

# First Workshop on Security and Privacy for Immersive Virtual Worlds (Secure Immersive Worlds)

As critical applications in healthcare, education, finance, teleoperation, and retail emerge in the future immersive worlds, ensuring security and privacy of users from internal and external attacks becomes vital. A significant quantity of sensitive data is likely to be generated by the widespread adoption of VR/XR/MR/AR technologies in "serious" immersive worlds. Traditional approaches for security and privacy fail to capture the subtleties of \*R hardware/software systems and the impact of human behavior. The Secure Immersive Worlds workshop aims to cover these open research and technological challenges and garner ideas in ensuring continued security and privacy of users in serious immersive worlds. The full-day workshop will bring researchers and industry practitioners together to discuss these new emerging research challenges and technologies. The workshop will consist of keynote speakers, juried paper presentations, and a panel discussion. We invite authors to submit 6-page (plus 1-page for references) research or position papers.

## Location

The workshop will be held remotely, details will be shared here later.

## Date

TBD

## Topics of interest

The topics of interest for the workshop are related to the following themes in security and privacy for serious immersive worlds:

- Privacy and security aware design considerations for serious immersive worlds
- Multi-system datasets for benchmarking algorithms for security
- Novel hardware for physical biometrics in VR/XR/MR/AR system
- Security and privacy challenges in remote and co-located immersive worlds
- Protecting at-risk populations, such as children, older adults, individuals with disabilities
- Emerging attack models for serious immersive worlds applications
- Case studies on usability of security models in real-world applications
- Psychological and physiological effects in behavior-based security
- Security and privacy in multi-user scenarios
- Compliance with legal policies in immersive worlds
- Privacy preserving data access and sharing
- Resiliency against attacks
- Verifiable security for immersive worlds applications

## Important Dates AOE

- Submission Deadline: January 6, 2023
- Notification: January 20, 2023

- Camera-Ready: February 3, 2023
- Workshop: TBD

## Paper Submission Information

All papers must be submitted online using the [PCS system](#) as a single PDF file using the [VGTC template](#). Authors must ensure that their papers are anonymized. All papers have a strict 6-page limit (excluding references, max 1-page for references). Authors are strongly encouraged to use the LaTeX template provided on the IEEE website for compiling their papers. The PCS system will enable authors to select IEEE VR 2023 as the conference and then IEEE VR 2023 Workshop: Secure Immersive Worlds as the track.

Upon acceptance, at least one author must register for the workshop as well as one day of the IEEE VR full conference. Accepted authors will be expected to give a 15-minute (12 minute talk + 2 minutes Q/A + 1 minute for transition) presentation at the workshop. The workshop will be held online with paper sessions in the morning and afternoon. Proceedings from the workshop will be submitted for inclusion in the IEEE Digital Library.

## Reviewing process

All papers will be reviewed by at least two experts in the domain. There will be no rebuttal phase for the submissions. Publication in the workshop will not prohibit future publications as full or journal papers with additional material. However, workshop papers cannot be submitted verbatim to another venue with additional material. Authors of accepted papers will be expected to make changes requested during the review and resubmit a final version by the camera-ready deadline.

## IEEE VR Resubmissions

Authors with papers that were rejected from the IEEE VR main conference track can submit their papers to the workshop as long as the paper fits the workshop themes and the authors follow the following resubmission guidelines. The revised submission must fit within the 6 page limits of the workshop. The changes made should be summarized in a revisions letter (max one A4 page) to be included with the submission. All revised papers must include the meta-reviews directly from the PCS system. Papers that do not meet these requirements will be desk rejected. All papers will be reviewed by at least two experts in the domain. There will be no rebuttal phase for the submissions.

## Organizers

Sean Banerjee - *Clarkson University, USA*  
Diksha Shukla – *University of Wyoming, USA*  
Natasha Banerjee - *Clarkson University, USA*

## Contact

If you have any questions, please contact Sean Banerjee at [sbanerje@clarkson.edu](mailto:sbanerje@clarkson.edu) and indicate Secure Immersive Worlds 2023 in the title.