Security of Biometric Authentication Systems

Vashek Matyas, joint work with Zdenek Riha

Faculty of Informatics, Masaryk University Brno

{matyas, zriha} at fi.muni.cz

Authentication at the time of war

- And the Gileadites took the passages of Jordan before the Ephraimites: and it was so, that when those Ephraimites which were escaped said, Let me go over; that the men of Gilead said unto him, Art thou an Ephraimite? If he said, Nay; Then said they unto him, Say now Shibboleth: and he said Sibboleth: for he could not frame to pronounce it right. Then they took him, and slew him at the passages of Jordan: and there fell at that time of the Ephraimites forty and two thousand. (Judges 12:5-6)

- Identify-Friend-or-Foe more critical than ever before
  - Systems watch and shoot at distances where visual target identification is impossible
  - Rise of "friendly fire" casualties from historical 10-15% to 25% in the First Gulf War (R Anderson, Security Engineering)

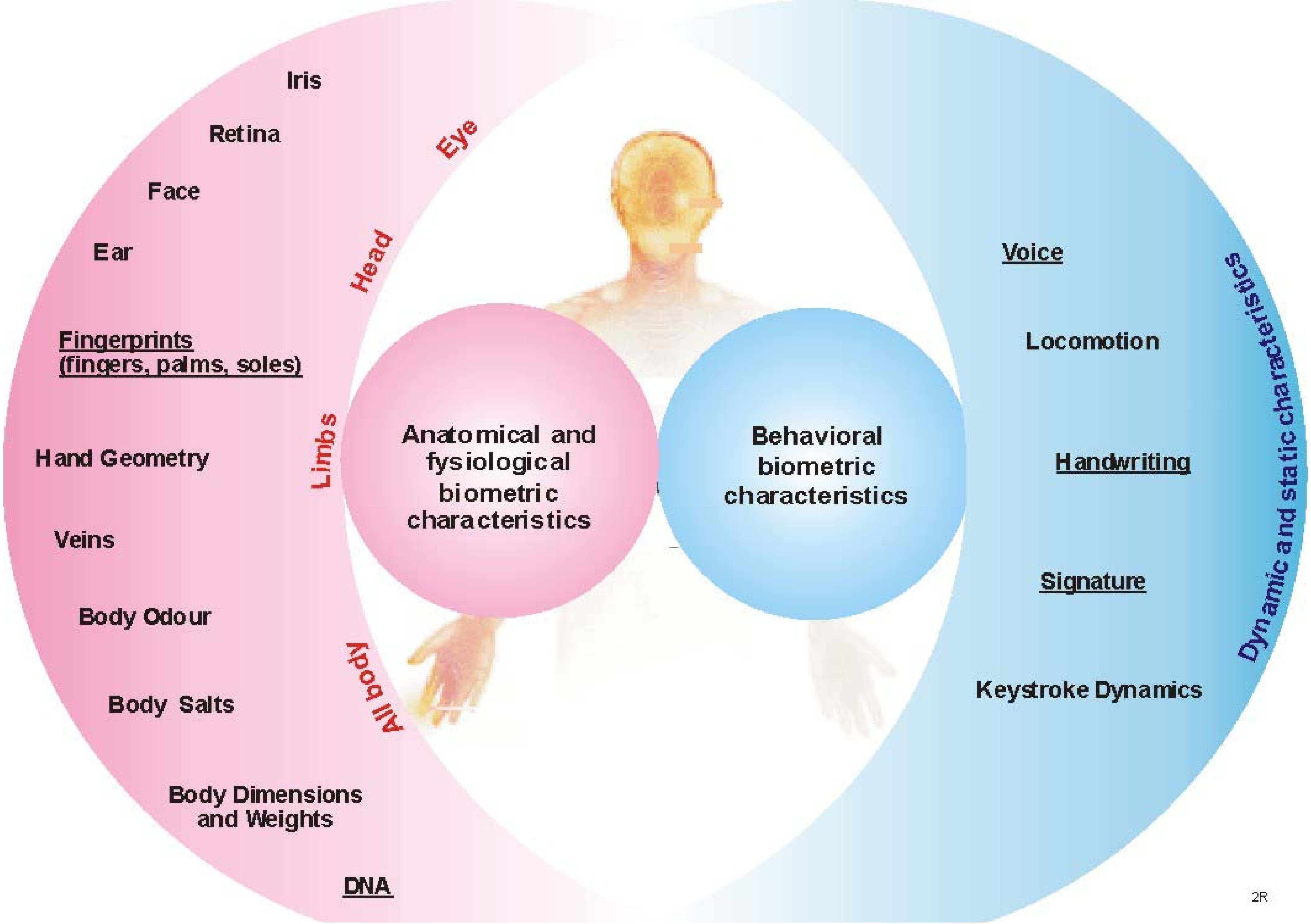
Means of authentication	Access to a service
• something you know (password, PIN)	• Access by a person (process) that knows a secret.
• something you have (key, smartcard)	• Access by a person possessing a “key”.
• something you are - biometrics	• Access by a person with this characteristic.
• *or combination of the above*	

Biometric techniques

- Biometrics – biological characteristics measurable by automated methods

- Physiological characteristics (hand, eye, face, etc.)
- Behavioral characteristics (signature dynamics, voice, etc.)

Biometric techniques



Iris
Retina
Face
Ear
Fingerprints (fingers, palms, soles)
Hand Geometry
Veins
Body Odour
Body Salts
Body Dimensions and Weights
DNA
Eye
Head
Limbs
All body
Anatomical and fysiological biometric characteristics
Behavioral biometric characteristics
Voice
Locomotion
Handwriting
Signature
Keystroke Dynamics
Dynamic and static characteristics
2R

Biometrics – authentication

- Biometrics almost never match at 100%!!!
- Threshold-based decision introduces the rates of false acceptance and rejection
  - Zero-effort or active bypassing?
- User group size vs. accuracy
  - Verification vs. identification?

Verification steps

1) First measurement/acquisition(s)
2) Creation of master characteristics
3) Storage of master in a database
4) *Subsequent acquisition(s)*
5) Creation of new characteristics
6) Comparison: new - master
7) Threshold-based decision

DNA as a biometric?

# of samples	Random match probability	Time (minutes)
1	10^{-18}, 16 markers	345
10	10^{-18}, 16 markers	450
90 semi-autom.	10^{-18}, 16 markers	830
90 fully autom.	10^{-18}, 16 markers	190
1 fully autom.	10^{-10}, 8 markers	93

Serial marker analysis (soon)

1st marker	60 minutes	10^{-2}
2nd marker	60 minutes	10^{-3}
3rd marker …	60 minutes	10^{-5}

Multiplexing (in few years)

3 markers	60 minutes	10^{-5}
next 3…	60 minutes	10^{-7}
next 3…	60 minutes	10^{-10}

Real-world use of biometrics

- UK Passport Service: Biometrics Enrolment trial 2005, success of registration & verification (registration)
  - Face
    - General population: 69% (99.85%)
    - Disabled: 47% (97.7%)
  - Iris
    - General population: 85.8% (87.7%)
    - Disabled: 55.6% (61%)
  - Fingerprint (10-print)
    - General population: 80.8% (99.3%)
    - Disabled: 77.4% (96.1%)
- US-VISIT program (2 index fingers) with 6,000,000 “not-wanted” entries in 2004 had official 0.31% false match rate and 4% missed match rate

Advantages of biometrics

- Actually authenticate the user
  - Provided they work correctly
- Not transferable
  - Yet characteristics can be copied/stolen
- Easy to use and usually fast
- Some allow for continuous authentication

Practical problems I.

- Trustworthy input device (liveness)
  - Is this from a living person?
  - Is this from the person presenting it?
- Performance – security vs. usability & cost
- Users with damaged, missing or “not usable” organs – Fail To Enroll (FTE) rate

Practical problems II.

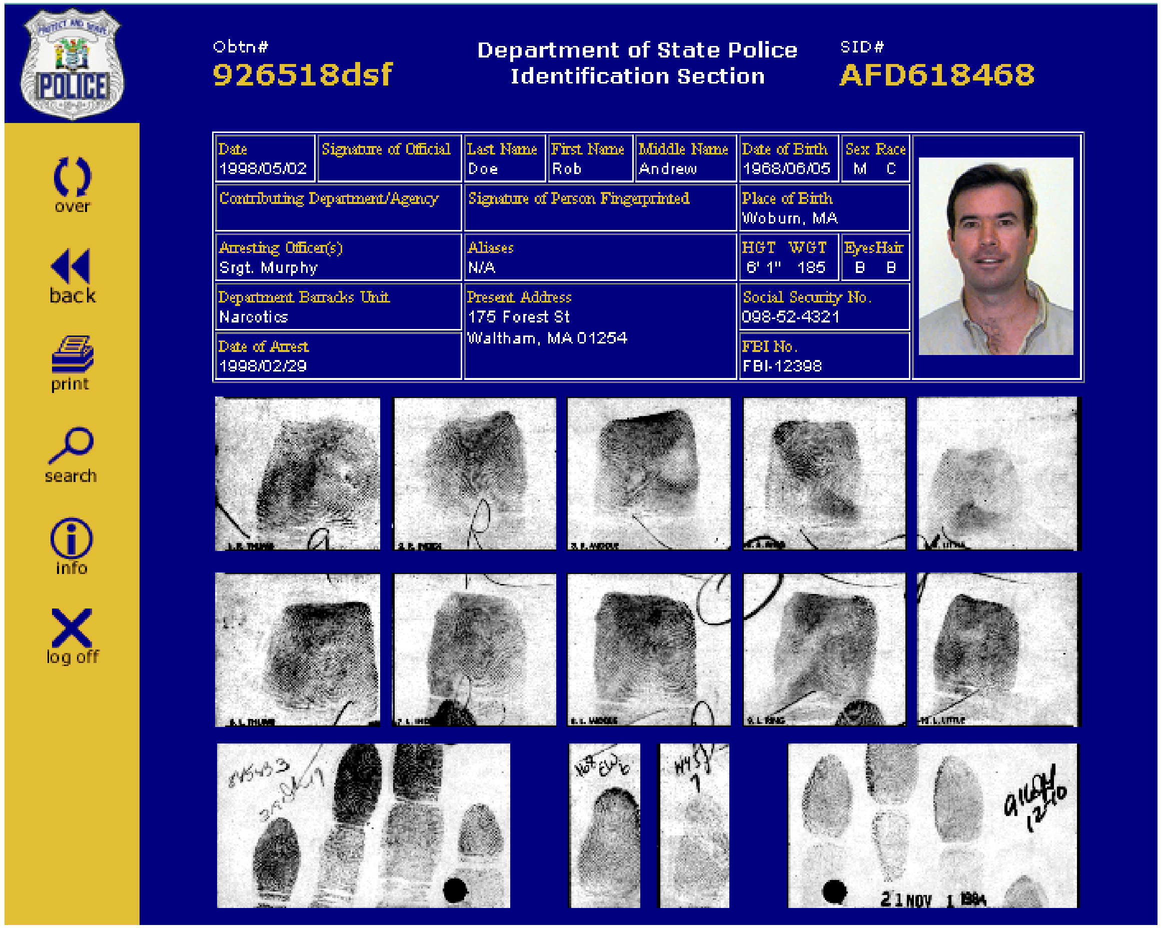
- Inflexibility of characteristics
  - one characteristic can be used in more systems!
  - compromising should not be critical to security
- Privacy and user acceptance issues
- Legislation and regulation

Commercial versus Forensic

- Automated assistance with human experts
- Higher accuracy

- Enrolment often cannot be repeated
- Characteristics usually with original samples

- Fully automated, computer peripherals
- Lower accuracy
- Enrolment can be repeated
- Typically only characteristics stored



Obtn#
926518dsf

Department of State Police
Identification Section

SID#
AFD618468

Date 1998/05/02	Signature of Official	Last Name Doe	First Name Rob	Middle Name Andrew	Date of Birth 1968/06/05	Sex Race M C
Contributing Department/Agency		Signature of Person Fingerprinted			Place of Birth Woburn, MA	
Arresting Officer(s) Srgt. Murphy		Aliases N/A			HGT WGT 6' 1" 185	EyesHair B B
Department Barracks Unit Narcotics		Present Address 175 Forest St Waltham, MA 01254			Social Security No. 098-52-4321	
Date of Arrest 1998/02/29					FBI No. FBI-12398	

Commercial versus Forensic II.

- Results in seconds
- Support needed at low-moderate level
- Size as small as possible
- Low cost, important factor

- Results even in days
- Expert maintenance and support required
- Size is relatively unimportant
- High cost, considerable but not important factor

Show me the magic…

- Biometrics are not secrets
  - Covert vs. overt acquisition
  - Many systems rely on secrecy of biometrics
- Many systems use the same biometrics
    - Yet have different security policies
    - Their owners are not aware of the extent
    - Does this resemble a password problem…???

Part of a bigger puzzle

- Not only the error rates and liveness check matter…
  - Storage and transfer of samples
  - Place of comparison

Biometrics – major lessons

- Same person never shows same results
- Biometric systems often terribly erroneous
- Biometrics are not secrets
- Input device is crucial (often physical protection)
- Liveness should be checked
- User authentication, not for machines or data
- New attack countermeasures => newer attacks

Key generation attempts

- User provides her/his biometric sample and her/his key can be generated from this sample
- Attractive benefits
  - Key re-generated “on the fly”
  - Key is used only with owner present
  - Can be used and then destroyed

Biometrics and key derivation

- Hash of a biometric measurement often suggested to be used – will not work as a simple password replacement
  - Such approaches useless – other ways to explore…
  - Biometric hash (representing characteristics "that are most likely" invariable) is effectively a sample creating algorithm
    - Worth investigating anyway (yet for different reasons)

Major problems

- Key-space
  - Limited by measurable characteristics
    - Entropy low for crypto keys
  - Probability of different values?
- Secret key protection
  - Biometrics are not secret
  - Can secret be added?
    - Where do we store that secret?
    - What are the chances of exhaustive search?

Minor problems

- Compromised key – key change?
- Organ damaged – key loss?
- Dependence on the reader

What can we generate?

- Key?
  - – Most probably not – open for future research
  - – Do we need random input?
    - This is the key then, more than anything else
- Non-trivial userID?

Key locking

- Biometrics applied to a random key
- "Locked" key leaks no data – neither about the key nor about biometric data
- Only the correct biometric data can "unlock" the key
- Key can be changed, yet biometric data compromise is still a problem

Digital signature & authentication

User — Computer — Data

Digital signature in theory

Secret Key + Document = Signature

Public Key + Signature + Document = Yes / No

Digital signature in real-life

- Public Key – critical for verification, use of certificates (PKI)

- Secret Key – must be kept secret otherwise others can create „your“ signatures

Protection of the secret key

- Stored on a computer, smartcard…
- Usually encrypted / locked
  - To use, one must provide a PIN/password and/or the smartcard
  - Is unencrypted during use – a Trojan horse or administrator can get hold of the secret key!!!

No reliable signature without a secret!

- Digital signature is based on limited access to the secret key

- It is not you (human), but the computer that signs!!!

Biometric signatures

- Biometrics are not secrets !!!

- Biometrics authenticate users, not computers nor messages...

The role of biometrics

- Biometrics can protect access to the secret key

- Signature chip + biometric sensor + biometric matching = … bright future?
  ☺ ☺ ☺

Conclusions

Iris

- Authentication/identification

  of the user
- Biometrics are not secrets
- Copying is neither trivial nor hard
- Biometric information can be very sensitive
- Assure *liveness*+ (often by a human guard) and take advantage of the accuracy & speed

Prospects for biometrics

- Device logon (standard workplace)
- Excellent additional authentication method
- Token/smartcard & PIN & biometrics
- AFIS & rough known-person search
- Consideration: user-friendliness & cost vs. security

Research ideas

- Text-prompted speaker (voice) recognition and challenge-response auth.
  - Enhancement with lip movement check
- Research into issues related to publicity of biometric data
- Challenge – liveness check with low FRR

Course reading – week 5

- *Security of Biometric Authentication Systems*, V. Matyáš, Z. Říha, International Journal of Computer Information Systems and Industrial Management Applications, Volume 3 (2011) pp. 174-184
- PDF in the IS

Term project presentations!!!

April 18:

Po přednášce...

- Konečný
- Mareček
- Hnízdil
- Tvrdý

May 2:

- Miklošovič
- Mokoš
- Sedlář
- Kompan
- Janáček
- Rodrigues
- Adam

May 9:

- Petruchová
- Prišťák
- Jurnečka
- Balážia
- Kretek
- Buda
- Iakym

May 16:

- Čermák
- Poul
- Chovanec
- Ošťádal
- Velan
- Víteček
- Güttner

Reminders: the presentation is worth (up to) 5 points from your course score; it should last at most 10 minutes (time for questions & discussion will be provided); laptop with AcroRead and PowerPoint will be available. ***Rehearse!!!!!***