Preventing Lunchtime Attacks: Fighting Insider Threats With Eye Movement Biometrics

Simon Eberz, Kasper B. Rasmussen, Vincent Lenders, Ivan Martinovic

Department of Computer Science
University of Oxford, UK

Armasuisse, CH

Threat Model

- Typical scenario: “Lunchtime Attack”
  - Attacker uses a co-worker's unlocked workstation while he is at lunch
- Other scenarios
  - Cleaning staff access workstation after hours
  - Compromised, or even wilfully shared password
- Insider threats are a significant problem:
  - 33% of electronic crimes committed by insiders
  - 60% of those involve a compromised account
  - 43% are performed locally, using physical access to the workstation
Why Eye Movements?

Pitt Early Autism Study for Infants

Market Research

Gaze-Based PIN entry, De Luca et al., 2007
Eyetracking prototype for the PS4

Introduction to Eye Tracking

- Several types of trackers
  - Eye-attached
  - Electric potential measurement
  - Video-Based
Research Questions

- What kind of eye movements have been identified in related work?
- Can we derive biometric features from these movements?
- Are they useful for transparent continuous authentication?
- Are the features stable over time?
- How quickly can imposters be detected?
- How likely are false positives?

Different Types of Eye Movements

The quick brown fox
Different Types of Eye Movements

Raw Gaze Sample

The quick brown fox

Gaze Fixations

Fixation Center
Different Types of Eye Movements

- Gaze Fixations
- Saccades
- Microsaccade
- Fixation Center

The quick brown fox
### Discriminative Features

#### Spatial Features

- Pupil Diameter

#### Temporal Features

- Pupil Diameter

<table>
<thead>
<tr>
<th>Feature</th>
<th>BMI</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Spatial features</strong></td>
<td></td>
</tr>
<tr>
<td>Distance from Center - Max</td>
<td>1.3%</td>
</tr>
<tr>
<td>Distance from Center - Mean</td>
<td>2.52%</td>
</tr>
<tr>
<td>Distance from Center - Min</td>
<td>0.72%</td>
</tr>
<tr>
<td>Distance from Saccade</td>
<td>1.23%</td>
</tr>
<tr>
<td>Distance from previous fixation</td>
<td>0.64%</td>
</tr>
<tr>
<td>Min Pupil Area Distance</td>
<td>1.25%</td>
</tr>
<tr>
<td>Min Pupil Area Distance X only</td>
<td>1.06%</td>
</tr>
<tr>
<td>Min Pupil Area Distance Y only</td>
<td>0.84%</td>
</tr>
<tr>
<td>Saccade Direction</td>
<td>0.08%</td>
</tr>
<tr>
<td><strong>Temporal features</strong></td>
<td></td>
</tr>
<tr>
<td>Acceleration - Max</td>
<td>2.49%</td>
</tr>
<tr>
<td>Acceleration - Mean</td>
<td>0.35%</td>
</tr>
<tr>
<td>Duration of Fixation</td>
<td>1.09%</td>
</tr>
<tr>
<td>Pupil Diameter - Max</td>
<td>4.99%</td>
</tr>
<tr>
<td>Pupil Diameter - Mean</td>
<td>5.36%</td>
</tr>
<tr>
<td>Pupil Diameter - Min</td>
<td>1.77%</td>
</tr>
</tbody>
</table>

#### Pupil Diameter

- Pupil diameter can be influenced through light stimulation

- Herbst et al., 2011

- Is reliable authentication possible without using this feature?
Study Design

Session 1  
30 subjects  
2 weeks

Session 2  
20 subjects  
1 hour

Session 3  
20 subjects

Long-term stability

Technical Artefacts

Classification Methodology

- Two classifiers
  - K-nearest neighbors
  - Support Vector Machines
- 5-fold stratified cross-validation
- Sliding window of size n

n samples
Tradeoffs

Results – Single Session

Session 1  Session 2  Session 3

2 weeks  1 hour

Full Featureset
Without pupil diameter

Equal Error Rate (EER)

Without pupil diameter
~15%

All features
~4%
Results

Session 1  2 weeks  Session 2  1 hour  Session 3

Equal Error Rate (EER)

- Full Featureset
- Without pupil diameter

Without Pupil diameter
14% [-1%]

All Features
6% [+2%]

Results – Over Two Weeks

Session 1  2 weeks  Session 2  1 hour  Session 3

Equal Error Rate (EER)

- Full Featureset
- Without pupil diameter

Without pupil diameter
16% [+1%]

All features
7.5% [+3.5%]
Results – Practical Performance

Time to Reject, n=180 t=18

- Attackers
- Legitimate Users

Time to Detection [s]
Cumulative Probability

0.0 0.2 0.4 0.6 0.8 1.0
0 10 20 30 40 50 60 70 80 90

Results – Practical Performance

Time to Reject, n=80 t=3

- Attackers
- Legitimate Users

Time to Detection [s]
Cumulative Probability

0.0 0.2 0.4 0.6 0.8 1.0
0 20 40 60 80 100 120 140 160 180

Simon Eberz, Preventing Lunchtime Attacks: Fighting Insider Threats With Eye Movement Biometrics
Machine Learning and Security

- What could possibly go wrong?

**Biometrics are not secrets!**

---

Machine Learning and Security

- Problem: Replay attacks
  - Solution: Timestamp and sign data
- Problem: Manual imitation attacks
### Manual Imitation Attacks

<table>
<thead>
<tr>
<th>Character</th>
<th>t</th>
<th>b</th>
<th>s</th>
<th>o</th>
<th>u</th>
<th>R</th>
<th>z</th>
</tr>
</thead>
<tbody>
<tr>
<td>Target time (ms)</td>
<td>20.66</td>
<td>20.03</td>
<td>20.49</td>
<td>20.48</td>
<td>20.48</td>
<td>20.49</td>
<td>20.48</td>
</tr>
<tr>
<td>User time (ms)</td>
<td>20.66</td>
<td>20.03</td>
<td>20.49</td>
<td>20.48</td>
<td>20.48</td>
<td>20.49</td>
<td>20.48</td>
</tr>
<tr>
<td>Penalty</td>
<td>2.57</td>
<td>2.46</td>
<td>2.18</td>
<td>2.16</td>
<td>2.17</td>
<td>2.16</td>
<td>2.18</td>
</tr>
</tbody>
</table>

Tey et al., NDSS 2013

### Machine Learning and Security

- **Problem:** Replay attacks
  - Solution: Timestamp and sign data
- **Problem:** Manual imitation attacks
  - Solution: Use features that are hard to imitate
- **Problem:** Automatic imitation attacks
Automatic Imitation Attacks

Serwadda et al., CCS 2014

Machine Learning and Security

- Problem: Replay attacks
  - Solution: Timestamp and sign data
- Problem: Manual imitation attacks
  - Solution: Use features that are hard to imitate
- Problem: Automatic imitation attacks
  - Solution: Liveness detection
Conclusion

- A new biometric based on eye movements
- High distinctiveness
- Remarkably stable over time
- But: Tricky to make a *system* secure

Future Work
- What about low-cost devices?
- Practical considerations

Conclusion – Questions?

- A new biometric based on eye movements
- High distinctiveness
- Remarkably stable over time
- But: Tricky to make a *system* secure
- Future Work
  - What about low-cost devices?
  - Practical considerations

Thank you for your attention. Questions?
simon.eberz@cs.ox.ac.uk