A Novel Behavior-Based User Authentication Scheme

Zeyu Wu

Indiana University - Purdue University Fort Wayne

Follow this and additional works at: http://opus.ipfw.edu/stu_symp2015

Part of the Computer Sciences Commons

Recommended Citation

http://opus.ipfw.edu/stu_symp2015/72
Abstract

In this project, we present a user-behavior-based authentication scheme, which completely removes the need for traditional alphanumeric passwords. In order to be granted access to the system, the user must correctly pinpoint a secret location on a map, which is pre-defined by the user. In addition, the user’s behavior as he/she navigates to the pre-defined secret geographic location on the map are also used. To uniquely identify different users, a number of metrics have been extracted from each user’s behaviors. Then, data mining algorithms are used to create a profile for each legitimate user based on their behaviors. Access will only be granted to the user who not only knows the secret location, but also behaves in his/her unique manner. Our evaluation results illustrate that our passwordless authentication scheme can provide identify most users correctly without producing any error, while deny the intruders who behavior differently from the legitimate users.

Methodology

Our methodology uses two-levels of authentication

Level 1: Location-Based
- The user logs in by navigating to the secret location he/she specified during the registration process.

Level 2: Behavior-Based
- To construct the user behavior profile, we formulate seven attributes, which can efficiently quantify the characteristics of a user’s behavior, when she interacts with the map.
- The attributes can be constructed by various data mining algorithms to construct behavior profile for a user.
  - We avoid using those attributes, which construct models that are to either general or too specific.

Implementation

We have implemented our prototype with the following components:
- A web-based map interface for user data collection implemented using Google Map’s JavaScript API.
  - 10 users are asked to navigate the map from the Great Pyramids at Giza to the Friends Circle at IPFW.
  - A Java program is used to extract the user behavior-related attributes.
  - Average time taken to extract attributes from one user is 0.0266 seconds.
  - Weka, a data mining software, is used to train, test, and visualize the data via various algorithms.

Results

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Weighted Avg. FP</th>
<th>Weighted Avg. TP</th>
</tr>
</thead>
<tbody>
<tr>
<td>SVM</td>
<td>0.009</td>
<td>0.92</td>
</tr>
<tr>
<td>Naive Bayes</td>
<td>0.016</td>
<td>0.86</td>
</tr>
<tr>
<td>Random Forest</td>
<td>0.018</td>
<td>0.84</td>
</tr>
</tbody>
</table>

SVM produces the best result with the lowest FP and highest TP.

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Weighted Avg. ROC Area</th>
<th>Worst ROC Area</th>
</tr>
</thead>
<tbody>
<tr>
<td>SVM</td>
<td>0.895</td>
<td>0.866</td>
</tr>
<tr>
<td>Naive Bayes</td>
<td>0.887</td>
<td>0.964</td>
</tr>
<tr>
<td>Random Forest</td>
<td>0.892</td>
<td>0.882</td>
</tr>
</tbody>
</table>

Based on ROC area, Naive Bayes is the algorithm with the best general performance.

Discussion and Future Direction

Discussion:
- We might choose the SVM algorithm for our future experiment since it produces low FP rate and high TP rate.
- The majority of the user can be identified without producing any error. False positives occurs in 40% of users.

Future Research:
- Application of our authentication scheme on wearable devices
- Exploring the possibility of uniquely identifying a user by his/her mouse movement alone.

Acknowledgement

We thank the great comments provided by Dr. Jin Soong Yoo.