Graphical-based User Authentication Schemes for Mobile Devices

Vitaly Petrov
Alexandra Afanasyeva
Department of Information Systems Security (ISS)
State University of Aerospace Instrumentation (SUAI)
St. Petersburg
Russia

Problem description

Personal information → Mobile devices

Loss or theft → Threat of disclosure

- **“Text passwords are inconvenient” - Google**
  - No keyboard
  - Bad memorability
- **Graphical Passwords (GP) as an alternative**
  - Better memorability [Paivio, 2006]
  - Ease of input (touchscreen)
  - Higher security level [Chiasson, 2009]

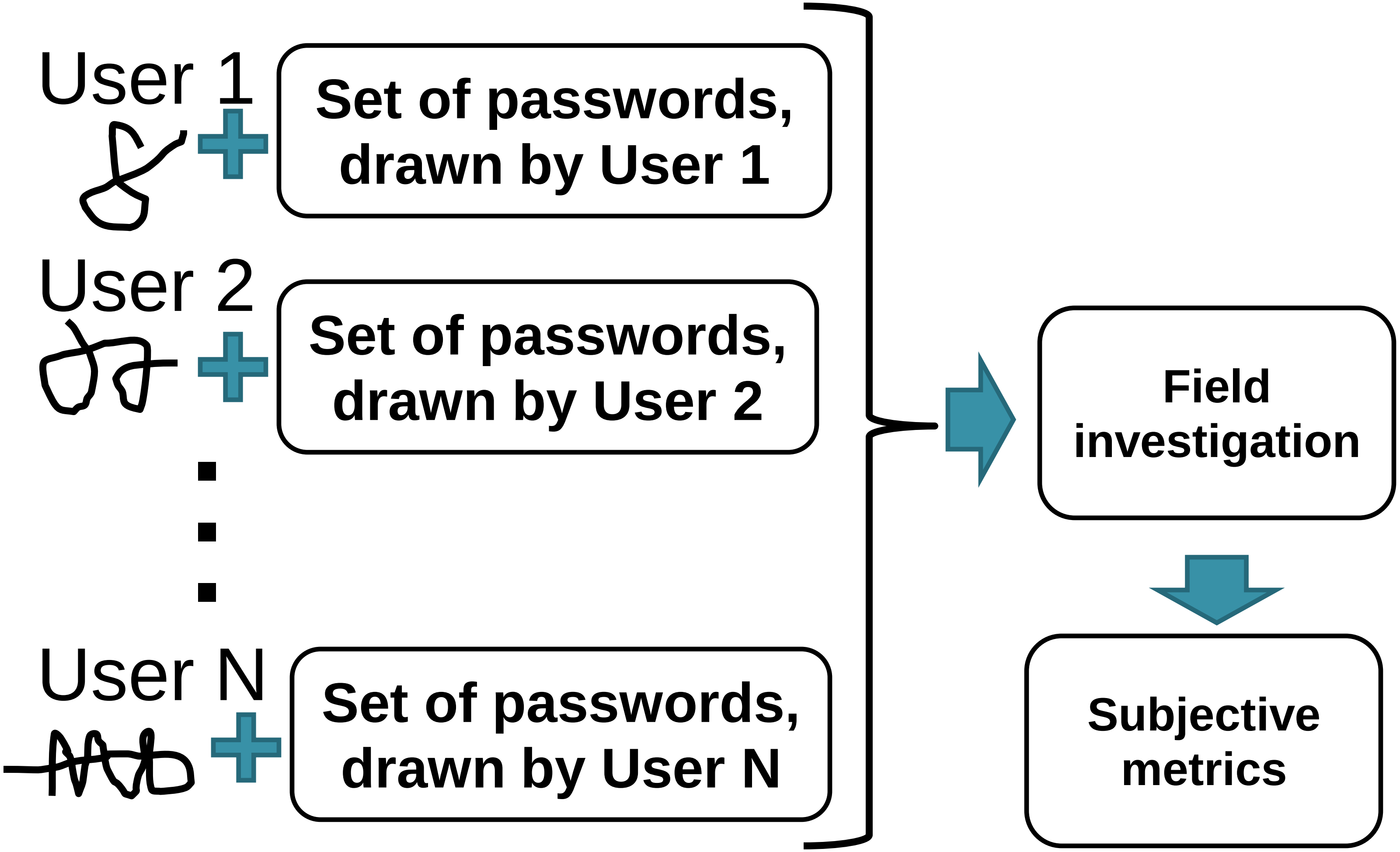
Graphical passwords issues

- Excessive variety of schemes
- Problems with storing passwords as a hash
- Absence of objective metrics
  - “Field investigation” – usability
    - expensive
    - subjective
    - not persuasive
  - No theoretical assessments - security

Project goal

Objective metrics and automated methods to evaluate different GP schemes

Traditional approach



User 1

Set of passwords, drawn by User 1

User 2

Set of passwords, drawn by User 2

⋮

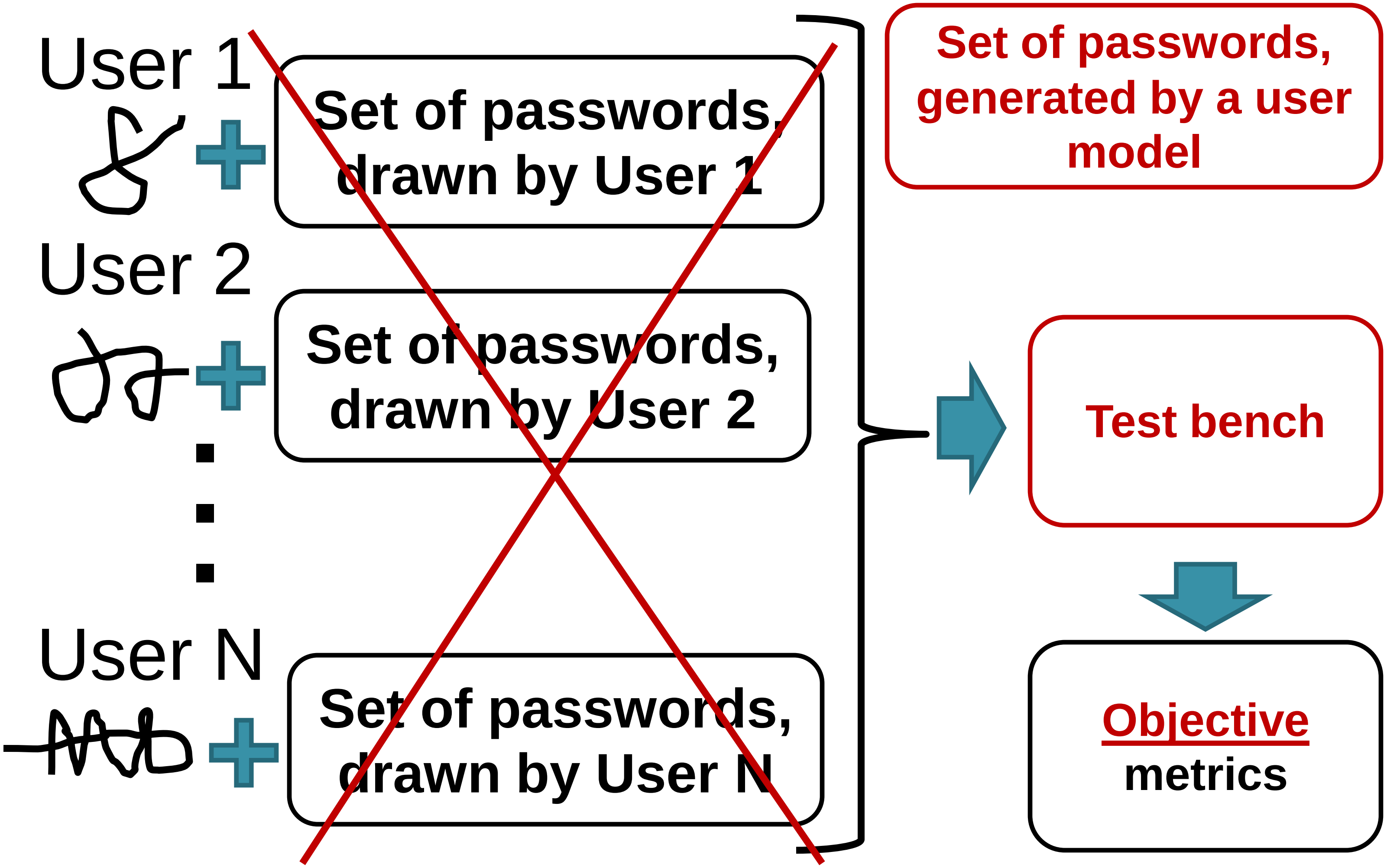
User N

Set of passwords, drawn by User N

Field investigation

Subjective metrics

Proposed approach



User 1

~~Set of passwords, drawn by User 1~~

User 2

~~Set of passwords, drawn by User 2~~

User N

~~Set of passwords, drawn by User N~~

Set of passwords, generated by a user model

Test bench

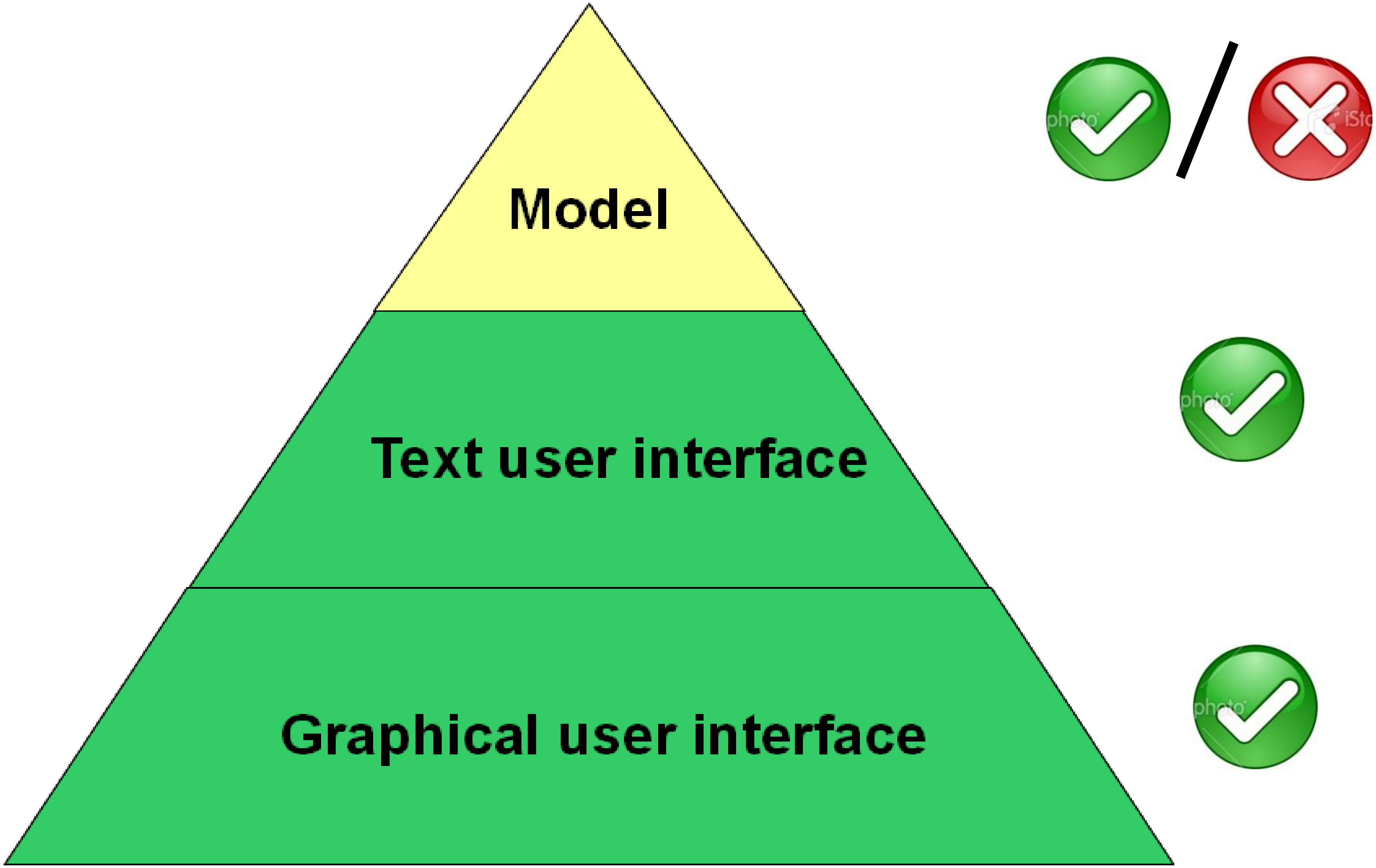
Objective metrics

Metrics chose

- False positive error rate
  - Valid password → ✗

- False negative error rate
  - Non-valid password → ✓

Test bench

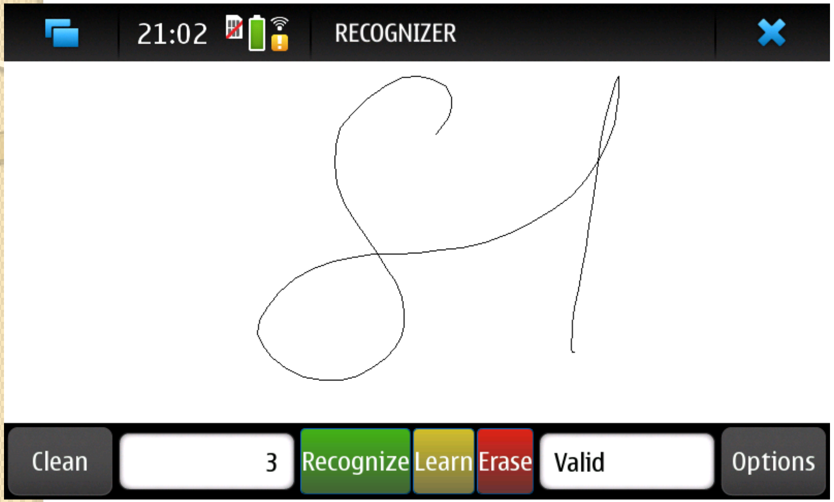


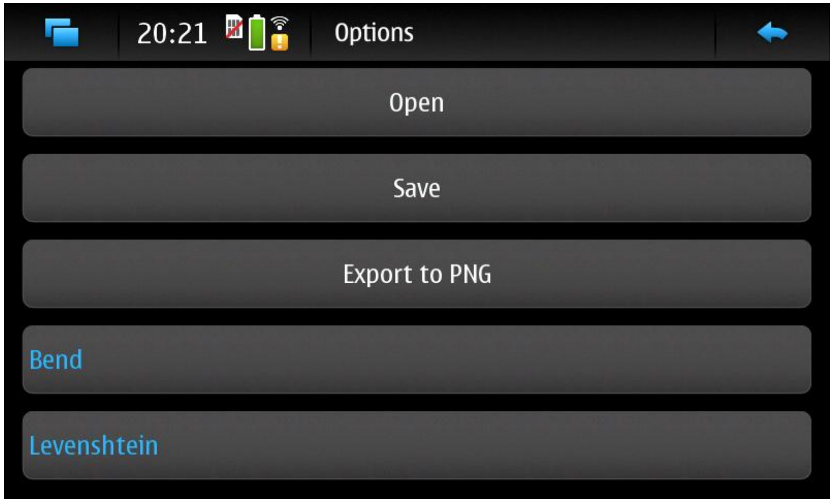
Model ✓ / ✗

Text user interface ✓

Graphical user interface ✓

Test bench GUI

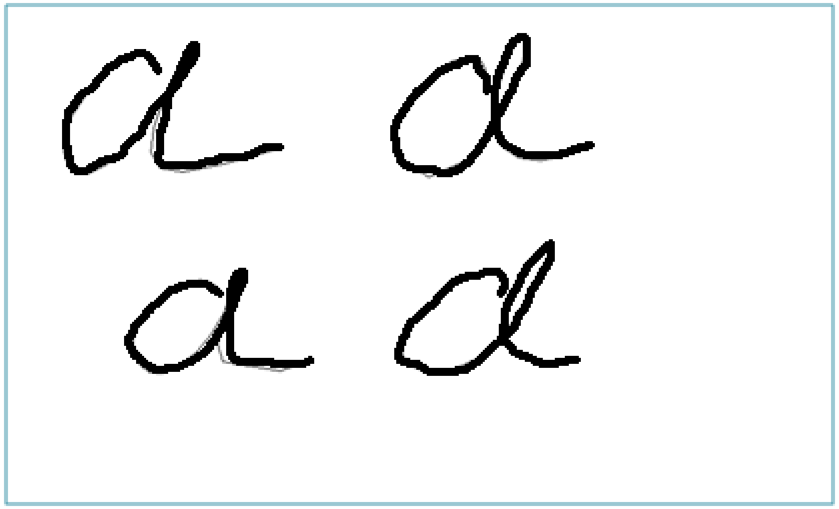


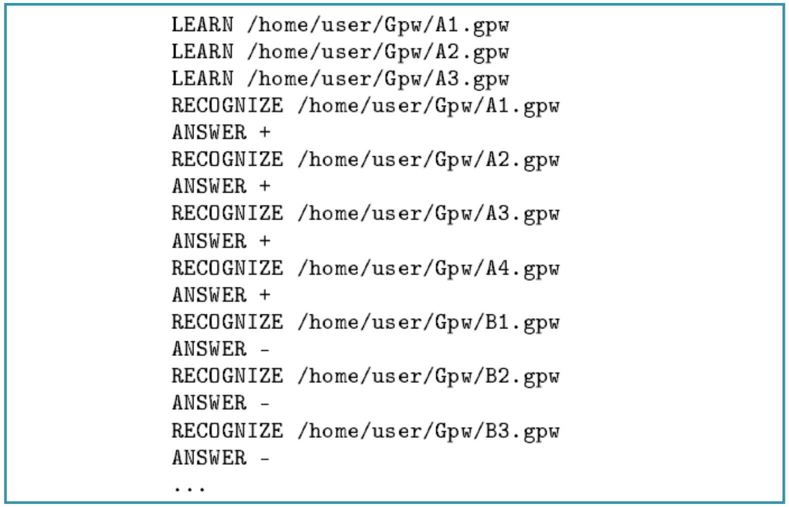


- Choose algorithm
- Set parameters
- Draw password
- Learn
- Recognize

- Erase password template
- Export
- **Save**
- Load

Test bench text interface



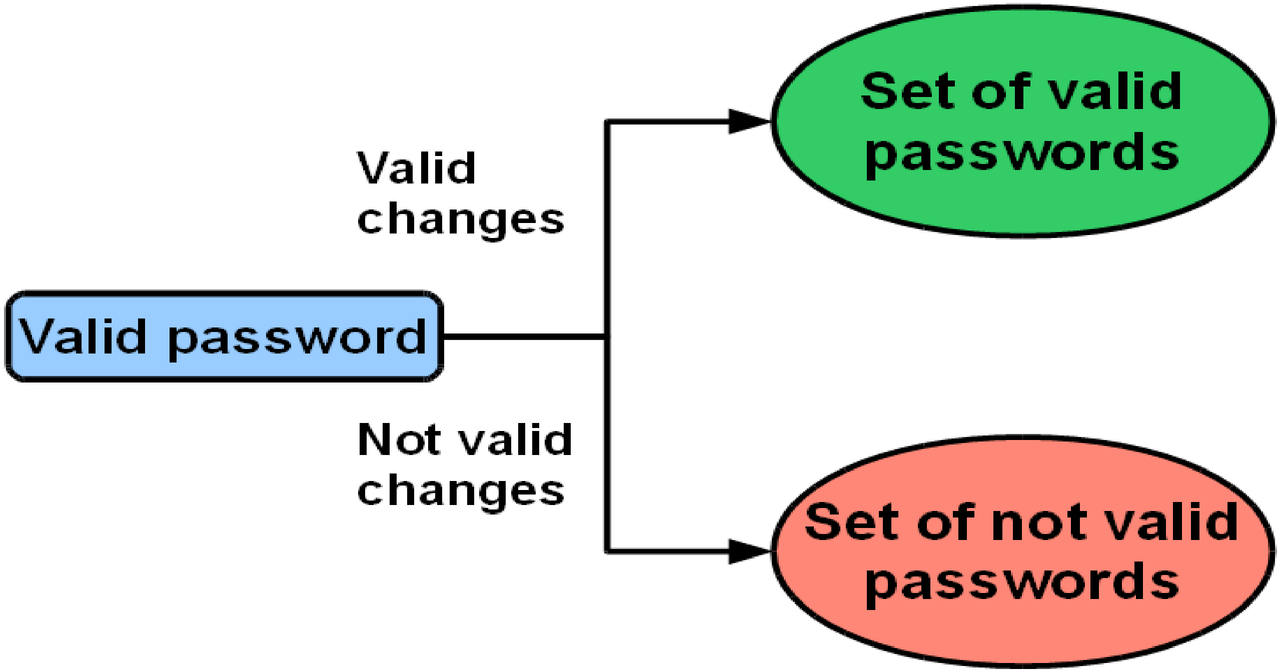


```
LEARN /home/user/Gpw/A1.gpw
LEARN /home/user/Gpw/A2.gpw
LEARN /home/user/Gpw/A3.gpw
RECOGNIZE /home/user/Gpw/A1.gpw
ANSWER +
RECOGNIZE /home/user/Gpw/A2.gpw
ANSWER +
RECOGNIZE /home/user/Gpw/A3.gpw
ANSWER +
RECOGNIZE /home/user/Gpw/A4.gpw
ANSWER +
RECOGNIZE /home/user/Gpw/B1.gpw
ANSWER -
RECOGNIZE /home/user/Gpw/B2.gpw
ANSWER -
RECOGNIZE /home/user/Gpw/B3.gpw
ANSWER -
...
```

- Get a set of entered passwords by GUI
- Write a configuration file, start application
- Get results
  - False negative error rate
  - False positive error rate

Test bench user model

- Valid changes
  - Turning
  - Scaling
  - Moving
  - Shaking
- Not valid changes
  - New intersections
  - New lines
  - Points deletion



Current status and future activities

- Done
    1. Test bench development
    2. Implementation of *DaS* and *PassShapes* schemes

- Current status
    1. Negative test implementation
    2. Proving of the model adequacy

- Future research directions
    1. Comparison of existing schemes using proposed method
    2. Improvement of *DaS* and *PassShapes* schemes according to the suggested metrics

References

- Passfaces Corporation, "The science behind PassFaces" White paper, http://www.passfaces.com/enterprise/resources/white_papers.htm, 2010
- R. Biddle, S. Chiasson, P.C. van Oorschot, "Graphical Passwords: Learning from Fisrt Generation", Technical Report TR-09-09, School of Computer Science, Carleton University, Ottawa, Canada, 2009
- H. Tao and C. Adams, "Pass-Go: A proposal to improve the usability of graphical passwords," International Journal of Network Security, vol. 7, no. 2, pp. 273–292, 2008
- R. Weiss and A. De Luca, "PassShapes - utilizing stroke based authentication to increase password memorability", in NordiCHI, ACM, pp. 383-392, 2008
- Google Corporation, "Android operation system", http://android.com, 2008
- S. Chiasson, P. C. van Oorshot and R. Biddle, "Graphical password authentication using Cued Click Points", in European Symposium On Research In Computer Security (ESORICS), LNCS 4734, pp. 359-374, 2007
- A. Paivio, "Mind and Its Evolution: A Dual Coding Theoretical Approach", Lawrence Erlbaum: Mahwah, N.J., 2006
- I. Jermyn, A. Mayer, F. Monrose, M. Reiter and A. Rubin, "The design and analysis of graphical passwords", in 8th USEFIX Security Symposium, 1999

Thank you for your attention

Questions?