Forgery-Resistant Touch-based Authentication on Mobile Devices

Neil Zhenqiang Gong, Iowa State University
Mathias Payer*, Purdue University
Reza Moazzezi, UC Berkeley
Mario Frank, UC Berkeley

* @gannimo, http://hexhive.github.io
Mobile access to private data

- Our mobile devices have access to private data
  - EMail, banking, pictures, social media, documents
Mobile authentication is tedious

- Authentication is often disabled (42%)
- Biometric (fingerprint, face) prone to replay
Continuous Touch-Based Authentication
Continuous authentication

- Users continuously interact with the device
- Leverage these interactions to authenticate

Assumption: each user interacts differently
- Collect touch strokes
- Train model
- Use model to authenticate

Mario Frank, Ralf Biedert, Eugene Ma, Ivan Martinovic, and Dawn Song "Touchalytics: On the Applicability of Touchscreen Input as a Behavioral Biometric for Continuous Authentication". TIFS '13
Continuous authentication
Biometrics pitfall: replay attacks

- Loosing trained model or touch data is fatal
- Automated replay attacks are possible

A. Serwadda and V. V. Phoha. “When kids' toys breach mobile phone security.” In CCS’13
Forgery-Resistant Touch-based Authentication
TouchAlytics 2.0: diversity

• Assumption: slight variances in screen settings influence touch behavior
  – Introduce a (flexible) layer of indirection between the user and the authentication system
  – Constantly vary the screen settings
TouchAlytics 2.0: indirection

- Sensor records x, y, pressure, area
- Control transformation of raw data to primitives

- Indirection for raw touch data interpretation
  - X-Distortion: stretch strokes along x-axis
  - Y-Distortion: stretch strokes along y-axis

- Application acts relative to current setting
  - Users change behavior to compensate
Required: stability and sensitivity

(a) Unstable and sensitive
Required: stability and sensitivity

(a) Unstable and sensitive  (b) Stable and insensitive
Required: stability and sensitivity

(a) Unstable and sensitive  (b) Stable and insensitive  (c) Stable and sensitive
Adaptive Authentication

- **Registration phase**
  - Collect models for different screen settings
  - Train authentication classifiers (SVM)

- **Authentication phase**
  - Switch screen settings randomly
  - Match touch behavior against trained profile
  - Trigger hard authentication on mismatch
Evaluation
User study

- Two “comparison” games,
  - Swipe horizontally to find errors in 2 images
  - Scroll vertically to compare geometric shapes
Two “comparison” games,
- Swipe horizontally to find errors in 2 images
- Scroll vertically to compare geometric shapes

25 users evaluated in study
- Measure touch interactions with different distortion settings
- 0.8, 0.9, 1.0, 1.1, 1.2 along X and Y axis
User study: stability

Touch behaviors of a user in one setting are closer to those of the user in another setting than those of other users.
User study: sensitivity

A user's touch strokes in different settings have a high degree of separability in the feature space.
Two (robot-based) attacks

• Random attack: an attacker replays a random user's touch data (i.e., the naïve attack)

• Targeted attack: an attacker replays the targeted user's touch data (i.e., attacker has access to full training data)
## EER*s in different settings

<table>
<thead>
<tr>
<th></th>
<th>Random attacks</th>
<th>Targeted attacks</th>
</tr>
</thead>
<tbody>
<tr>
<td>S-Baseline-a</td>
<td>0.12 (0.1067)</td>
<td>0.50 (0.0000)</td>
</tr>
<tr>
<td>S-Baseline-b</td>
<td>0.11 (0.0819)</td>
<td>0.50 (0.0000)</td>
</tr>
<tr>
<td>S-Baseline-c</td>
<td>0.14 (0.1111)</td>
<td>0.50 (0.0000)</td>
</tr>
<tr>
<td>S-Baseline-d</td>
<td>0.14 (0.1051)</td>
<td>0.50 (0.0000)</td>
</tr>
<tr>
<td>S-Baseline-e</td>
<td>0.17 (0.1187)</td>
<td>0.50 (0.0000)</td>
</tr>
<tr>
<td>S-Baseline-improved</td>
<td>0.12 (0.0777)</td>
<td>0.45 (0.0364)</td>
</tr>
<tr>
<td>S-ATCA</td>
<td><strong>0.08 (0.0542)</strong></td>
<td><strong>0.33 (0.0502)</strong></td>
</tr>
</tbody>
</table>

* EER: Equal Error Rate, equilibrium of false acceptance and false rejection rates
* ATCA: Adaptive Touch-based Continuous Authentication
More screen settings help
Attacking TouchAlytics

- Detect screen setting
  - Measure “swipe” distance and leak screen setting
  - Still leaves some strokes unprotected
Conclusion
Conclusion

- Users subconsciously adapt behavior, different screen settings do not affect user experience
- Adaptive touch-based continuous authentication randomly changes screen settings to fool attacks
- (Small) user study shows promising results
- Touch behavior is both stable and sensitive
- Future work: larger study, more screen settings, leverage sloppiness and jitter
Thank you!

Questions?

Mathias Payer, Purdue University
http://hexhive.github.io