PassFrame: Generating Image-based Passwords from Egocentric Videos

Introduction
We propose an approach to generate always-fresh, temporal and personalized passwords from images captured by a wearable camera (w/o eye tracking data).

PassFrame: Generating Image-based Passwords from Egocentric Videos
Using scene segmentation and clustering, we implement two password formats: **image-arrangement** and **image-selection**.

**Image-arrangement**
- Head-mounted camera was used.
- Users interact with objects in an office, then arrange 4 images in the right order.
- A new password appears if a wrong arrangement is submitted.
- Attackers know the layout of the office but not the activity order
  - Attackers’ effort is higher than that of the legitimate users.

<table>
<thead>
<tr>
<th>User</th>
<th>Attacker</th>
</tr>
</thead>
<tbody>
<tr>
<td>Entry time (s)</td>
<td>9.77 (5.00)</td>
</tr>
<tr>
<td># attempts</td>
<td>1.21 (0.66)</td>
</tr>
</tbody>
</table>

**Image-selection**
- Chest-mounted camera was used.
- Users wear the camera daily, then select images satisfying a condition.
- We randomize the number of images and the ratio of valid images.

![Diagram of image-arrangement and image-selection](image-url)