University of Missouri

SaTC: CORE: Small: Modeling and Defense of Cyber Attacks for Improving Social Virtual Reality Resilience

Challenge:

- How to model & analyze security, privacy, and safety (SPS) threats in social Virtual Reality Learning Environments (VRLEs).
- How to collect threat intelligence on VRLE cyber attacks to deploy effective defense?

Solution:

- Use of attack fault trees for modeling SPS threats and probabilistic model checking to analyze them (TDSC 2021).
- Collect threat intelligence on cyber attacks, immersion attacks, and fault attacks. Use this knowledge base for real-time attack detection in VRLEs (FiCloud 2021).

Figure 1: Chaperone file attack to disrupt the users' physical safety due to content unavailability.

Scientific Impact:

- Novel formalization of AFT for modeling cyber attack and fault trade-offs and scalable analysis of AFTs using graph decomposition method.
- Novel anomaly detection approaches based on machine learning algorithms and statistical analysis technique.
- Published several papers in first year of the project: IEEE TDSC'2021, IEEE FiCloud'2021.

Broader Impact and Broader Participation:

- The project outcomes will impact workforce training, education/special education, public safety, telehealth, and advanced manufacturing.
- One Ph.D. student is mentored through this grant. An existing REU site at MU is used to involve URM students in this project.
- A new curriculum will be developed from the outcome of this research and will be integrated with Cloud computing, Cyber defense, and Formal method courses.

CNS- 2114035. PIs: Khaza Anuarul Hoque, Prasad Calyam.
Email: hoquek@missouri.edu