Extending AR Authoring Tools with Built-in Support for Privacy and Security Analysis

Shwetha Rajaram
University of Michigan
shwethar@umich.edu

Michael Nebeling
University of Michigan
nebeling@umich.edu

ABSTRACT

Augmented reality (AR) experiences are becoming much easier to create due to a growing number of novice-friendly design tools that lower the technical barrier to entry. However, critically evaluating design concepts with respect to safety, privacy, and security often still requires significant technical knowledge and domain expertise. We discuss our vision for integrating built-in support with AR authoring tools for analyzing potential privacy and security harms and suggesting design revisions to mitigate these harms.

CCS CONCEPTS

• **Human-centered computing** → **Interface design prototyping**; **Mixed / augmented reality**; • **Security and privacy / Privacy protections**;

KEYWORDS

augmented reality, authoring tools

ACM Reference Format:
Shwetha Rajaram and Michael Nebeling. 2022. Extending AR Authoring Tools with Built-in Support for Privacy and Security Analysis. In *CHI Conference on Human Factors in Computing Systems (CHI '22), April 29-May 5, 2022, New Orleans, LA, USA.* ACM, New York, NY, USA, 2 pages.

1 INTRODUCTION

The HCI community has dedicated significant research towards enabling novice designers to create AR experiences. Prior work has contributed a large body of authoring tools which lower the technical barrier to entry for novice creators by capitalizing on designers' familiar skills, e.g., leveraging physical prototyping with paper and play-doh to enable creation of 3D content [8, 9] and incorporating video editing techniques to implement interactions without the need for programming [5, 6]. Higher fidelity tools simplify the development effort required to make use of AR devices' unique input and output capabilities, including utilizing depth capture information [7], recognizing hand gestures [11], and performing rendering techniques like occlusion and light estimation [3].

While creating AR experiences is becoming increasingly approachable for novice designers, significant domain expertise is still needed to more holistically evaluate design concepts, e.g., with respect to safety and accessibility. In particular, assessing privacy & security implications of AR experiences often requires a technical understanding of AR devices' capabilities including environmental tracking mechanisms, common interaction modalities and the types of data they rely on, and rendering techniques [10]; knowledge of established privacy & security laws involving biometric data collection and informed consent is also essential.

To lower the barrier to entry for novice creators to critically evaluate their design concepts, we are currently investigating how to best extend existing AR authoring toolkits with built-in support to identify potential privacy & security harms in prototypes and formulate mitigation strategies. A key challenge with designing such a tool is automating the process of educating designers to analyze potential threats that their design concepts may raise, assuming that they may not have prior training in privacy & security. We take inspiration from prior work in developing educational games to inform novice technologists about privacy & security issues [2], but are particularly interested in how to dynamically identify risks and propose design revisions based on a semantic understanding of a designer's prototype. In this position paper, we discuss opportunities and open questions raised in our ongoing work, including the difficulty of applying existing privacy & security guidelines to lower-fidelity AR prototypes and balancing requirements of traditional prototyping tools (e.g., efficiency and expressive leverage) with new requirements that an automated analysis of risks may introduce.

2 INTEGRATING SUPPORT FOR AR RISK ANALYSIS IN AUTHORING TOOLS

We are currently exploring how AR authoring tools can provide built-in support for designers to *(1)* analyze their prototypes and identify potential privacy and security risks which could arise in various usage scenarios, and *(2)* implement design revisions to mitigate these risks, following design guidelines from industry and academic research. We believe that offering designers a means to critically analyze their prototypes within an authoring tool itself will help to place safety considerations at the forefront of designers' workflows and provide support to smaller or less experienced design teams, who may not have access to privacy & security experts to facilitate a risk assessment. In this section, we discuss two main challenges encountered in our work thus far:

Determining the "right" stage of prototyping to incorporate privacy & security design guidelines. Following established frameworks like Privacy by Design [1], privacy & security should ideally be prioritized as a design goal in the earliest stages of prototyping. However, from conducting an initial review of AR privacy & security guidelines from five XR vendors, two non-profit organizations, and three research studies, we find that many existing guidelines are not easily transferable to prototyping tools, as they

CHI EA '22, Proceedings of the 1st Workshop on Novel Challenges of Safety, Security and Privacy in Extended Reality, April 29-May 5, 2022, New Orleans, LA, USA

offer overly technical advice which may not be achievable during lower-fidelity prototyping or provide abstract suggestions on how to implement the design principles. For example, Microsoft's design guidelines[1] for rendering holograms with sufficient brightness and transparency to promote physical safety may only feel relevant in high-fidelity prototyping stages, after designers have explored basic content layouts and interactions through physical prototyping. Guidelines to adopt data minimization policies and obtain informed consent from users can provide designers with guidance in deciding which AR interaction modalities to utilize, but leave ambiguity in how the consent interface should be designed and when it should be presented to users.

To inform the design of an authoring tool capable of assessing prototypes with respect to privacy & security recommendations, we are continuing to analyze existing AR design guidelines alongside examples of low to high fidelity prototypes from novice designers. Through our analysis, we hope to refine and adapt these existing recommendations to create a "test suite" of guidelines which we can use to identify potential risks within AR prototypes and measure the extent to which they are addressed.

Balancing tradeoffs between the authoring tool's usability, expressive leverage, and intelligence in suggesting privacy & security improvements. Another challenge is how to preserve important requirements for traditional authoring tools (e.g., enabling designers to efficiently and fully express their design concepts with minimal effort [4]) while integrating automated assistance for analyzing potential risks and implementing design revisions, which requires the system to gain semantic understanding of the AR prototype and corresponding usage contexts. For example, to identify privacy risks for bystanders, the authoring tool may need to distinguish between physical and virtual objects in the designers' prototype, simulate how the user would navigate in a specific environment (e.g., outdoors or in a classroom), and understand other types of AR users or non-users who may be present; asking designers to depict all of this information in their prototypes could be inefficient and disrupt their creative processes.

One approach to balance usability and system intelligence is providing a library of 3D assets and simulation environments (similar to Unity MARS[2]) which are pre-labeled to give the system semantic understanding of any prototype created; however, this approach could limit designers' ability to express a wide range of design concepts. We are also exploring how to leverage human intelligence in automating the risk analysis. Inspired by the popular game Among Us[3], we envision pairing two AR creators to collaboratively prototype, with one working in a designer role to build an AR scene, and the other working in an "adversary" role to sabotage the prototype by injecting gamified characters which represent specific privacy & security threats.

3 CONTRIBUTION TO THE WORKSHOP

Through participating in the SSPXR Workshop at CHI 2022, we hope to share our insights from this ongoing work with other participants, particularly regarding the challenges with integrating automated support for AR risk assessments in authoring tools, which we are working to address. From other workshop participants, we hope to learn about novel approaches to making XR experiences more safe for various stakeholders and engage in broader discussions around best practices for integrating concrete design recommendations in XR creators' workflows.

4 AUTHORS' BACKGROUNDS

Shwetha Rajaram is a PhD student at the University of Michigan School of Information, where she studies XR design & development tools and how to make XR systems more privacy-friendly for users. Michael Nebeling is an Assistant Professor at the University of Michigan School of Information, where his HCI research lab focuses on XR systems design. He created low-fidelity and immersive XR authoring tools, often with a focus on rapid prototyping. With Shwetha, he is currently exploring ways of eliciting privacy design considerations and incorporating them into XR design processes.

REFERENCES

[1] Ann Cavoukian. 2010. Privacy by Design: The 7 Foundational Principles. Revised: October 2010.

[2] Tamara Denning, Adam Lerner, Adam Shostack, and Tadayoshi Kohno. 2013. Control-Alt-Hack: The Design and Evaluation of a Card Game for Computer Security Awareness and Education. In *Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security* (Berlin, Germany) *(CCS '13)*. Association for Computing Machinery, New York, NY, USA, 915–928. https://doi.org/10.1145/2508859.2516753

[3] Ruofei Du, Eric Turner, Maksym Dzitsiuk, Luca Prasso, Ivo Duarte, Jason Dourgarian, João Afonso, Jose Pascoal, Josh Gladstone, Nuno Cruces, Shahram Izadi, Adarsh Kowdle, Konstantine Tsotsos, and David Kim. 2020. DepthLab: Real-time 3D Interaction with Depth Maps for Mobile Augmented Reality. In *UIST '20: The 33rd Annual ACM Symposium on User Interface Software and Technology, Virtual Event, USA, October 20-23, 2020*. ACM, 829–843. https://doi.org/10.1145/3379337.3415881

[4] Dan R. Olsen Jr. 2007. Evaluating user interface systems research. In *Proceedings of the 20th Annual ACM Symposium on User Interface Software and Technology, Newport, Rhode Island, USA, October 7-10, 2007*. ACM, 251–258. https://doi.org/10.1145/1294211.1294256

[5] Germán Leiva and Michel Beaudouin-Lafon. 2018. Montage: A Video Prototyping System to Reduce Re-Shooting and Increase Re-Usability. In *The 31st Annual ACM Symposium on User Interface Software and Technology, UIST 2018, Berlin, Germany, October 14-17, 2018*. ACM, 675–682. https://doi.org/10.1145/3242587.3242613

[6] Germán Leiva, Cuong Nguyen, Rubaiat Habib Kazi, and Paul Asente. 2020. Pronto: Rapid Augmented Reality Video Prototyping Using Sketches and Enaction. In *CHI '20: CHI Conference on Human Factors in Computing Systems, Honolulu, HI, USA, April 25-30, 2020*. ACM, 1–13. https://doi.org/10.1145/3313831.3376160

[7] Leon Müller, Ken Pfeuffer, Jan Gugenheimer, Bastian Pfleging, Sarah Prange, and Florian Alt. 2021. SpatialProto: Exploring Real-World Motion Captures for Rapid Prototyping of Interactive Mixed Reality. In *CHI '21: CHI Conference on Human Factors in Computing Systems, Virtual Event / Yokohama, Japan, May 8-13, 2021*. ACM, 363:1–363:13. https://doi.org/10.1145/3411764.3445560

[8] Michael Nebeling and Katy Madier. 2019. 360proto: Making Interactive Virtual Reality & Augmented Reality Prototypes from Paper. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems, CHI 2019, Glasgow, Scotland, UK, May 04-09, 2019*. ACM, 596. https://doi.org/10.1145/3290605.3300826

[9] Michael Nebeling, Janet Nebeling, Ao Yu, and Rob Rumble. 2018. ProtoAR: Rapid Physical-Digital Prototyping of Mobile Augmented Reality Applications. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems, CHI 2018, Montreal, QC, Canada, April 21-26, 2018*. ACM, 353. https://doi.org/10.1145/3173574.3173927

[10] Franziska Roesner, David Molnar, Alexander Moshchuk, Tadayoshi Kohno, and Helen J. Wang. 2014. World-Driven Access Control for Continuous Sensing. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, Scottsdale, AZ, USA, November 3-7, 2014*. ACM, 1169–1181. https://doi.org/10.1145/2660267.2660319

[11] Maximilian Speicher and Michael Nebeling. 2018. GestureWiz: A Human-Powered Gesture Design Environment for User Interface Prototypes. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems, CHI 2018, Montreal, QC, Canada, April 21-26, 2018*. ACM, 107. https://doi.org/10.1145/3173574.3173681

[1] https://docs.microsoft.com/en-us/windows/mixed-reality/design/color-light-and-materials

[2] https://unity.com/products/unity-mars

[3] https://www.innersloth.com/games/among-us/