UTSA®

ALVAREZ
College of Business
The University of Texas at San Antonio

Using Virtual Reality to Increase Cyber Situational Awareness

Dr. Nicole L. Beebe
Dr. Brita Munsinger

Discussion Outline

- Project overview & goals
- Background
  - SOC operations & investigation paradigms
  - Situational awareness (SA)
  - Virtual reality
- Theoretical perspective
  - Mapping VR constructs to SA constructs
- Study methodology
  - Experimental approach
  - Datasets
  - VR code
- Current status & next steps

Project Overview & Goals

- Focus:
  - Empirically examine whether VR can improve cyber situational awareness
- Scope:
  - 1 year; $75K (partially funded post-doc)
  - Leverage existing VR code previously developed (Kullman 2018, 2019)
  - Consult with real-world SOCs
  - Experiment with synthetic but realistic datasets

SOC Operations & Investigations

- What do SOCs do?
  - Collect, monitor, aggregate, analyze host and network sensor and log data
  - User behavior analytics
  - Alert analysis & response
  - Playbook implementation
  - Assess, report, integrate threat intel data
  - Investigate intrusions
- What are the challenges?
  - Information overload
  - Lack of 'single pane of glass' solution
  - SOC operator input is still largely textual / 2D graphical

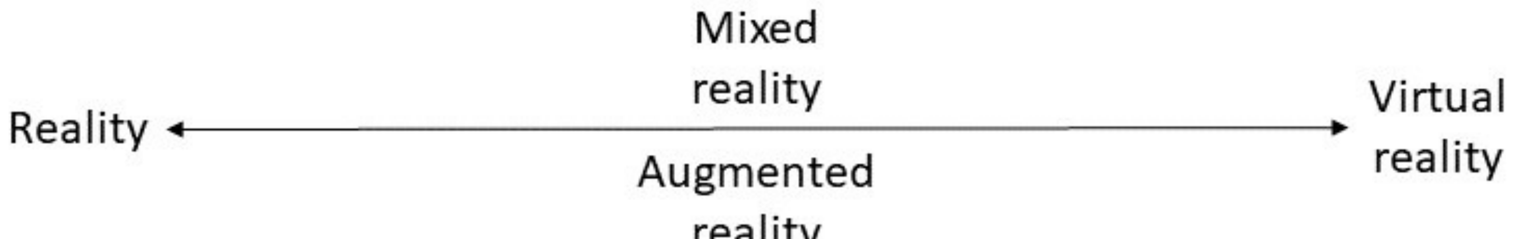
Situational Awareness Overview

- Definition:
  - Ability to perceive and comprehend environmental elements in time and space to the point of being able to project their meaning and state into the future (Endsley 1995)
- Key components
  - Perception: Searching for information
  - Comprehension: Understanding a complex, evolving situation
  - Projection: Ability to apply info to predict near-term
- SA impacts decision making quality and speed when performing dynamic tasks

Cyber Situational Awareness

- SA research has been active in many domains *except cyber operations* (Gutzwiller et al. 2015)
- Fatigue & cognitive overload particularly problematic for cyber operators (Paul & Dykstra 2017)
- Limited cyber SA studies focused on SA improvements from simple data fusion
- Other "SA" studies have focused on benefits of different visualizations (Whitlock 2020)

Virtual Reality Overview

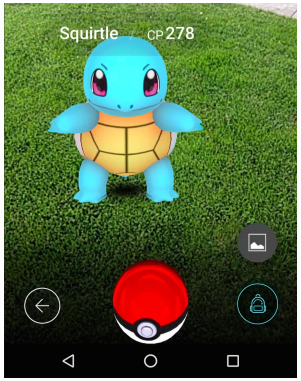


Mixed reality

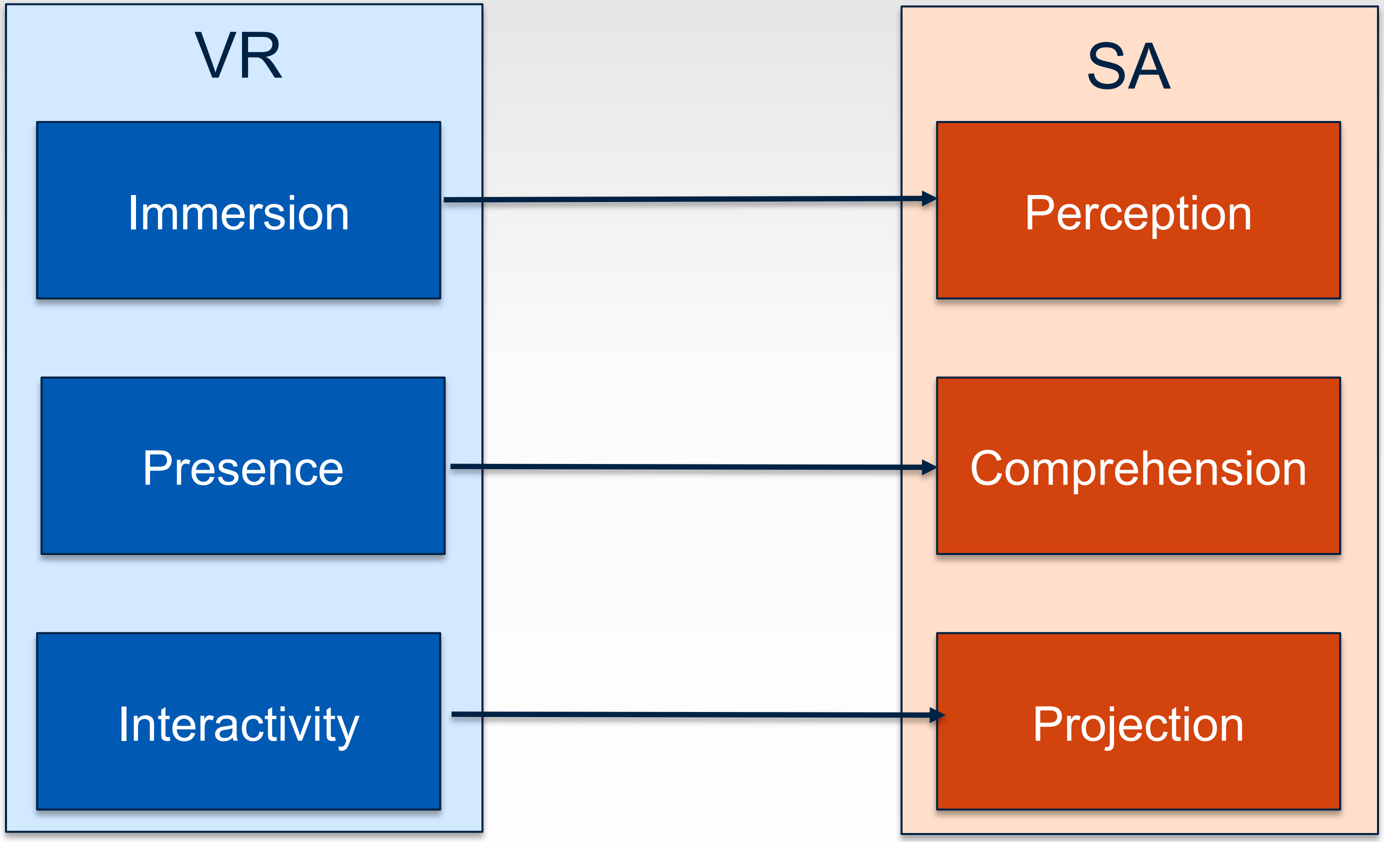
Reality

Virtual reality

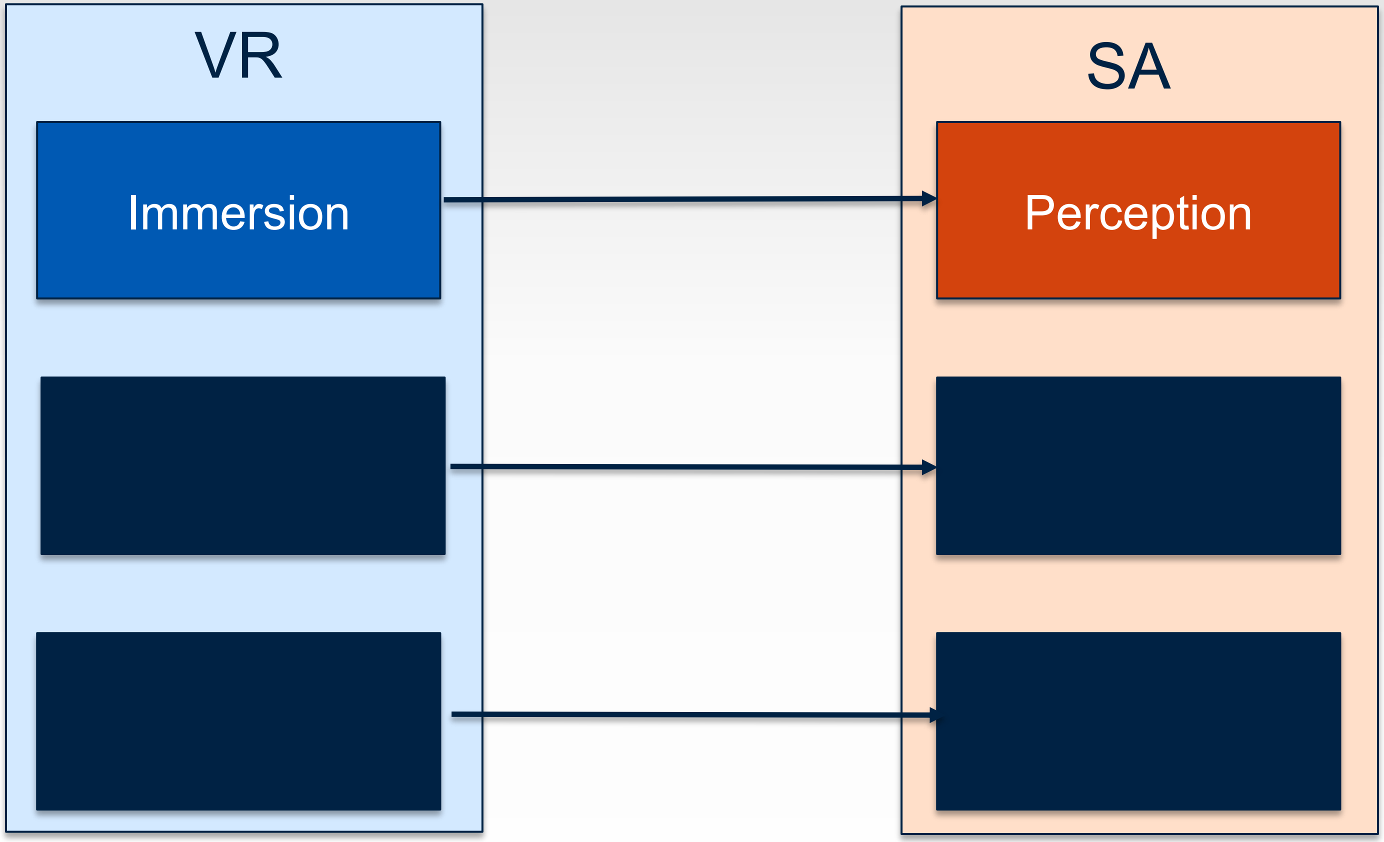
Augmented reality



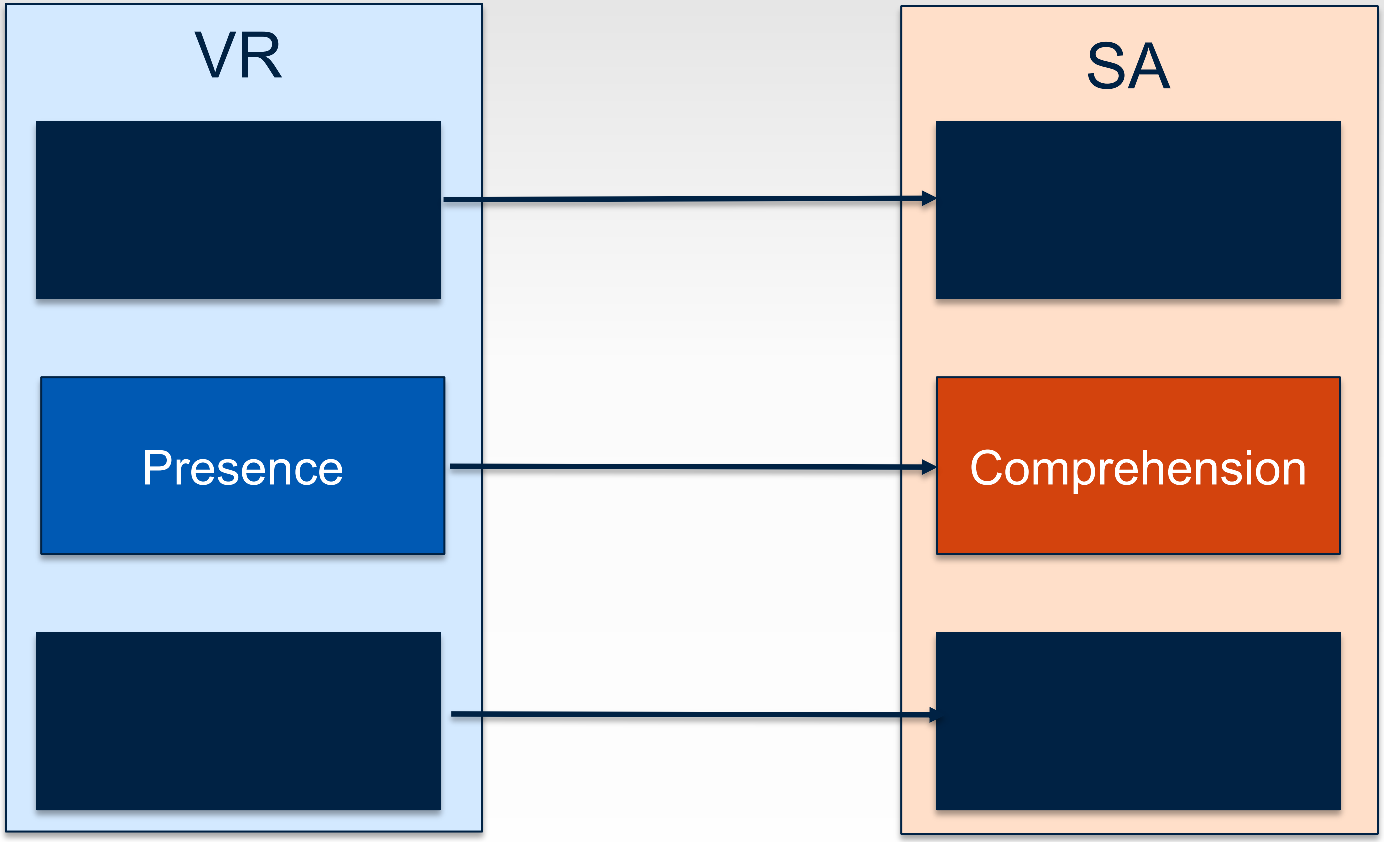
Linking VR to SA Theoretically



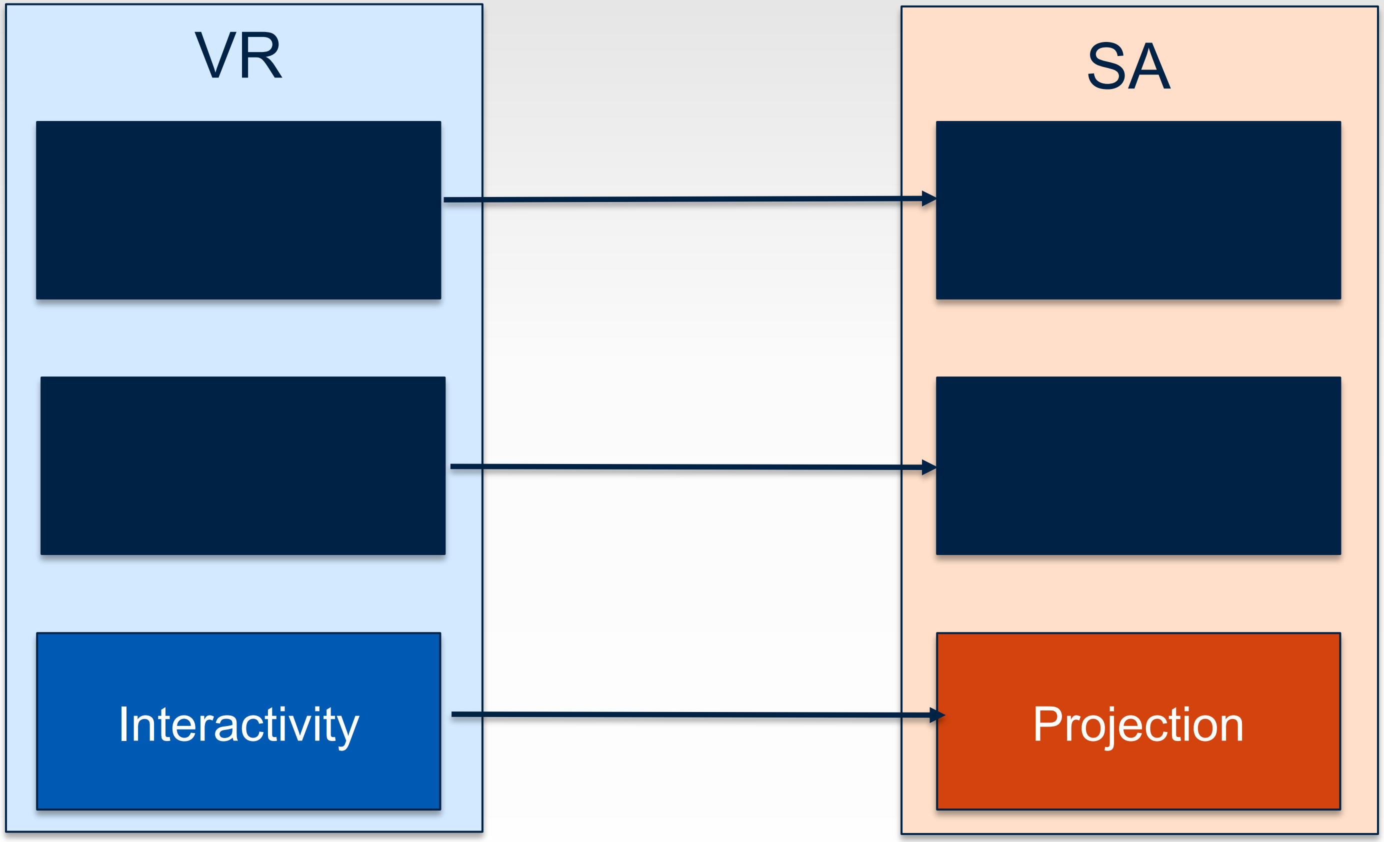
Linking VR to SA Theoretically



Linking VR to SA Theoretically



Linking VR to SA Theoretically



VR

SA

Interactivity

Projection

Study Methodology

- Experimental approach
- Datasets
- VR code

Experimental approach

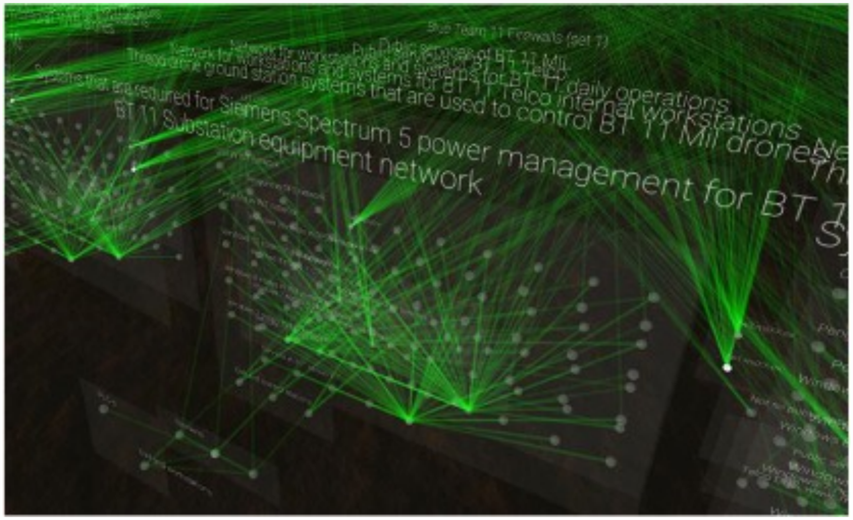
- Adapting the SAGAT (Situation Awareness Global Assessment Technique) approach (Endsley 2000)
  - Pause participant's progress (freeze)
  - Ask questions about their status and thoughts (probe)
- Participants are divided randomly into two groups
  - One group performs threat analysis using standard tools
  - Other group uses standard tools plus VR
- Does the VR group achieve higher SA?

Datasets

- Considered a variety of datasets
- Selected two from UTSA professional education cyber range
  - Contain lateral movement / data transfer
  - Sophisticated but small to enable experiments

VR code

- VDE (Virtual Data Explorer) Kaur Kullman, ARL and now UMBC
- Displays nodes in a network and traffic between them
- User may mark nodes as harmful to track threats


Systems that are used to control BT 11 Mil drones
daily operations
internal workstations
Siemens Spectrum 5 power management for BT 1
BT 11 Substation equipment network

Current Status & Next Steps

- IRB approval acquired
- Code acquired & working
- Datasets collected
- Currently preparing for experiments
- Writing theory & empirical papers
- Next steps:
  - Conduct experiments
  - Finish papers

Nicole.Beebe@utsa.edu; bmunsing@trinity.edu

QUESTIONS & COMMENTS?