



# Undergraduate Research Symposium May 17, 2019 Mary Gates Hall

## Online Proceedings

### SESSION 1R

#### COMPUTER SECURITY, PRIVACY, ACCESSIBILITY, AND GRAPHICS

*Session Moderator: Franziska Roesner, Computer Science and Engineering*

**JHN 026**

*12:30 PM to 2:15 PM*

\* Note: Titles in order of presentation.

##### **Analysis of the Susceptibility of Smart Home Interfaces to End User Error**

*Mitali Vishwesh Palekar, Senior, Computer Science  
UW Honors Program*

*Mentor: Franziska Roesner, Computer Science and Engineering*

*Mentor: Earlence Fernandes, CSE*

Trigger-action platforms enable end-users to program their smart homes using simple conditional rules of the form: if condition then action. Although these rules are easy to program, subtleties in their interpretation can cause users to make errors that have consequences ranging from incorrect and undesired functionality to security and privacy violations. Based on prior work, we enumerate a set of nine error classes that users can make, and we empirically study the relationship between these classes and the interface design of eight commercially available trigger-action platforms. Particularly, we examine whether each interface prevents (e.g., via good design) or allows each class of error. Based on this analysis, we develop a framework to classify errors and extract insights that lay a foundation for the design of future trigger-action programming interfaces where certain classes of errors can be mitigated by technical means or by alerting the user to the possibility of an error. For instance, we identify that an analysis of a dataset of functionally-similar trigger-action rules could be used to predict whether certain types of error patterns are about to occur. We believe that this work is a first step towards trigger-action interface designs that significantly mitigate user error.

### SESSION 1R

#### COMPUTER SECURITY, PRIVACY, ACCESSIBILITY, AND GRAPHICS

*Session Moderator: Franziska Roesner, Computer Science and Engineering*

**JHN 026**

*12:30 PM to 2:15 PM*

\* Note: Titles in order of presentation.

##### **Secure Multi-User Content Sharing for Augmented Reality Applications**

*Kimberly Christine Ruth, Senior, Computer Engineering, Mathematics*

*Goldwater Scholar, Mary Gates Scholar, UW Honors Program, Washington Research Foundation Fellow*

*Mentor: Franziska Roesner, Computer Science and Engineering*

*Mentor: Tadayoshi Kohno, Computer Science and Engineering*

Augmented reality (AR) for the consumer market is gaining momentum and public attention. Besides smartphone platforms, early-stage head-mounted displays such as the Microsoft HoloLens are now publicly available. Many compelling uses of these AR technologies are multi-user: for instance, in-person collaborative tools, multiplayer gaming, and telepresence. Although multi-user AR technologies enable new forms of interaction, they also raise new security and privacy challenges, not only from untrusted applications but also from other users' malicious or unthinking behavior. It is imperative that these challenges be addressed while the technology is still new and highly malleable. In this work, I explore emerging challenges in securing multi-user AR content sharing from user-to-user threats. I argue that supporting secure and private AR content sharing when users can augment each other's reality requires careful consideration of AR's tight integration with the physical world. I systematize design goals for security and functionality that an AR content sharing module should support, and I design and prototype an application-level module for the HoloLens that meets these goals. By evaluating my module against representative application case studies, I show that it meets desired security and functionality goals flexibly across a range of use cases. I further demonstrate that applications' content sharing needs can

be achieved in relatively few lines of code and with low performance overhead. I am currently converting my research prototype into an open-source toolkit so that developers can address these challenges in practice. This work opens up directions for future research on supporting developers in effectively addressing these issues in practice, including making recommendations on how these underlying paradigms should manifest in user interface design. By building foundations for secure multi-user AR content sharing, my work takes steps toward allowing AR to securely reach its full potential.