8TH INTERNATIONAL CONFERENCE
INTER-ENG 2014
TIRGU MURES, OCTOBER 9–10, 2014.

Keystroke Dynamics on Android Platform

Margit Antal, László Zsolt Szabó, Izabella László
Sapientia University Faculty of Technical and Human Sciences

PROBLEM STATEMENT

- Password-based User Authentication is widely used

PROBLEM STATEMENT

- Password-based User Authentication is widely used

- Develop a strengthening mechanism for password-based authentication

PROBLEM STATEMENT

- People store sensitive information on mobile devices

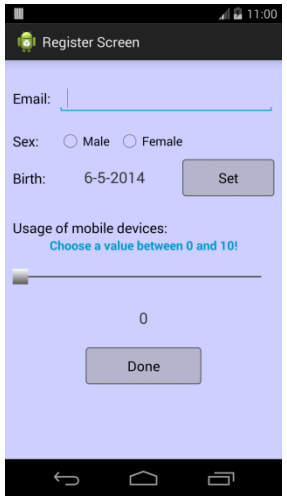
- Develop a strengthening mechanism for password-based authentication

- Research shows that users have unique password typing patterns

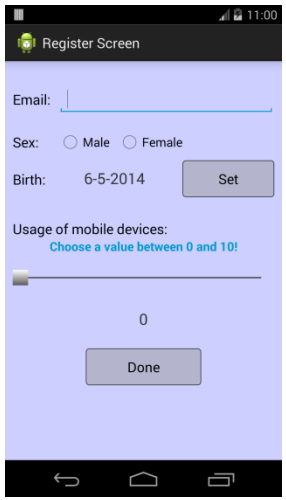
RESEARCH QUESTION

- Can new features provided by touchscreens – such as pressure or finger area – improve the accuracy of keystroke based authentication?

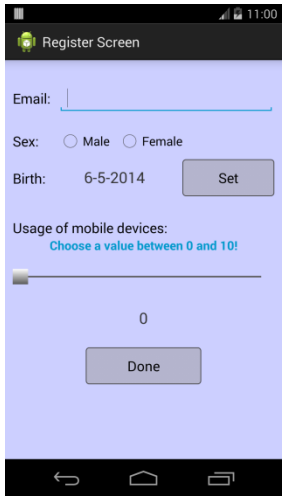
METHODS – Data collection



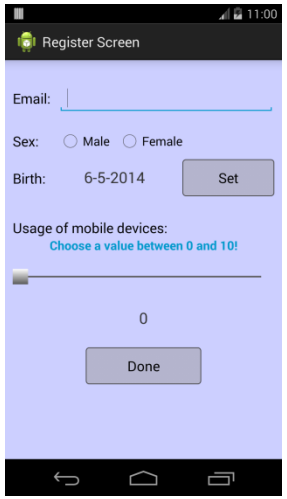
METHODS – Data collection



METHODS – Data collection



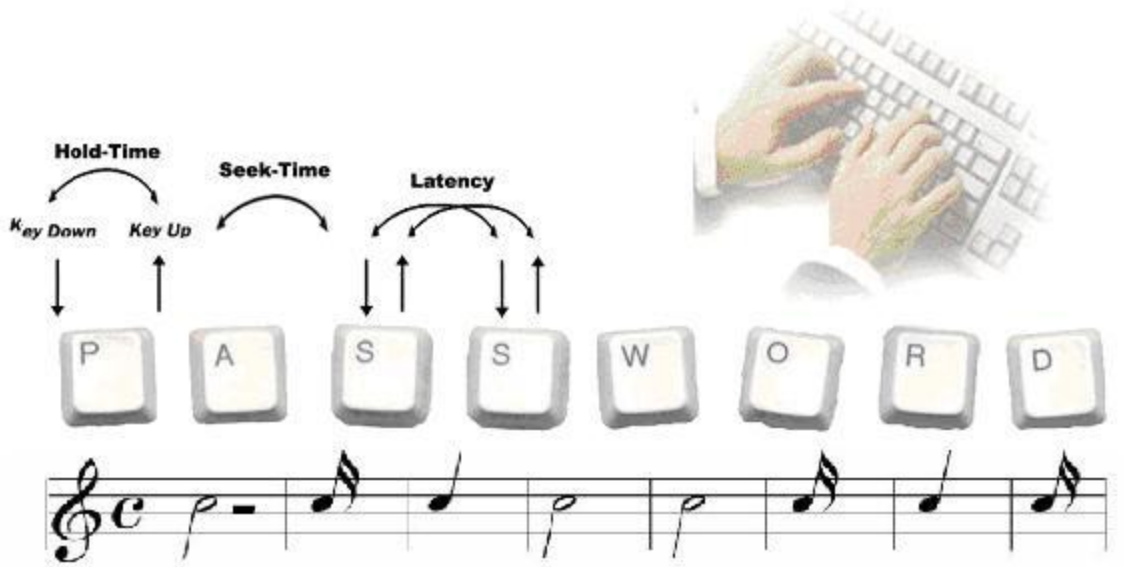
METHODS – Data collection



METHODS – Data collection

- 2 different Android devices
  - Nexus 7: 1080x1205 resolution
  - Mobil LG Optimus L7 II P71071
- Subjects: 42
  - 24 male
  - 18 female
- Samples
  - 51 samples/subject
- Multiple sessions
  - At least 2 sessions/user
- Strong password: .tie5Roanl

METHODS – Raw data



METHODS – Feature Set 1 – Time-based features (41 features)

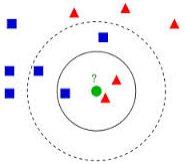
Feature name	Explanation	Number of features
Key hold time (H)	Time between key press and release	14
Down-down time (DD)	Time between consecutive key presses	13
Up-down time (UD)	Time between key release and next key press	13
Average hold time (AH)	Average of key hold times	1

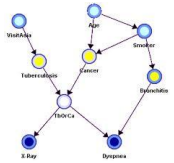
METHODS – Feature Set2 – Time- + touchscreen-based features (71 features)

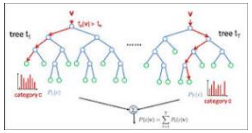
Feature name	Explanation	Number of features
Key hold time (H)	Time between key press and release	14
Down-down time (DD)	Time between consecutive key presses	13
Up-down time (UD)	Time between key release and next key press	13
Key press pressure (P)	Pressure at the moment of key press	14
Finger area (FA)	Finger area at the moment of key press	14
Average hold time (AH)	Average of key hold times	1
Average finger area (AFA)	Average of finger areas	1
Average pressure (AP)	Average of key pressures	1

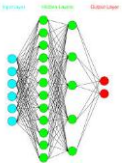
EVALUATION

- Identification (N-class classification)
  - Naïve Bayes
  - Bayesian Networks
  - C4.5 (J48)
  - K-NN (IBk)
  - SVM (LibSVM)
  - Random forests
  - MLP



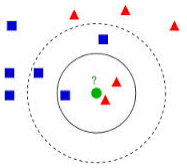


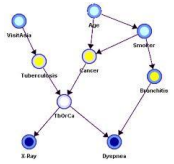


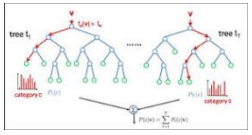


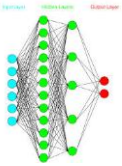
EVALUATION

- Identification (N-class classification)
  - Naïve Bayes
  - Bayesian Networks
  - C4.5 (J48)
  - K-NN (IBk)
  - SVM (LibSVM)
  - Random forests
  - MLP





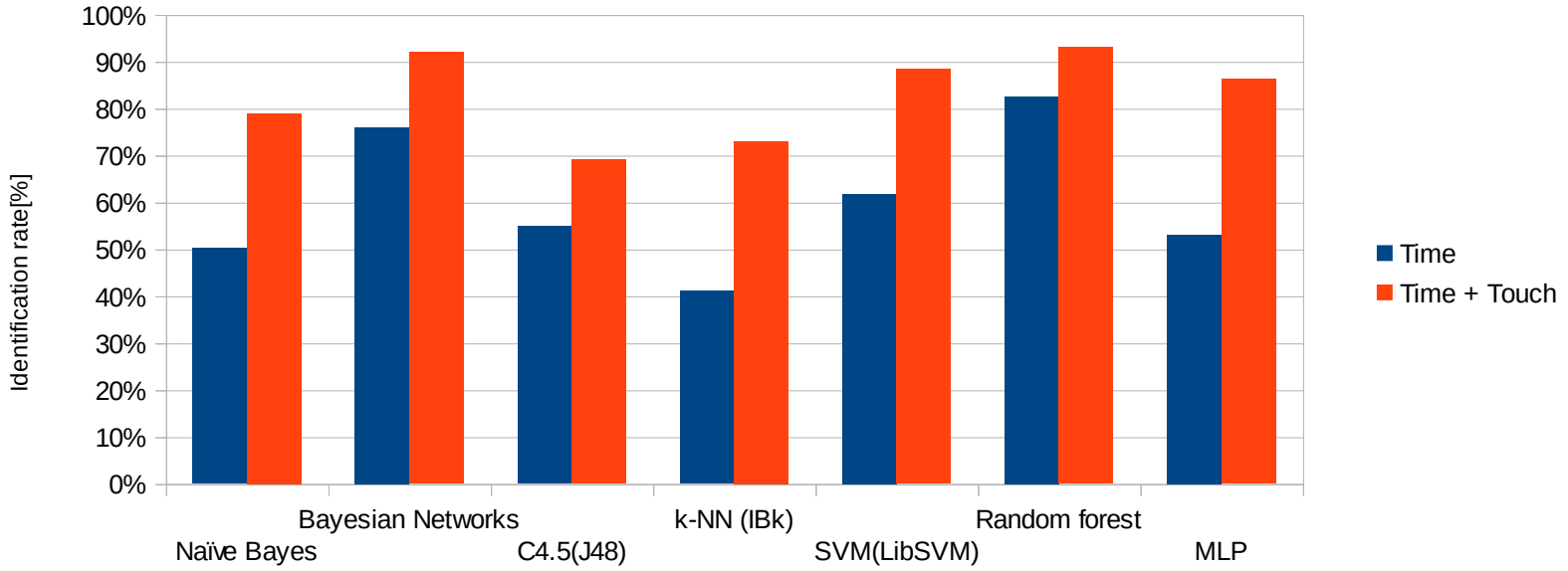




- Authentication (2-class classification): Accept/Reject
  - $U = \{u_1, u_2, \ldots, u_N\}$
  - 1. class: Patterns from a given user: u_i
  - 2. class: Patterns from the other users: $U-\{u_i\}$ (randomly selected)

EVALUATION: User Identification

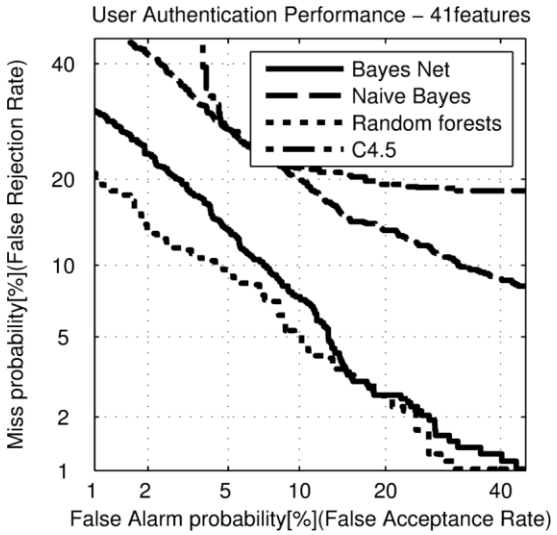
- 10-folds stratified cross validation (total: 100 runs)



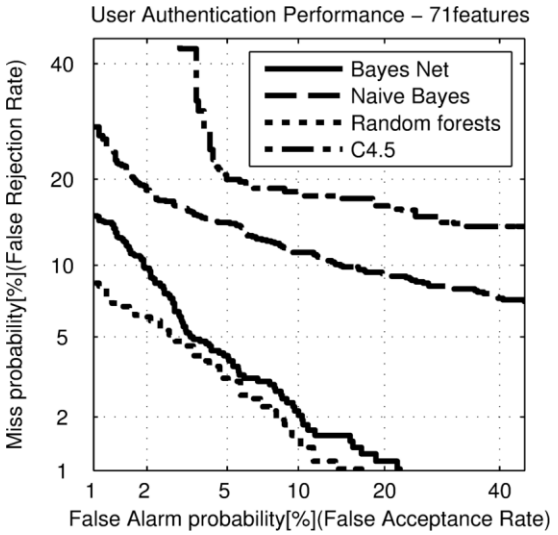
EVALUATION: User Authentication

Detection Error Trade Curves

Time-based features
EER: ~8% Random forests



Time- and touch-based features
EER: ~4% Random forests



CONCLUSIONS

- Touch-based features (pressure + finger area) improved significantly the accuracy of identification and authentication

CONCLUSIONS

- Touch-based features (pressure + finger area) improved significantly the accuracy of identification and authentication

- Best performers:
  - Random forests
  - Bayes Net

CONCLUSIONS

- Touch-based features (pressure + finger area) improved significantly the accuracy of identification and authentication

- Best performers:
  - Random forests
  - Bayes Net

- Advantages
  - cheap
  - non-intrusive → good user acceptance

CONCLUSIONS

- Touch-based features (pressure + finger area) improved significantly the accuracy of identification and authentication

- Best performers:
  - Random forests
  - Bayes Net

- Advantages
  - cheap
  - non-intrusive → good user acceptance

- Disadvantage
  - not a stable biometrics (affected by multiple factors)

FUTURE DIRECTIONS

- Study the typing of several passwords
  - Easy (e.g. jimmorrison)
  - Strong, illogical (.tie5Roanl)
  - Strong, logical (kktsf2!) kicsi kutya tarka se fule se farka

- Study free-text typing

Thank you for your attention!

Questions?