K-means++ vs Behavioral biometrics: One Loop to Rule Them All

Parimarjan Negi, Prafull Sharma, Vivek Jain, Bahman Bahmani
Stanford University
What is behavioral biometrics?

Historically:

- Handwriting recognition
- Telegraph Operators in WWII
Behavioral Biometrics: Modern Version

- Typing (Keystroke Dynamics)
- Mouse movements
- Typing, or swiping on a smartphone
- Through other smartphone sensors, e.g., gait analysis
Secondary Authentication

- Most secondary authentication methods involve the user actively doing something, e.g. two factor authentication.
- Behavioral Biometric methods function in the background
Popular

Al-based typing biometrics might be authentication's next big thing

The Future of Biometrics Could Be in What You Type

Biometrics: A Stepping-Stone To Eliminating The Password Forever

Behavioral Biometrics "stole the show"* at Google I/O
Quantifying Errors

False Rejection Rate: How many genuine samples get rejected?

False Acceptance Rate: How many impostor samples get accepted?

Equal Error Rate: Threshold where FAR = FRR
General Scenario

- Attacker knows the target user’s password
- Target user’s account protected using keystroke dynamics system
- Attacker does not have access to typing data from user

Attacker Aim

- Produce timings (key-press time, duration between keys) for a given password
How many tries does it take an attacker to “fool” such systems?
Targeted Attack Scenario

- Idealized scenario for the adversary
- has unlimited to attack single target
- Can generate a lot of timing samples for the target’s password from MTurk
Indiscriminate Attack Scenario

- Leaked database of passwords - attacker wants to quickly try these passwords for all accounts
- Too expensive to collect samples for each password
- Has access to precomputed datasets of typing data from the general population
Example Password: “Mustang”

- mutter, mumble
- bus, fuss
- tryst, list
- data, iota
- than, crane
- bang, rang
Is everyone’s behaviour unique?
Hypothesis: belongs to a bigger family of similar patterns
Hypothesis: If we find another user in the same “family”, we can “fool” the classifier
Idealized Algorithm: Randomly Choose first try
Idealized Algorithm: Choose next try from another cluster
Idealized Algorithm: Choose next try from another cluster
Hypothesis: If we find another user in the same “family”, we can “fool” the classifier
K-means++

- Initialization routine for centroids of K-means clustering
- At each successive iteration, finds centroids that are “far away” from the previous centroid
  - i.e., similar to finding a new try from a different family
Dataset I: DSN

- password: .tie5RoanI
- 51 subjects
- 400 repetitions
Dataset II: MTurk

- passwords: mustang, password, letmein, abc123, 123456789
- 583 subjects
- ~100 repetitions per password
One Class Classifiers

- Manhattan
- SVM
- Autoencoder
- Contractive Autoencoder
- Gaussian
- Gaussian Mixture
Two Class Classifiers

- Random Forests
- K-Nearest Neighbors
- Fully Connected Neural Network
# EER Scores

<table>
<thead>
<tr>
<th>Name of Classifier</th>
<th>DSN EER</th>
<th>MTurk EER</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manhattan</td>
<td>0.091</td>
<td>0.097</td>
</tr>
<tr>
<td>SVM</td>
<td>0.087</td>
<td>0.097</td>
</tr>
<tr>
<td>Gaussian</td>
<td>0.121</td>
<td>0.109</td>
</tr>
<tr>
<td>Gaussian Mixture</td>
<td>0.137</td>
<td>0.135</td>
</tr>
<tr>
<td>Autoencoder</td>
<td>0.099</td>
<td>0.099</td>
</tr>
<tr>
<td>Contractual Autoencoder</td>
<td>0.086</td>
<td>0.099</td>
</tr>
<tr>
<td>Random Forest</td>
<td>0.08</td>
<td>0.067</td>
</tr>
<tr>
<td>k-NN</td>
<td>0.09</td>
<td>0.090</td>
</tr>
<tr>
<td>FC Neural Net</td>
<td>0.08</td>
<td>0.091</td>
</tr>
</tbody>
</table>
Results

MTurk Dataset

SVM
Results

MTurk Dataset
Random Forests
Usual Threshold

User Scores

EER Threshold
Conservative Threshold

User Scores

Median Threshold
Conservative Thresholds I

Targeted Manhattan
Conclusion

● Behavioral Biometrics are promising but we need to improve them with regards to motivated adversaries
● Classifiers can potentially be made more robust by aiming to thwart such adversarial models
● datasets, code