Seamless and Secure VR

Adapting and Evaluating Established Authentication Systems for Virtual Reality

Ceenu George, Mohamed Khamis, Emanuel von Zezschwitz, Marinus Burger, Henri Schmidt
Florian Alt, Heinrich Hussmann
LMU Munich, Media Informatics Group, Germany
Seamless authentication in VR environments can solve practical security problems without reducing usability.
Growing interest in VR consumer products
Use cases for authentication in VR have already been established.

Virtual online shopping - Confirming an Order

Social Applications - Signing In
Head mounted displays (HMDs) are ubiquitous devices, striving towards being wireless. 

Device becomes self contained

No external display or keyboard

Need for seamless authentication, without taking the headset off
VR experiences differ from previous research on observation-resistant authentication

No visual cues of the input interface for real world observers

Mid-air interactions are observable from the real world

Fully immersed users do not notice observers
Threat Model

The victim is using VR with friends and family around

Attackers have perfect sight on victims’ hand movements

Attacker cannot see what the user sees in the HMD
Threat Model

Unlike shoulder surfing in the real world, the attacker in our threat model cannot be seen by the user.

The victim authenticates with PIN and pattern in order to complete an in-app purchase.

Immediately after authenticating, she takes off the headset in order to step out for a break.

The attacker picks up the headset, continues playing the game and when prompted authenticates for another in-app purchase with the victim's password.
Two main metaphors influence VR interaction

**Virtual Hand**
‘Tapping’ Objects to interact

**Virtual Pointer**
Using a ‘Laser Pointer’ to interact
HTC Vive Controllers have the same look and feel in the virtual and real world

Real world

Virtual representation

Controller buttons used for interaction
Transferring well established methods from the real world into virtual reality

Personal Identification Number

Android Unlock Patterns
We built upon the existing usable security research to create a design space for VR.
Our design space included four Input Modalities

1. Large/Pointer
2. Medium/Pointer
3. Medium/Tap
4. Small Stylus/Tap
Four Input Modalities

- Large/Pointer
- Medium/Pointer
- Medium/Tap
- Small Stylus/Hybrid
1. “Large/Pointer”
Four Input Modalities

Large/Pointer

Medium/Pointer

Medium/Tap

Small Stylus/Hybrid
“Medium/Pointer”
Four Input Modalities

- Large/Pointer
- Medium/Pointer
- Medium/Tap
- Small Stylus/Hybrid
“Medium/Tap”
Four Input Modalities

- Large/Pointer
- Medium/Pointer
- Medium/Tap
- Small Stylus/Hybrid
“Small Stylus/Tap”
Main study was completed in two parts

1. **Usability**

Participants use the system to enter passwords. We log how fast they enter the passwords and how many mistakes they make.

2. **Security**

Participants observe the experimenter using the system. Can they replicate the passwords entered?
## Usability Study - Variables

### Independent Variables
- Password Type
- Input Modality

### Dependent Variables
- Authentication Time
- Errors
- Perceived Ease of Use

![Study Environment](image)
## Security Study - Variables

<table>
<thead>
<tr>
<th>Independent Variables</th>
<th>Dependent Variables</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Password Type</td>
<td>• Binary Success Rate</td>
</tr>
<tr>
<td>• Input Modality</td>
<td>• Relative Success Rate</td>
</tr>
<tr>
<td></td>
<td>• Perceived Security</td>
</tr>
</tbody>
</table>
Usability – Entry time results

Overall averages across all input modalities:
- Pin: 2.7s
- Pattern: 3.2s
→ significant difference (p<0.001)

Medium/Tap performed significantly worse than all other input modalities (p<0.001)
Security - Results

18% out of 400 entered passwords were guessed correctly

Pointer conditions performed **significantly** better than tapping

Medium/Tap showed **significantly (p<0.05)** worse shoulder surfing resistance compared to all other conditions

The most secure modality for both PIN and Pattern input was Large/Pointer
Usability and Security – Perception results

Medium/Pointer was perceived to be significantly ($p<0.001$) more secure and usable than Medium/Tap (before and after study completion)
Conclusion

PIN and Pattern capable for VR application

Virtual pointer outperforms virtual tap for authentication purposes

Possibly more secure than mobile device authentication as attacker has no visual feedback of input surface

Seamless authentication in VR environments can solve practical security problems without reducing usability
Future Work

**Next step** would be

Combining our insights on interaction styles to create a [graphical] password space for VR.

Combining the secret channel provided by HMDs and the new password space to generate VR specific password schemes.

VR authentication option I

VR authentication option II
Thank you

Seamless authentication in VR environments can solve practical security problems without reducing usability

{ ceenu.george, mohamed.khamis, emanuel.von.zezschwitz, florian.alt, heinrich.hussmann}@ifi.lmu.de
{ h.schmidt, marinus.burger}@campus.lmu.de
Password Properties: PIN

Transformability

- Two types of password sets were used in Security Study:
  - Transformable and non-transformable PINs
- Transformability was originally intended for classification of easy/hard-to-guess PINs
- Transformability often comes along with
  - consecutive
  - repeated
  - neighboring digits
Password Properties: Pattern

[A] Knight move: A connection between two points that are not immediate neighbors

[B] Intersection: The crossing of one or more lines.

[C] Overlap: A line that crosses a point that has already been activated as part of another line

[D] Transformability: The pattern can be drawn in multiple positions on the grid
Conclusions Pattern

- Only **Touch** input has significant drawbacks (30% slower, ~half as secure)

- **Large Pointer** and **Handheld** lead in popularity (Combining 13 / 15 Votes)

- **Large Pointer** is most secure (6% attack success vs. 15% hand)

- **Large Pointer** generates fewer errors (0.083 Errors / Entry vs. 0.153)

- Entry times comparable to smartphone (3.2 excl. Touch vs. Harbach et al. 3.0s, von Zezschwitz et al. 3.1s)

- Security is potentially improved (overall binary success-rate of 14.58%, given 3 guesses compared to i.e. Zakaria et al, 19% with shielding, one guess)
References

http://store.steampowered.com/app/447270/

https://www.facebook.com/zuck/videos/10103154531425531/

“Bendy” - Figure © by Valve, https://support.steampowered.com/steamvr/HTC_Vive/

1, 2 - Mark Mine et al. Virtual environment interaction techniques. UNC Chapel Hill


SuperDataThere are several other news site reporting or projecting similar numbers (werables.com, forbes.com, businessinsider.com).

P. Lee, D J. Maida.

https://www.vive.com/us/pr/newsroom-gallery/