  - Screen saver unlocking
  - Password provider
  - Hard disk encryption
  - PKI, etc...



- Smart card (VeriFone)
  - Biometrically locking smart card contents
- Web / Internet Commerce (SecureWeb)

SecureSuite

- SecureStart - Secure logon system for Windows 95/98/NT
- SecureFolder - Windows file / folder encryption application
- SecureSession - Windows password bank / provider
- SecureEntrust - PKI based authentication and encryption provider for Entrust
- SecureApp - Windows based application execution control

- SecureWeb - Customizable web server access control solution

I/O Software, Inc.

Provider of innovative software solutions

1533 Spruce St.
Riverside, CA 92507
(909) 222-7600
(909) 222-7601 FAX
Web: www.iosoftware.com
E-Mail: William@iosoftware.com