Game Based Authentication: Mimicry Attack

Summer 2018
REU Fellow: Camera Finn
Faculty Mentors: Dr. Jonathan Voris
Affiliation: ¹Hobart and William Smith Colleges and ²School of Engineering and Computing Science, NYIT
Emails: camera.finn@hws.edu, jvoris@nyit.edu

ABSTRACT
Mobile devices are a growing target for theft due to the growth infeasibility of the information that users store in their devices. Current authentication methods have been criticized to be invasive and not very usable. In response to this, game based authentication study has been conducted and shown to have great potential for authenticating users. We investigate whether or not game-based authentication is susceptible to shoulder mimicry attacks. The results suggest that game based authentication is not significantly impacted from an attacker observing and mimicking the user.

STUDY COMPONENTS

Games

Samsung Galaxy S3

Participants: 8 REU Fellows

Touch Sensors: Collect and process touch data by extracting features and saving to csv files

R scripts and LibSVM based “e1071” R package: Model and Analyze Data One-class Classification SVMs

Features:
1. Initial x coordinate, (2) initial y coordinate, (3) final x coordinate, (4) final y coordinate, (5) time period during gesture, (6) average finger area coverage, (7) average finger width contacting the screen, (8) gesture’s length along x-axis, (9) gesture’s length along y-axis, (10) distance traveled during gesture, (11) direction of gesture, (12) gesture’s speed along x-axis, (13) gesture’s speed along y-axis, (14) gesture’s speed along trajectory, (15) gesture’s velocity, (16) gesture’s angular velocity, and (17) finger orientation change during gesture

Steps (Touch Sensor running in background during each gameplay)
1. Have users play game, 5 minutes each (no observation)
2. Pair users up, one be user A and other be user B
3. User A plays and user B watches
4. User B plays and user A watches
5. Repeat steps 3 and 4 for each game
6. User B plays and user A watches
7. User A plays and user B watches
8. Repeat steps 6 and 7 for each game
9. Put all data for each game together separated into files based on game and observation scenario
10. Implement one-class SVM using R scripts LibSVM based “e1071” R package

Generate 2 models for each game, each user, one pre-observation and one post-observation

Calculate and generate ROC and DET curves per model

Analyze performance of models and games both pre- and post-observation by comparing the average AUCs and EERs, which are computed using the ROC and DET curves

RESULTS

Table of Average AUC and EER Per Game Before and After Observation

<table>
<thead>
<tr>
<th>Game</th>
<th>Average AUC</th>
<th>Average EER</th>
<th>Change before and After Observation</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Before Observation</td>
<td>After Observation</td>
<td></td>
</tr>
<tr>
<td>Angry Birds</td>
<td>0.881</td>
<td>18.4203</td>
<td>0.8637</td>
</tr>
<tr>
<td>Fruit Ninja</td>
<td>0.9212</td>
<td>15.1966</td>
<td>0.8609</td>
</tr>
<tr>
<td>Temple Run</td>
<td>0.8065</td>
<td>21.2034</td>
<td>0.889</td>
</tr>
</tbody>
</table>

CONCLUSION
While game based authentication shows high performance for authenticating users, it’s important to see how strong it is against simple attacks, more specifically over the shoulder mimic attacks, which this study addresses. The results suggest that observing doesn’t have a significant impact on the performance of using the game Angry Birds, Fruit Ninja, and Temple Run for user authentication based on the average AUCs and average EERs for each game from pre- and post-observation. However, more study will be conducted to obtain more accurate results and see how significant observation has on the performance of game based authentication.

REFERENCES

ACKNOWLEDGEMENT
This research was supported by the National Science Foundation (NSF) Research Experiences for Undergraduates (REU) program. I would like to thank all of the mentors and research fellows at the New York Institute of Technology for providing help and guidance to me throughout the study.

This project is funded by National Science Foundation Grant No. CNS-1559652 and New York Institute of Technology.