Secure Multi-User Content Sharing for Augmented Reality Applications

Kimberly Ruth, Tadayoshi Kohno, Franziska Roesner

University of Washington
Emerging AR/MR Technologies
Emerging AR/MR Technologies

Technologies that *continuously process sensory input* from the user’s surroundings and *overlay digital content* on top of the user’s perception of the world.
AR Security Research Context

Sensory Input → AR App → Digital Output
AR Security Research Context

[Raw Input] → [Trusted Input Module] → [Filtered Input] → [AR App] → [Digital Output]

[Jana, Molnar, Moshchuk, Dunn, Livshits, Wang, & Ofek, 2013]
[Roesner, Molnar, Moshchuk, Kohno, & Wang, 2014]
[Templeman, Korayem, Crandall, & Kapadia, 2014]
[Raval, Srivastava, Razeen, Lebeck, Machanavajjhala, & Cox, 2016]
AR Security Research Context

Raw Input → Trusted Input Module → Filtered Input → App Outputs → Trusted Output Module → Constrained Visual Output

[Jana, Molnar, Moshchuk, Dunn, Livshits, Wang, & Ofek, 2013]
[Roesner, Molnar, Moshchuk, Kohno, & Wang, 2014]
[Templeman, Korayem, Crandall, & Kapadia, 2014]
[Raval, Srivastava, Razeen, Lebeck, Machanavajjhala, & Cox, 2016]

[Lebeck, Kohno, & Roesner, 2016]
[Lebeck, Ruth, Kohno, & Roesner, 2017]
[Ahn, Gorlatova, Naghizadeh, Chiang, & Mittal, 2018]
Amazing new technology…

… what could possibly go wrong?
John Doe: This is a reminder that your credit card payment is overdue.
John Doe:
This is a reminder that your credit card payment is overdue.

Private content is publicly visible

Virtual vandalism
John Doe: This is a reminder that your credit card payment is overdue.

Private content is publicly visible

Virtual vandalism

Violation of user's personal space

↓ KICK ME
John Doe:
This is a reminder that your credit card payment is overdue.

- Private content is publicly visible
- Virtual vandalism
- Unwanted virtual content
- Violation of user’s personal space

↓ KICK ME
Precursors Today

In VR:

● Sexual harassment occurs between player avatars
● Offensive remarks and standing in personal space is a meme
Precursors Today

In VR:

- Sexual harassment occurs between player avatars
- Offensive remarks and standing in personal space is a meme

In smartphone AR:

- Virtual “Balloon Dog” sculpture vandalized in Snapchat
- Unauthorized AR content in MoMA Picasso exhibit
Goal: Design multi-user AR security and privacy primitives
Case Studies as Design Development Tool
Case Studies as Design Development Tool

Opt-in, co-located: Paintball
Case Studies as Design Development Tool

Opt-in, co-located: **Paintball**

Opt-in, not co-located: **Multi-Team Whiteboards**
Case Studies as Design Development Tool

Opt-in, co-located: Paintball

Opt-in, not co-located: Multi-Team Whiteboards

Opt-out, co-located: Community Art
Threat Model

Scope: multiple users of a single application
Untrustworthy users may attempt to:
Threat Model

Scope: multiple users of a single application
Untrustworthy users may attempt to:

1. **Share unwanted AR content** with other users
Threat Model

Scope: multiple users of a single application
Untrustworthy users may attempt to:

1. **Share unwanted AR content** with other users
2. **See private AR content** belonging to another user
Threat Model

Scope: multiple users of a single application
Untrustworthy users may attempt to:

1. **Share unwanted AR content** with other users

2. **See private AR content** belonging to another user

3. **Perform unwanted manipulations on AR content** belonging to another user
Goal: Design multi-user AR security and privacy primitives that protect users from each other
Goal: Design *functionality-friendly* multi-user AR security and privacy primitives that protect users from each other.
One Size Does Not Fit All

KICK ME vs.
One Size Does Not Fit All

- Both involve attaching virtual content to users
One Size Does Not Fit All

- Both involve attaching virtual content to users
- Bad vs. good is dependent on application semantics
One Size Does Not Fit All

• Both involve attaching virtual content to users
• Bad vs. good is dependent on application semantics
• Cannot distinguish these in a general-purpose solution

↓ KICK ME
Goal: Design functionality-friendly multi-user AR security and privacy primitives that *help developers* to protect users from each other
Goal: Design *functionality-friendly* multi-user AR security and privacy primitives that *help developers to protect users from each other*
Approach: App-Level Developer Toolkit

- Benefit: packaging controls behind an API reduces developer burden
- Benefit: lack of reliance on OS support facilitates ease of deployment in practice
- Benefit: opens possibility of cross-platform compatibility
- Limitation: cannot protect against misuse or abuse by app developer
Design Components

<table>
<thead>
<tr>
<th></th>
<th>Outbound sharing controls</th>
<th>Inbound sharing controls</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>What and with whom?</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Where?</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>How much?</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Outbound sharing controls</td>
<td>Inbound sharing controls</td>
</tr>
<tr>
<td>---------------------------</td>
<td>---------------------------</td>
<td>--------------------------</td>
</tr>
<tr>
<td><strong>What and with whom?</strong></td>
<td>Permission management</td>
<td>Two-party sharing consent</td>
</tr>
<tr>
<td><strong>Where?</strong></td>
<td>Location coupling</td>
<td>Personal space</td>
</tr>
<tr>
<td><strong>How much?</strong></td>
<td>Private content in a shared world</td>
<td>Clutter management</td>
</tr>
</tbody>
</table>
## Design Components

<table>
<thead>
<tr>
<th></th>
<th>Outbound sharing controls</th>
<th>Inbound sharing controls</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>What and with whom?</strong></td>
<td>Permission management</td>
<td>Two-party sharing consent</td>
</tr>
<tr>
<td><strong>Where?</strong></td>
<td>Location coupling</td>
<td>Personal space</td>
</tr>
<tr>
<td><strong>How much?</strong></td>
<td>Private content in a shared world</td>
<td>Clutter management</td>
</tr>
</tbody>
</table>

Key challenge: integration with physical 3D space
### Design Components

<table>
<thead>
<tr>
<th>What and with whom?</th>
<th>Outbound sharing controls</th>
<th>Inbound sharing controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>Where?</td>
<td>Location coupling</td>
<td>Personal space</td>
</tr>
<tr>
<td>How much?</td>
<td>Private content in a shared world</td>
<td>Clutter management</td>
</tr>
</tbody>
</table>

**Key challenge:** integration with physical 3D space
Problem: Private Content in a Shared World

John Doe: This is a reminder that your credit card payment is overdue.
Problem: Private Content in a Shared World

Left user’s view: virtual content obscured

John Doe:
This is a reminder that your credit card payment is overdue.
Problem: Private Content in a Shared World

Left user’s view: virtual content obscured

Right user’s view: no behavioral cue

John Doe: This is a reminder that your credit card payment is overdue.
Problem: Private Content in a Shared World

Left user’s view: virtual content obscured
Right user’s view: no behavioral cue

John Doe: This is a reminder that your credit card payment is overdue.
Solution: Ghosting

User’s view:

John Doe: This is a reminder that your credit card payment is overdue.

Others’ view:
Solution: Ghosting

Left user’s view: full virtual content

Right user’s view: behavioral cue

John Doe: This is a reminder that your credit card payment is overdue.
Implementation: ShareAR

- App-level library written for Microsoft HoloLens
- Assumes Unity development environment
- Network shim layer uses Microsoft MixedRealityToolkit Sharing; can be swapped out to use another networking solution
Evaluation

1. Analysis of compatibility with existing design recommendations
Evaluation

1. Analysis of compatibility with existing design recommendations
2. Construction of representative case study applications
Evaluation

1. Analysis of compatibility with existing design recommendations

2. Construction of representative case study applications
Evaluation

1. Analysis of compatibility with existing design recommendations

2. Construction of representative case study applications

3. Assessment of case study applications’ security properties
Evaluation

1. Analysis of compatibility with existing design recommendations
2. Construction of representative case study applications
3. Assessment of case study applications’ security properties
4. Performance measurement, scaling with number of users and number of objects
Evaluation

Continued evaluation in practice:

- 2 undergraduates this summer building apps using ShareAR
- Toolkit available for other developers and researchers to download; looking for further feedback from practical use
- Visit arsharingtoolkit.com to try it out
Summary

Multi-user AR security is a topic that warrants the attention of the security community.

Security is not enough: practicality requires building security solutions based on functionality requirements.

This work contributes:
- A set of goals for a multi-user AR security framework,
- A design that meets those goals, and
- An implementation that helps multi-user AR app developers in practice to achieve functionality and security.
Acknowledgements

Franziska Roesner
Tadayoshi Kohno
Henry Bowman
Security and Privacy Lab

Project website: arsharingtoolkit.com

Questions? Kimberly Ruth – kcr32@cs.washington.edu