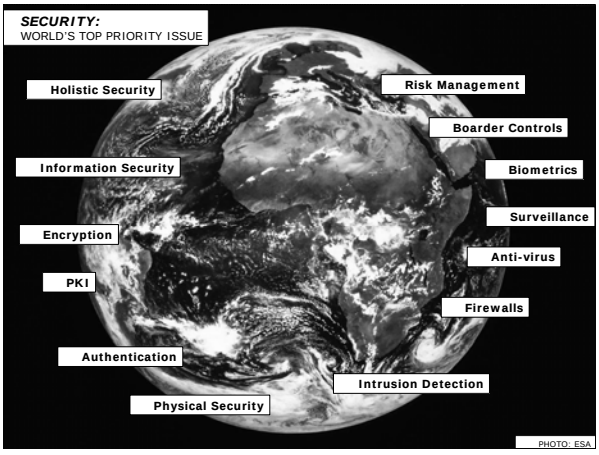
Security and Biometrics

Babak Goudarzi Pour, CEO
Optimum Biometric Labs, OBL

Agenda

- *Part I,*
  Security from a "holistic concept" viewpoint
- *Part II,*
  Methods for personal identification/verification,
  emphasis on **Biometrics**



Can we define "Security"?

part I

- Definition of security is totally application dependent
- Real security is about achieving a balance (Holistic security)
- Historically: protection of physical assets from the bad guys, Physical security
- Generally: security deals with:
  - ✓ Prevention, (*e.g.* locks on doors)
  - ✓ Detection, (*e.g.* imposter alarm)
  - ✓ Response, (*e.g.* SOS alarm)

- Yesterday, we had:
  - Computer security, Network security, etc
- Today, things are much more complex, hence we call it
  - Information security

The goals of information security

part I

Information security is a process with no single clear-cut definition!

No solution has 100% security, because there is no such a thing as 100% security in real life either

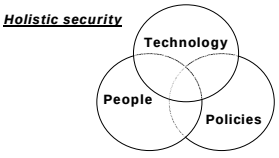
The CIA of information security (Gollman)

- **Confidentiality**: Prevention of unauthorized disclosure of information
- **Integrity**: Prevention of unauthorized modification of information
- **Availability**: Prevention of unauthorized withholding of information or resources

What is the "Holistic security" concept?

part I

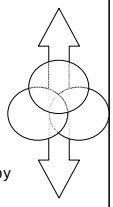
- Security need to be considered beyond the technical aspects: Social, political, cultural, and legal impacts on security requirements need to be considered as well.



Components of the "Holistic security"

part I

- Technology:
  All high-tech systems that you use in order to secure a facility or an information
- Procedures:
  Set of rules that you develop to ensure the technology is used appropriately
- People:
  All the employees/customers/partners who are impacted by the technology and procedures



The optimum security solution is achieved when you find an operational interplay between these three components

Ok, but…where should you begin?

part I

- Risk Analysis (RA)
  - ✓ Define what to protect and why
  - ✓ Explain in terms of utility, cost saving, numbers, money

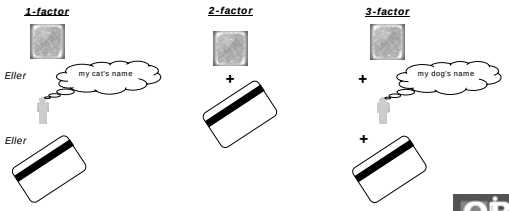
  Remember:
  1. Security in itself is nothing but a set of measures, controls and safeguards that must support and enable your company's business, mission, and objectives
  2. With an effective Risk Analysis, only those controls and safeguards that are actually needed will be implemented
- Protection
  - ✓ Choosing, implementing, maintaining, and evaluating the best possible means (holistic security) of protection

Personal authentication principles

part II

- *What You Know: p*assword, PIN-codes
- *What You Have:* tokens and cards
- *What You Are:* biometrics

- *Multi-factor authentication,* (Security versus Convenience)



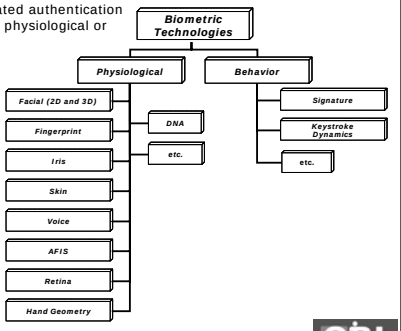
What are Biometrics?

part II

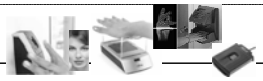
- Biometrics are automated authentication technologies based on physiological or behavioral attributes of an Individual

Most used today: Hand geometry- and Fingerprint scanning

On the way: Iris and facial recognition

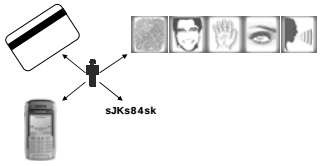


Benefits with Biometrics



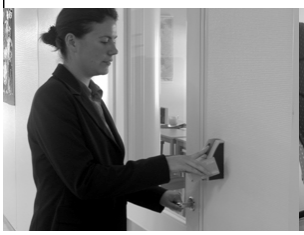
- Password, magnet stripe, token are subjected to
  - Malfunction
  - Be forgotten
  - Borrowed to someone
  - Get stolen

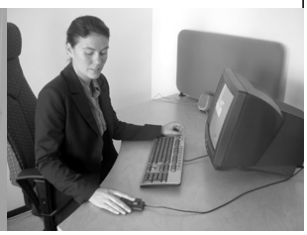
With Biometrics You Increase:
- ✓ Security
- ✓ Comfort
- ✓ Efficiency



Applications

- Physical access control
- Computer & network log-on
- Time & Attendance
- Business transaction
- Biometric passports
- National ID-cards
- Surveillance
- Entertainment
- Profile adjustment (car, home HiFi-system, etc.)
- many more ...!

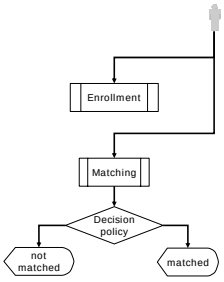




General Biometric Procedure

part II

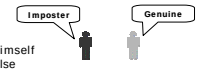
- *Enrollment:*
  - Creation of a template when a biometric feature is presented to a biometric system
- *Matching:*
  - Comparing a "live" biometric sample to a stored template
- *Decision Policy:*
  - ✓ Threshold level dependent
  - ✓ One-strike
  - ✓ Multi-strike



Classification of Biometric Applications 1(3)

part II

- *Types of Identity Claims:*
  - Genuine / Imposter
    - ✓ Genuine: User Truthfully Claim To Be Herself/Himself
    - ✓ Imposter: User Falsely Claim To Be Someone Else



- *Classification of Biometric Applications:*
  - Overt / Covert:
    - ✓ If the individual is aware/unaware of being biometrically measured
  - Assisted / Non-Assisted:
    - ✓ If the user is/is not observed and/or guided during the biometric measurement
  - Habituated / Non-Habituated:
    - ✓ Habituated: If the user has presented his/her biometric feature to the application on daily basis
    - ✓ Non-habituated: If the user has not ever or recently presented his/her biometric feature to the application

Classification of Biometric Applications 2(3)

part II

- Open / Closed
  - An open system requires interoperability with other system managements in terms of data format, compression and other format standards

- Positive/Negative:
  - ✓ Positive: You Are Who You Claim You Are
  - ✓ Negative: You Are Not Who You Claim You Are Not

- Cooperative / Non-Cooperative:
  - ✓ In a typical access control application when the identity claim is positive verification the user is cooperative
  - ✓ In a application verifying a negative identity claim the user is usually not cooperative

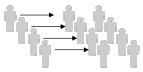
Classification of Biometric Applications 3(3)

part II

- Verification (1:1)
  - ✓ To assess the probable truth of the claim to an identity made by a previously enrolled user in a system

- Identification (1:Many or 1:Few)
  - ✓ To probabilistically link an individual to a list of enrolled individuals

- Recognition (N:M)
  - ✓ A surveillance application where one or several individual are searched through a list of enrolled individual
    Typical example: Las Vegas Casinos



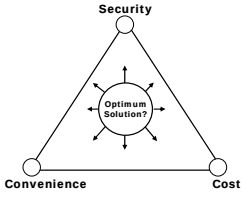
What is the Best Biometric? ...

part II

❖ *How do You define the Best biometric?*

- ✓ Best capable of enrolling the users?
- ✓ Best capable of rejecting imposter attempts or accepting genuine attempts or both (EER)?
- ✓ Most spoof-proof?
- ✓ Least expensive to deploy?
- ✓ Most privacy-protective?
- ✓ Easiest to use?
- ✓ Best for a certain demographic?
- ✓ etc…

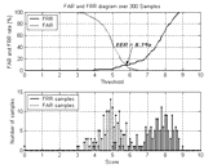
❖ *The question is:*
What is the Requirements of Your Specific Application?



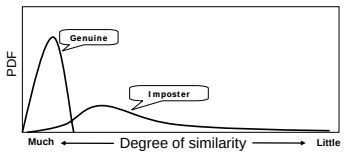
How secure are biometrics?

part II

- *Decision error rates:*
  - False Accept Rate (FAR)
  - False Reject Rate (FRR)
- *Biometric acquisition error rates:*
  - Failure-to-Enroll (FTE)
  - Failure-to-Acquire (FTA)



Example: facial recognition



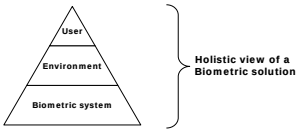
Performance Evaluation

part II

- *Types of Evaluations*
  - *Technology:*
    - ✓ Technology
    - ✓ Scenario
    - ✓ Operational
  - Vulnerability Assessment
  - Business Cases
    - ✓ Cost
    - ✓ Saving
- *Test Centers*
  - ✓ British Biometric Working Group
  - ✓ FRVT
  - ✓ FVC
  - ✓ International Biometric Group (IBG)
  - ✓ Optimum Biometric Labs (OBL)

Which factors are against a biometric security employment?

part II



Holistic view of a Biometric solution

- Environmental factors:
  - Bad light condition / noisy / cold or humid / etc.
- User:
  - Biometric unable, Non-habituated, Non-cooperative, etc.
- Biometric system:
  - Not technically performing, Vulnerable, etc.

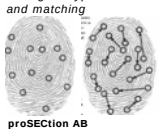
Different approaches on handling sensitive biometrics *part II*

Match-on-Server (Match-on-PC)
Template storage and matching process are on a PC

Match-on-Card
Template storage and matching process are on a smart card

Precise Biometrics AB,
Precise Match-on-Card™

Strong encryption at enrollment and matching



proSECtion AB

PKI and biometrics, Template need not to be stored

GenKey

A Case Study: "Stockholm School System" *part II*

- Number of students: Approx. 6000
- Application: Network access

- Before
  - Students forgot their passwords
  - Extensive administration costs
  - Passwords were written on the whiteboards
  - Elder students borrowed passwords from younger students
- ....After Biometrics were put in place
  - ✓ Lecture times were used more efficient
  - ✓ Less administration costs
  - ✓ Prevention of identity frauds

Optimum Biometric Labs

PRODUCTS
Unmanned & Proactive Performance Monitoring of Biometric Security Systems.

We turn Information into Knowledge allowing You to turn that Knowledge into Value.

MISSION
Remain in the forefront in biometric security industry by delivering unparallel innovation and services.

Clients, Affiliations, and Awards

CLIENTS

Government Agencies
- The Swedish Data Inspection Board

Biometric Industry
- Precise Biometrics

Entertainment Industry
- Kreativum

Academic institutions and schools
- Blekinge Institute of Technology

AFFILIATIONS
- ISO/IEC/JTC 1/SC 37 - Biometrics
- Swedish Standards Institute
- Swedish National Biometric Association
- Biometric Consortium

AWARDS (selected list)
- VINN NU (Swedish top-20 start-up)
- ALMI Innovation Prize
- Venture Cup
- Innovation Cup

Thank you for your attention!

Please don't hesitate to ask your questions

Optimum Biometric Labs AB
Org. Number: 55 66 58 – 0485
Campus Gräsvik 5, 371 75 Karlskrona, Sweden
URL: www.optimumbiometrics.com

E-mail: info@optimumbiometrics.com
Phone: +46 (0)8 5000 7206
CEO-phone: +46(0)707404
Fax: +46(0)455 304 223