GREYC
E-payment & Biometrics

Enhancing the Password Security with Keystroke Dynamics

Christophe Rosenberger
GREYC Research Lab - France

Passwords^12

OUTLINE

- GREYC - E-payment & Biometrics
- User authentication
- Keystroke dynamics
- Perspectives

GREYC Research Lab

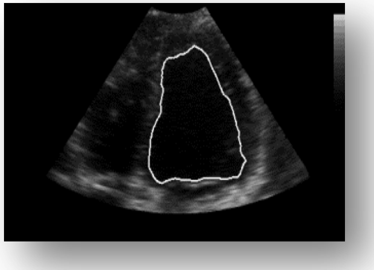
Research Group in Computer science, Automatics, Image processing and Electronics of Caen

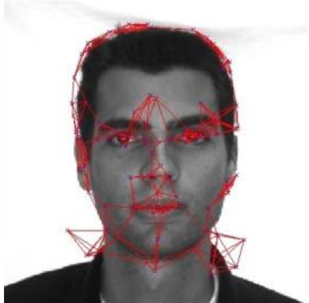
Laboratory staff:

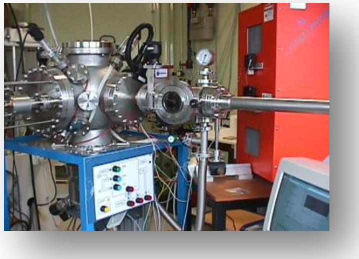
- 7 CNRS researchers
- 25 Full professors
- 18 Associate professors
- 48 Assistant professors
- 79 PhD students
- 17 permanent staff
- 30 Engineers and post-doc

Research topics:

- Electronics
- Image processing
- Algorithmic
- Document analysis
- Multi-agents
- Robotics navigation
- Automatics
- Computer security
- Natural language processing
- Biometrics
- Cryptography







E-payment & Biometrics

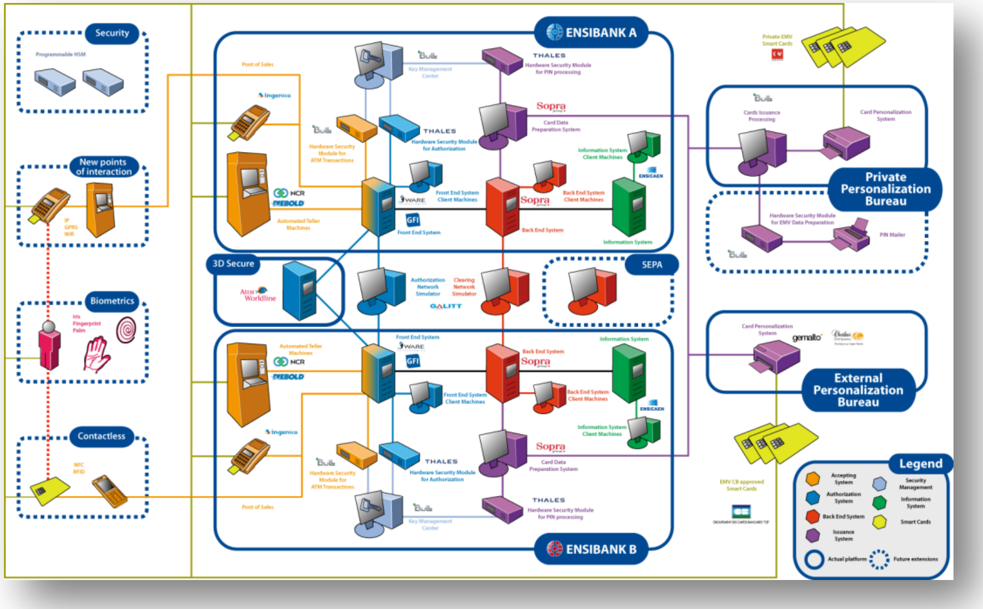
GREYC

Members (30):
3 full professors, 2 associate professors, 4 assistant professors, 4 permanent engineers, 8 PhD students, 1 Post-doc, 8 engineers.

Research topics (2): Biometrics and Trust

Application: E-payment

Research projects: ASAP(ANR), LYRICS(ANR), PAY2YOU(FUI), CAPI(FUI), ADS+(FUI), INOSSEM(GE), LUCIDMAN(EUREKA)


Security
Programmable HSM
New points of interaction
IP
GPRS
Wifi
Biometrics
Iris
Fingerprint
Palm
Contactless
NFC
RFID
ENSIBANK A
Pont of Sales
ingenico
Bull
Key Management Center
THALES
Hardware Security Module for PIN processing
Hardware Security Module for ATM Transactions
Hardware Security Module for Authorization
Sopra
Card Data Preparation System
Information System Client Machines
ENSICAEN
NCR
DIEBOLD
Automated Teller Machines
Front End System Client Machines
WARE
GFI
Front End System
Back End System Client Machines
Back End System
Information System
3D Secure
Atos Worldline
Authorization Network Simulator
Clearing Network Simulator
GALITT
SEPA
ENSIBANK B
Private EMV Smart Cards
Cards Issuance Processing
Card Personalization System
Private Personalization Bureau
Hardware Security Module for EMV Data Preparation
PIN Mailer
gemalto
External Personalization Bureau
EMV CB approved Smart Cards
Legend
Accepting System
Authorization System
Back End System
Issuance System
Security Management
Information System
Smart Cards
Actual platform
Future extensions

gemalto
security to be free

inside SECURE

Bull

SFR

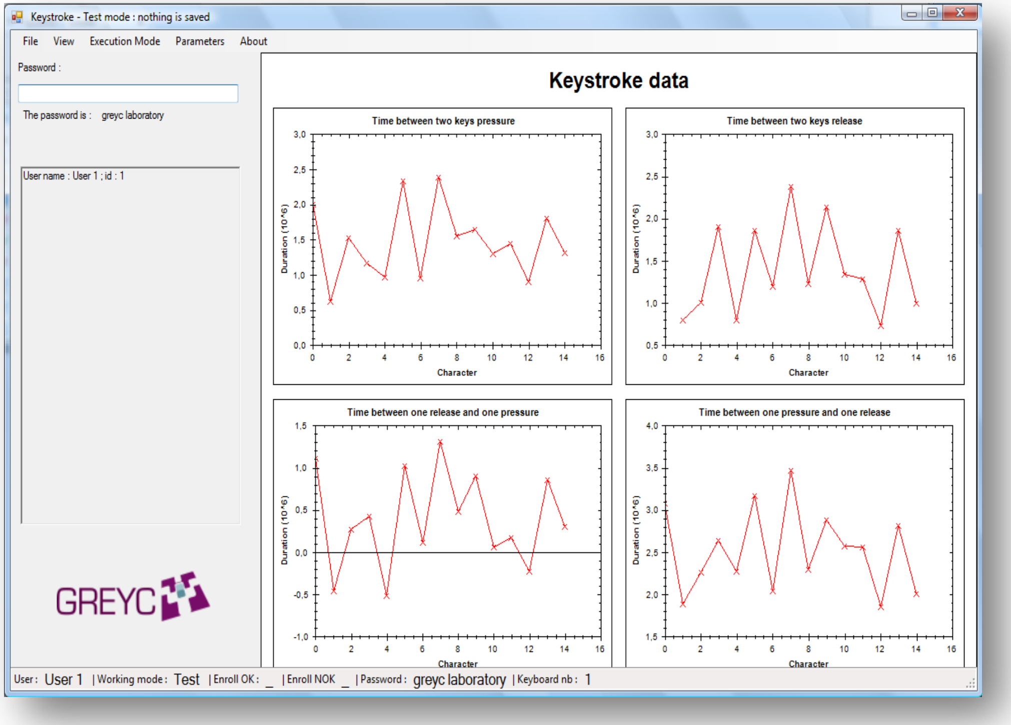
orange™

natural security

E-payment & Biometrics

Biometrics: Operational authentication that respects the privacy of users

- ❑ Biometric authentication (keystroke dynamics, fingerprint…)
- ❑ Evaluation of biometric systems (performance, usability, security..)
- ❑ Protection of biometrics (cancellable biometrics, smartcards…)


Keystroke - Test mode : nothing is saved

Password :

The password is : greyc laboratory

User name : User 1 ; id : 1

User : User 1 | Working mode : Test | Enroll OK : _ | Enroll NOK _ | Password : greyc laboratory | Keyboard nb : 1

File
View
Execution Mode
Parameters
About
Keystroke data
Time between two keys pressure
Time between two keys release
Time between one release and one pressure
Time between one pressure and one release
Duration (10^6)
Character
3,0
2,5
2,0
1,5
1,0
0,5
0,0
-0,5
-1,0
4,0
3,5
0
2
4
6
8
10
12
14
16
GREYC

GREYC Keystroke
Keystroke dynamics authentication

pôle TES
e-secure transactions

User authentication

User authentication:

Authentication methods are based on:

- We know [Secret]
- We own [Token, smartcard, RFID tag]
- We Are [Biometrics]
- The way we do things [Behavioral biometrics]

They are called authentication factors.

User authentication

Why passwords are (nearly) always used?

Choice made by the service provider (SP)

- ❑ Very convenient for the SP (very easy to verify)
- ❑ No need of a complex infrastructure (like OTPs)
- ❑ Nothing cheaper than a password (especially if it is stored in clear text)

Consequences

- ❑ Usability lacks: ask the user to use a “complex” password to “enhance the security of user authentication”
- ❑ Privacy issues are only considered for the specific SP

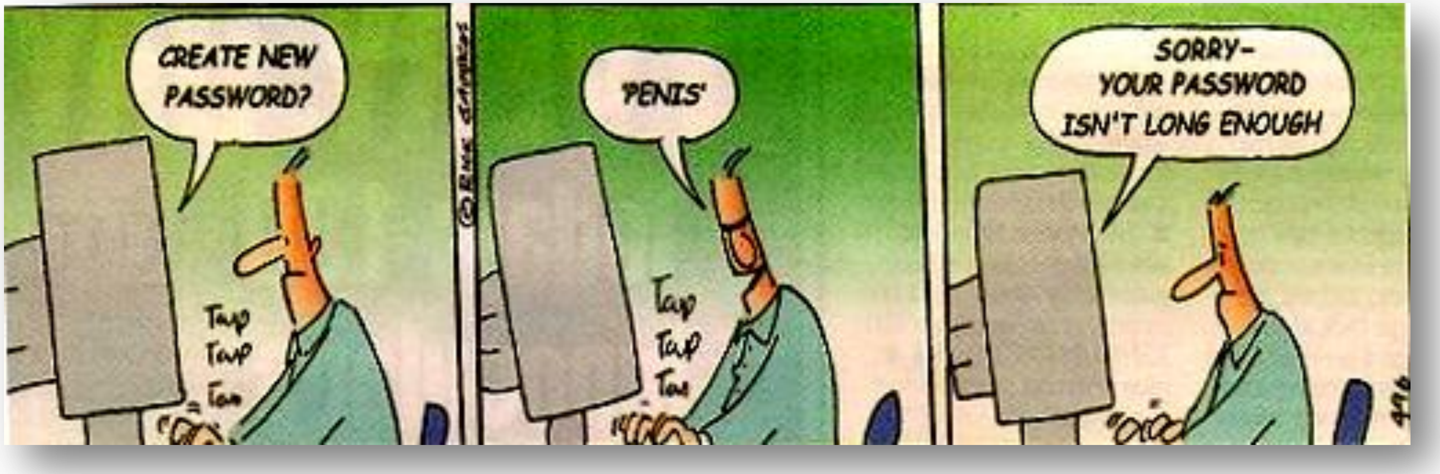
User authentication

Best practices for user authentication with passwords

User authentication

Why a static password is not a satisfying solution?

- Not very convenient for users having different services
- Bypass strategies permit attacks but also privacy intrusion
- No real relationship between an user and its password



User authentication

Biometrics is the ONLY one user authentication method

- ❑ Password based solutions realize a risk management on user's identity
- ❑ Biometrics guarantees the strongest link between the user and its authenticator

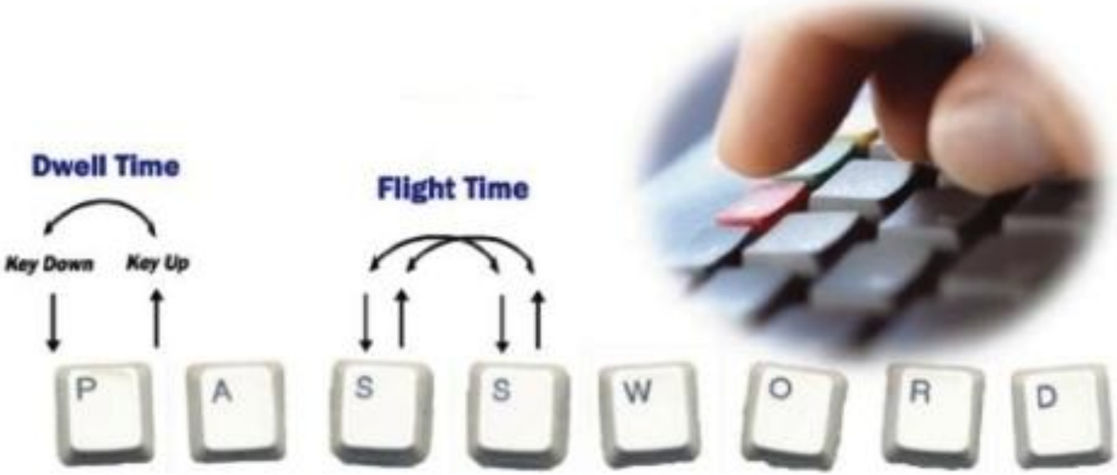
➡ Keystroke dynamics can be a good (operational) solution

Keystroke dynamics

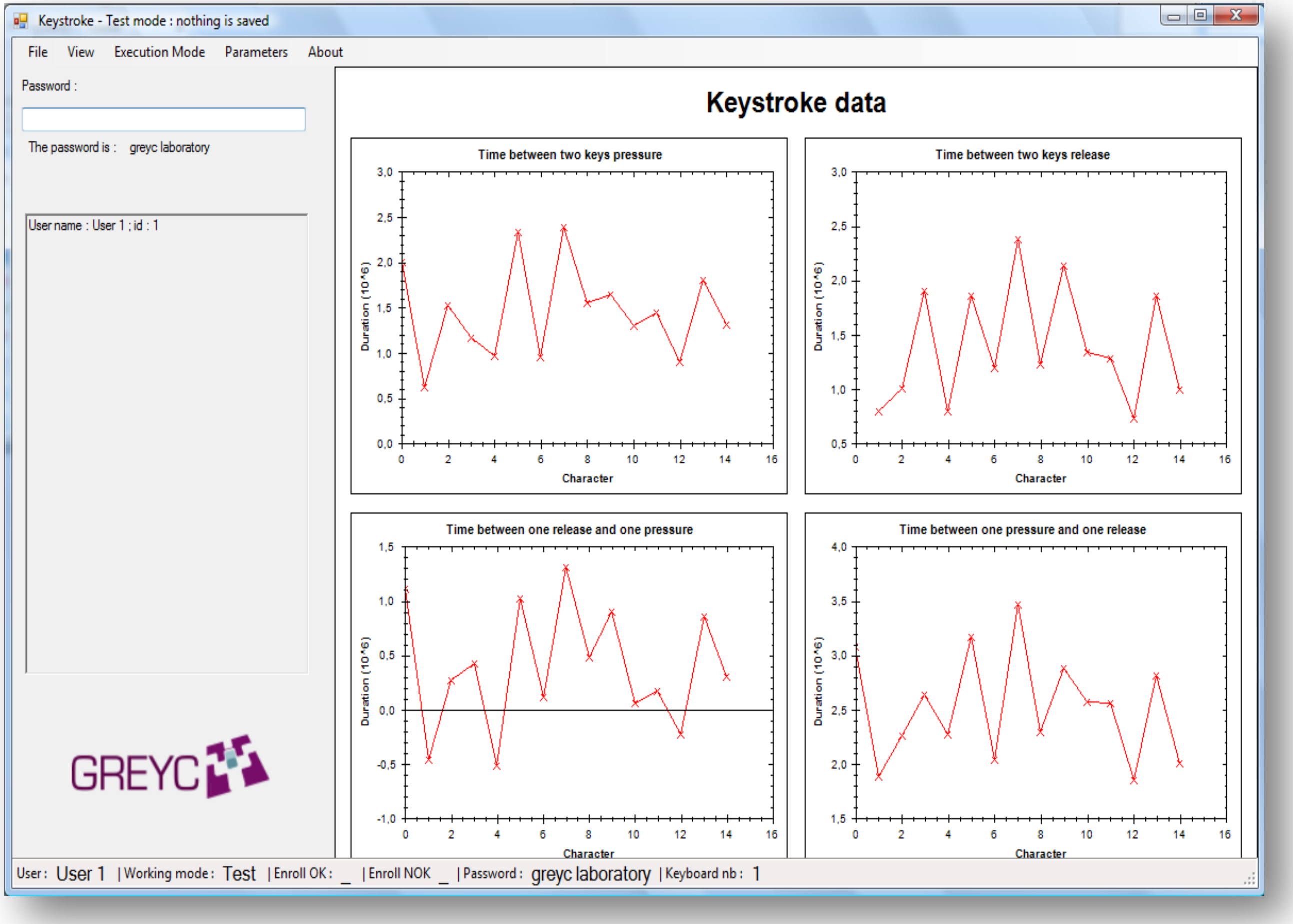
How it works ?

- ❑ Record different times: PP (latency between two pressures), RR (latency between two releases), RP (latency between one release and one pressure) and PR (duration of a key press),

- ❑ Use this feature vector to measure the similarity of keystroke dynamics.



Keystroke dynamics



Keystroke - Test mode : nothing is saved

Password :

The password is : greyc laboratory

User name : User 1 ; id : 1

User : User 1 | Working mode : Test | Enroll OK : _ | Enroll NOK _ | Password : greyc laboratory | Keyboard nb : 1

File
View
Execution Mode
Parameters
About
GREYC
Keystroke data
Time between two keys pressure
Time between two keys release
Time between one release and one pressure
Time between one pressure and one release
Duration (10^6)
Character
0
2
4
6
8
10
12
14
16
3,0
2,5
2,0
1,5
1,0
0,5
0,0
-0,5
-1,0
4,0
3,5

DEMO

Keystroke dynamics

Properties

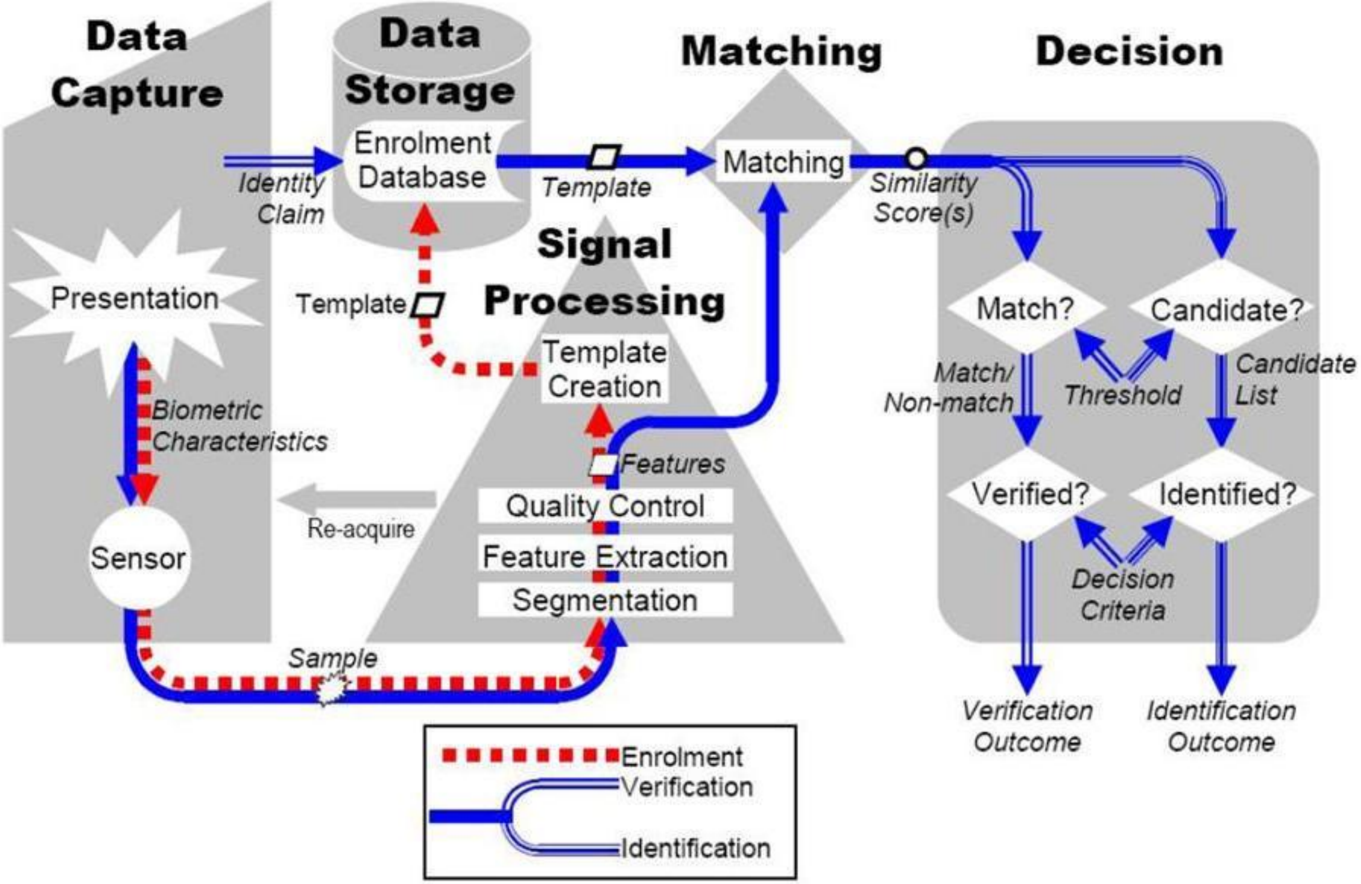
- ❑ A two authentication factor method
  - ✓knowledge of the password
  - ✓password typing

- ❑ Good acceptance
  - ✓ invisible for a user (passphrase or password)
  - ✓ no privacy issue (easy to change the password)
  - ✓ avoid complex passwords difficult to remind
  - ✓ still a low cost solution (software based solution)
  - ✓ can be used on all computers (no additional sensor)

Keystroke dynamics

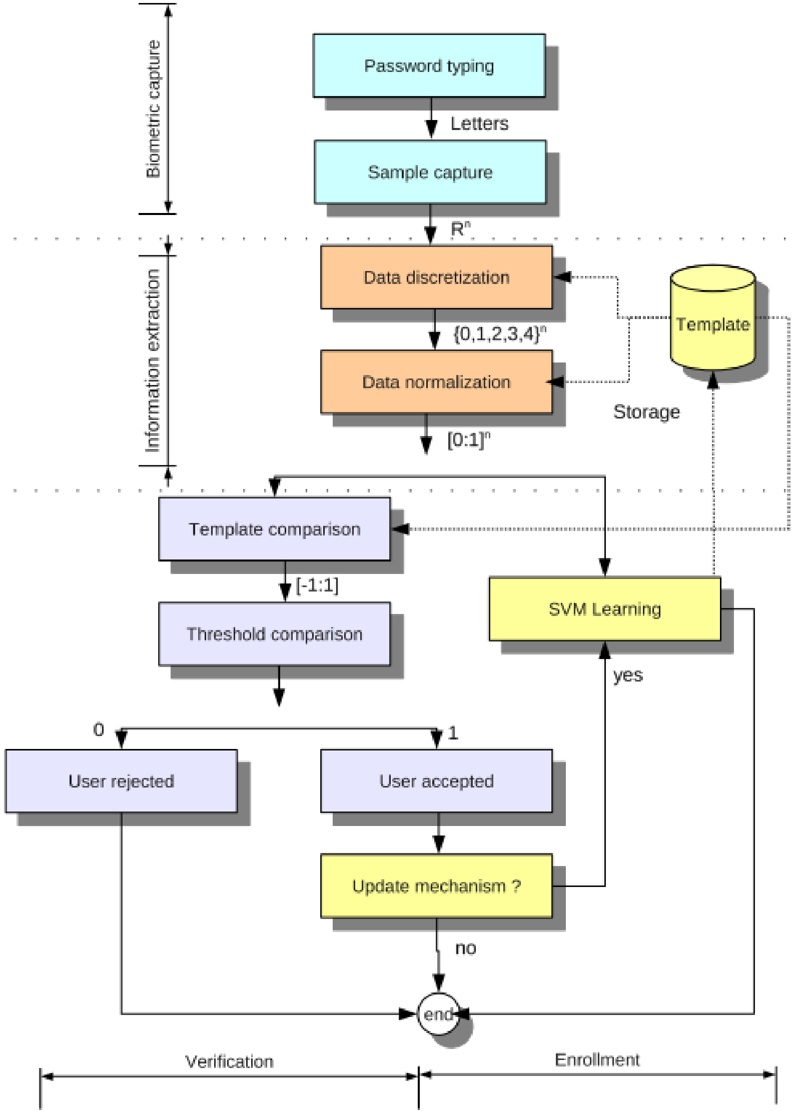
Functions in a biometric system

ISO /IEC JTC1 SC37 SD11



Keystroke dynamics

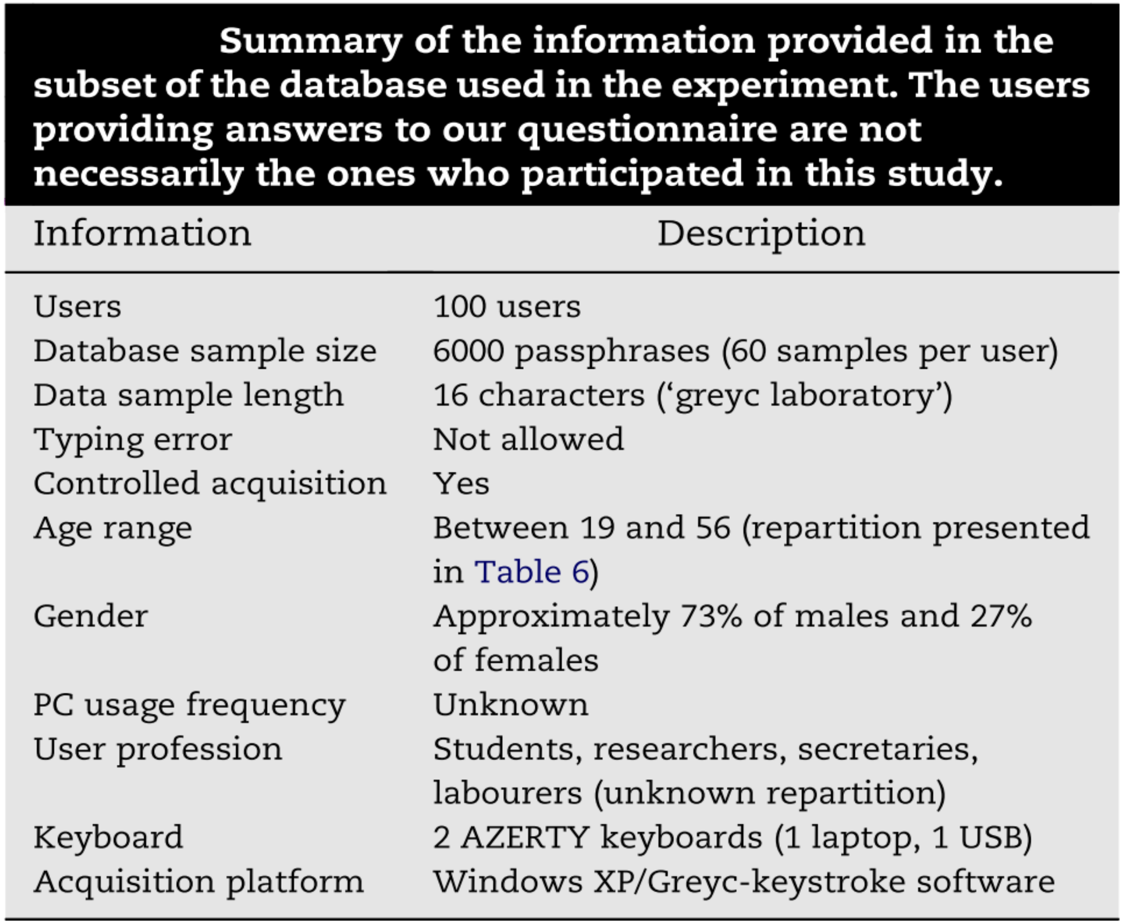
Authentication with a passphrase


Biometric capture
Information extraction
Password typing
Letters
Sample capture
R^n
Data discretization
$\{0,1,2,3,4\}^n$
Data normalization
$[0:1]^n$
Template
Storage
Template comparison
[-1:1]
Threshold comparison
SVM Learning
yes
0
1
User rejected
User accepted
Update mechanism ?
no
end
Verification
Enrollment

- Using the same word for all users
- Data discretisation to limit noise impact
- SVM learning
- Template mechanism

Keystroke dynamics

Proposed benchmark: GREYC Keystroke



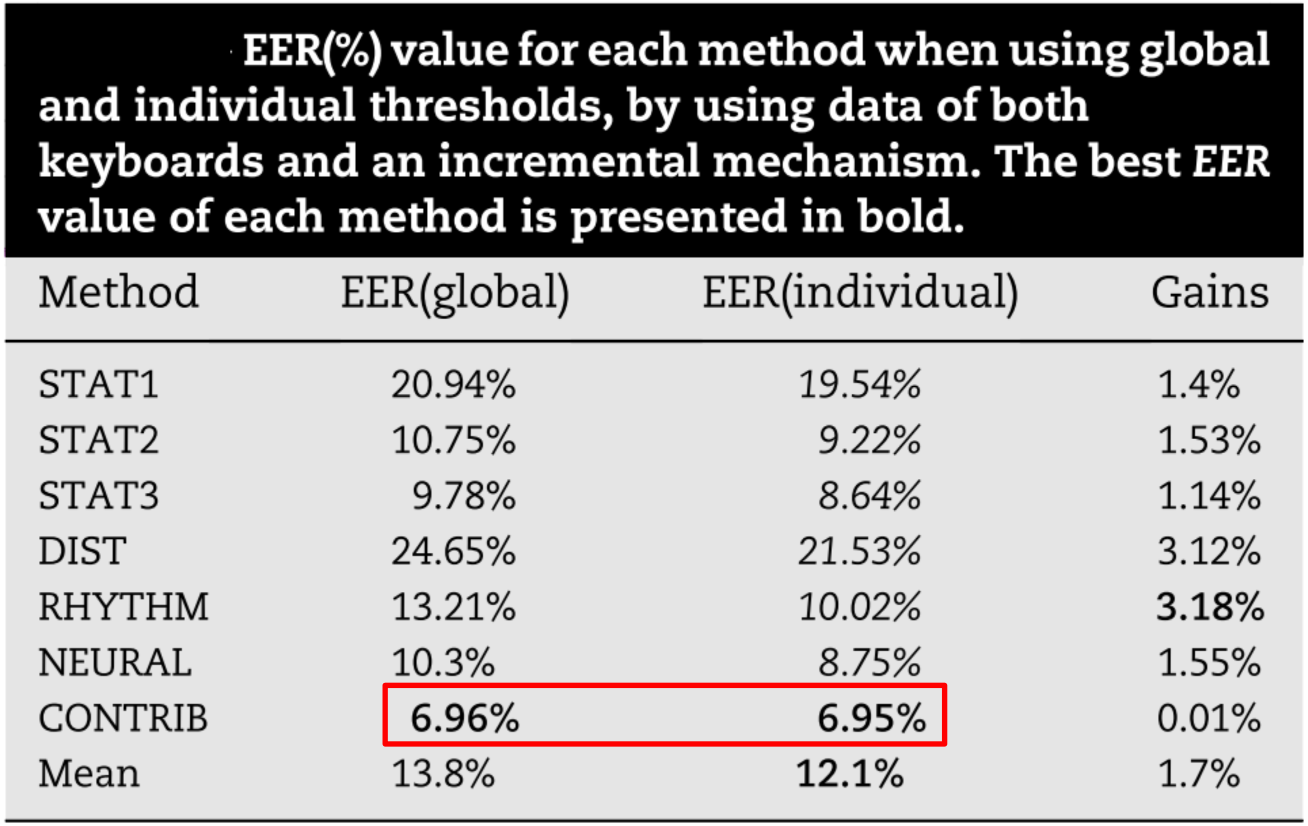
Summary of the information provided in the subset of the database used in the experiment. The users providing answers to our questionnaire are not necessarily the ones who participated in this study.

Information	Description
Users	100 users
Database sample size	6000 passphrases (60 samples per user)
Data sample length	16 characters ('greyc laboratory')
Typing error	Not allowed
Controlled acquisition	Yes
Age range	Between 19 and 56 (repartition presented in Table 6)
Gender	Approximately 73% of males and 27% of females
PC usage frequency	Unknown
User profession	Students, researchers, secretaries, labourers (unknown repartition)
Keyboard	2 AZERTY keyboards (1 laptop, 1 USB)
Acquisition platform	Windows XP/Greyc-keystroke software

R. Giot, M. El-Abed, and C. Rosenberger, "GREYC Keystroke: a Benchmark for Keystroke Dynamics Biometric Systems," in Proc. IEEE International Conference on Biometrics: Theory, Applications and Systems (BTAS 2009), pp. 1-6, Washington, USA, 2009

Keystroke dynamics

Performance evaluation



EER(%) value for each method when using global and individual thresholds, by using data of both keyboards and an incremental mechanism. The best *EER* value of each method is presented in bold.

Method	EER(global)	EER(individual)	Gains
STAT1	20.94%	19.54%	1.4%
STAT2	10.75%	9.22%	1.53%
STAT3	9.78%	8.64%	1.14%
DIST	24.65%	21.53%	3.12%
RHYTHM	13.21%	10.02%	**3.18%**
NEURAL	10.3%	8.75%	1.55%
CONTRIB	**6.96%**	**6.95%**	0.01%
Mean	13.8%	**12.1%**	1.7%

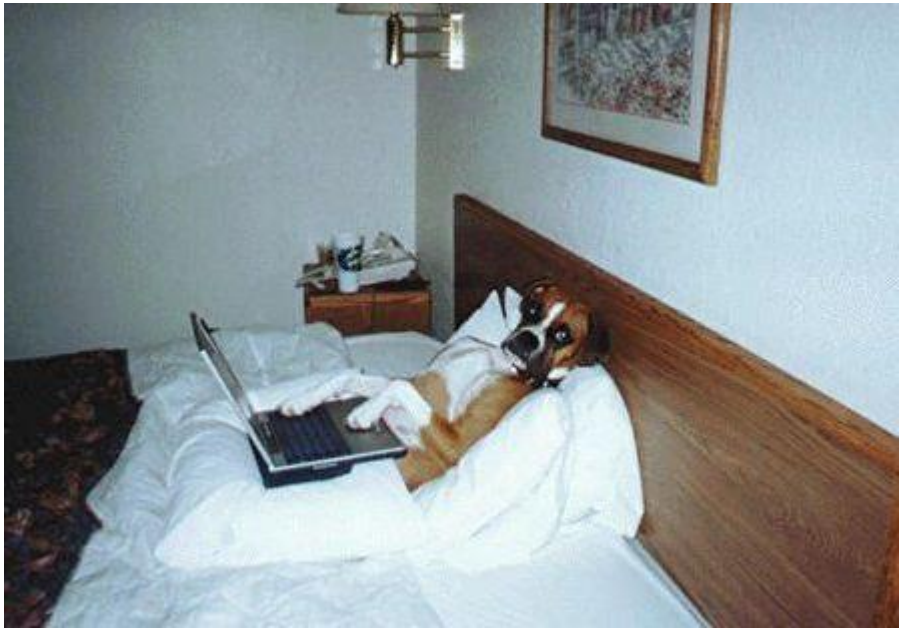
G. Romain, M. El Abed, B. Hemery, and C. Rosenberger, "Unconstrained Keystroke Dynamics Authentication with Shared Secret," Elsevier International Journal on Computers & Security, 2011.

Keystroke dynamics

A good candidate

To enhance the security of passwords

To profile the user: soft biometrics



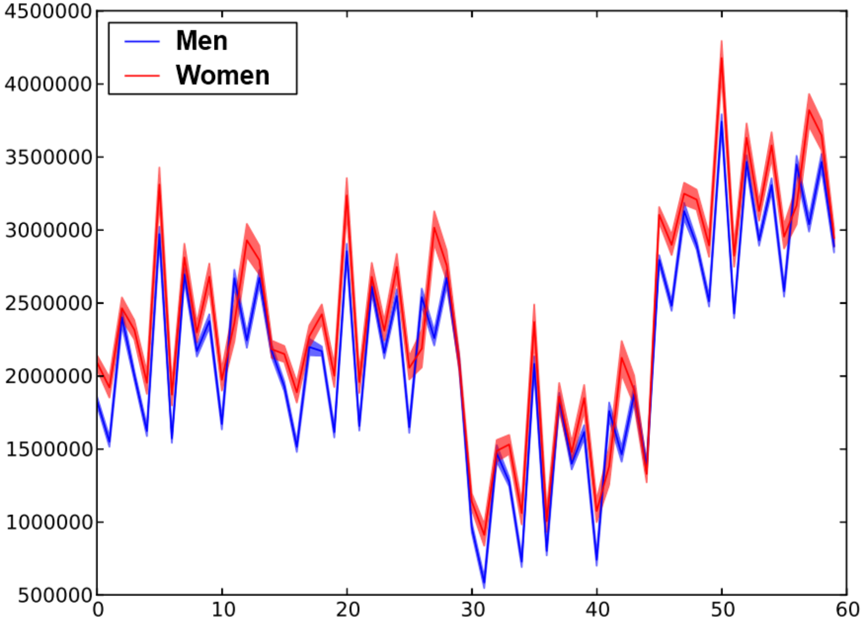
This guy seems to like bones

Keystroke dynamics

Gender recognition:

For a specific passphrase « Greyc laboratory »
~90% (based on SVM learning)

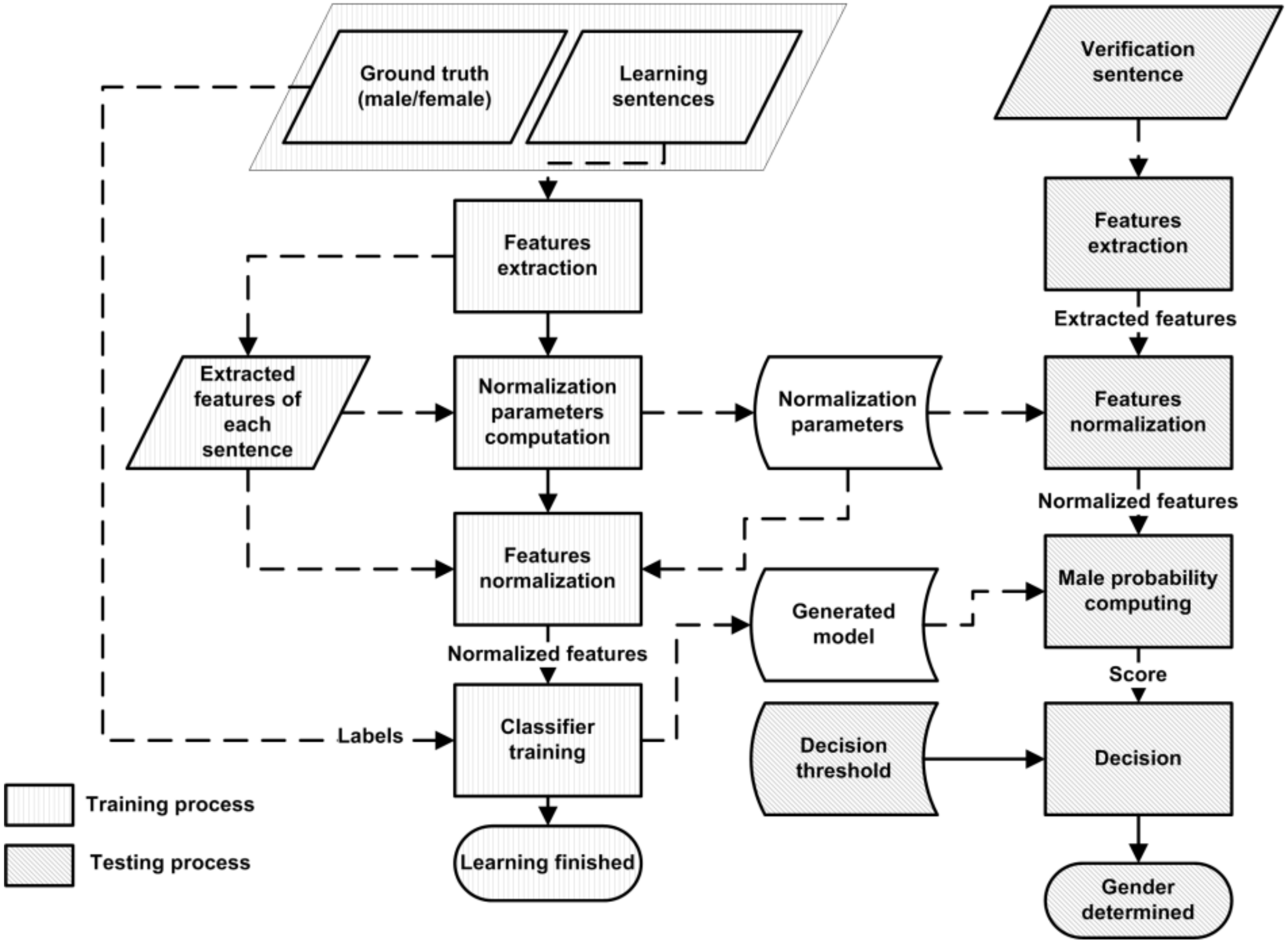
For free text
Gender recogntion:
~ **75%** for one sentence
~ **80%** for ten sentences



R. Giot, C. Rosenberger, "A New Soft Biometric Approach For Keystroke Dynamics Based On Gender Recognition" International Journal of Information Technology and Management (IJITM) Special Issue on : "Advances and Trends in Biometrics". Dr Lidong Wang, pages 1-16, 2011.

Keystroke dynamics

Gender recognition: free text



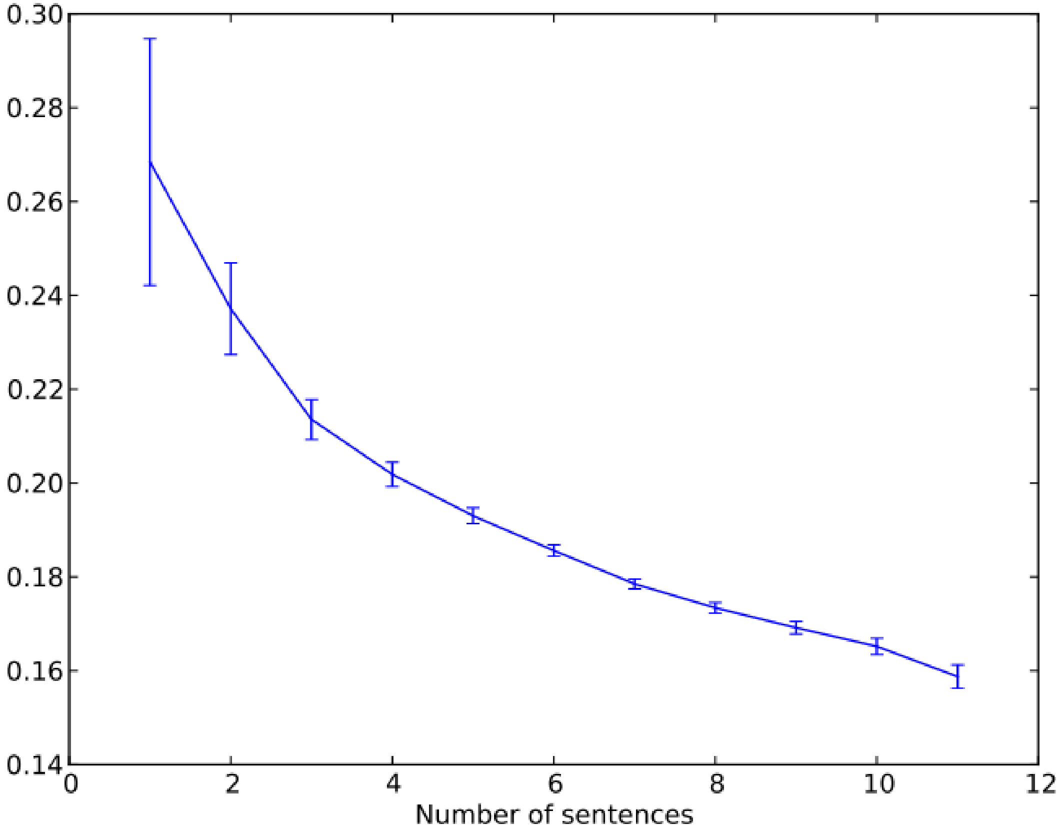
Keystroke dynamics

Age category:

On free text: Decide if the user is over 30 years old

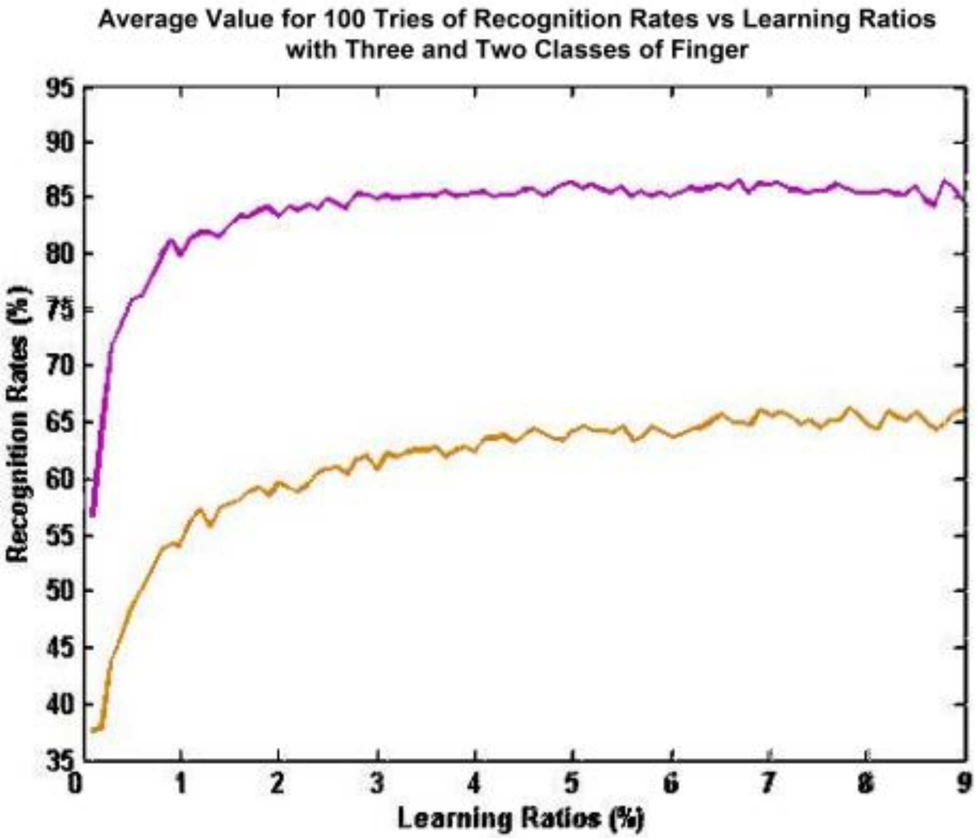
~ **70%** for one sentence

~ **83%** for ten sentences



Keystroke dynamics

Way of typing recognition:



Syed Zulkarnain Syed Idrus, Estelle Cherrier, Christophe Rosenberger and Patrick Bours, 2012, "A Preliminary Study of a New Soft Biometric Approach for Keystroke Dynamics". Poster presented at the 9th Summer School for Advanced Studies on Biometrics for Secure Authentication: Understanding Man Machine Interactions in Forensics and Security Applications Alghero, Sardinia, Italy, 2012.

Conclusion

Keystroke dynamics

- ❑ An interesting biometric modality (usable, privacy compliant, low cost…)
- ❑ Provides a better security (not perfect, does it exist ?)

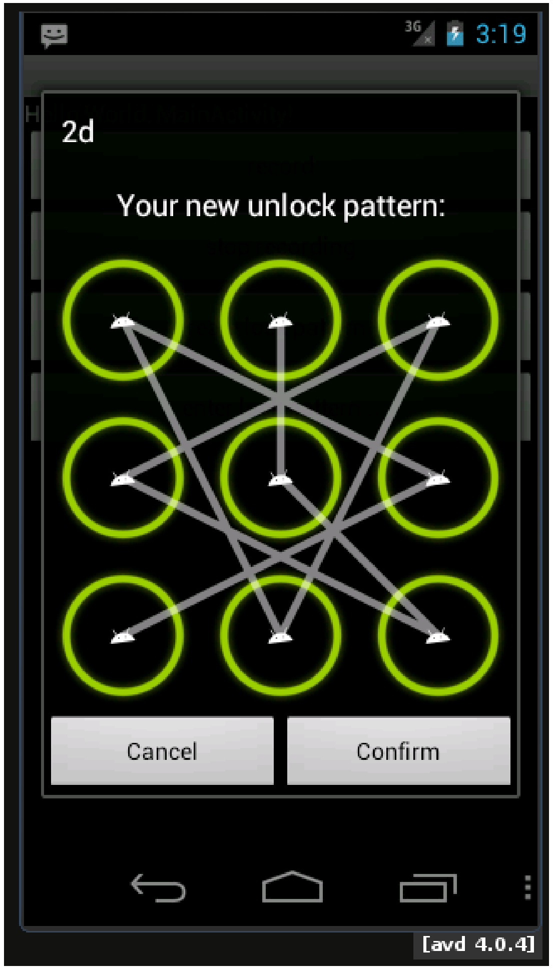
Many trends have to be more studied

- ❑ Avoiding the replay attack (joint work with P. Bours)
- ❑ Better user’s profiling
- ❑ Generalization of the keystroke dynamics for touch screens

Conclusion

Biometric pattern based password

- ❑ Combining knowledge of the secret path and the way of making it (X,Y positions with time, surface in contact with time...)
- ❑ Difficult to forge
- ❑ Usable solution and fast



http://www.epaymentbiometrics.ensicaen.fr/