

Dynamic and Personalized Deception using Human Experiments and Cognitive Agents

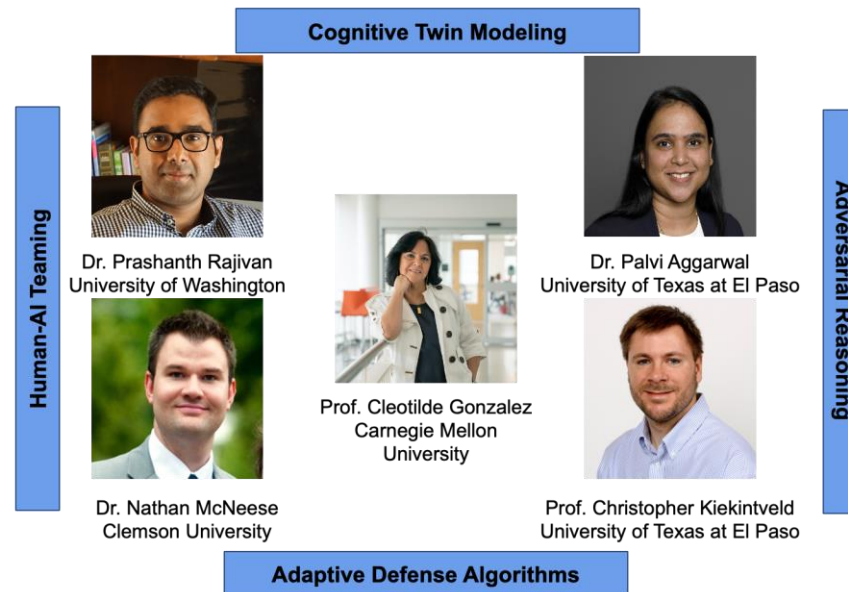
Palvi Aggarwal

Assistant Professor

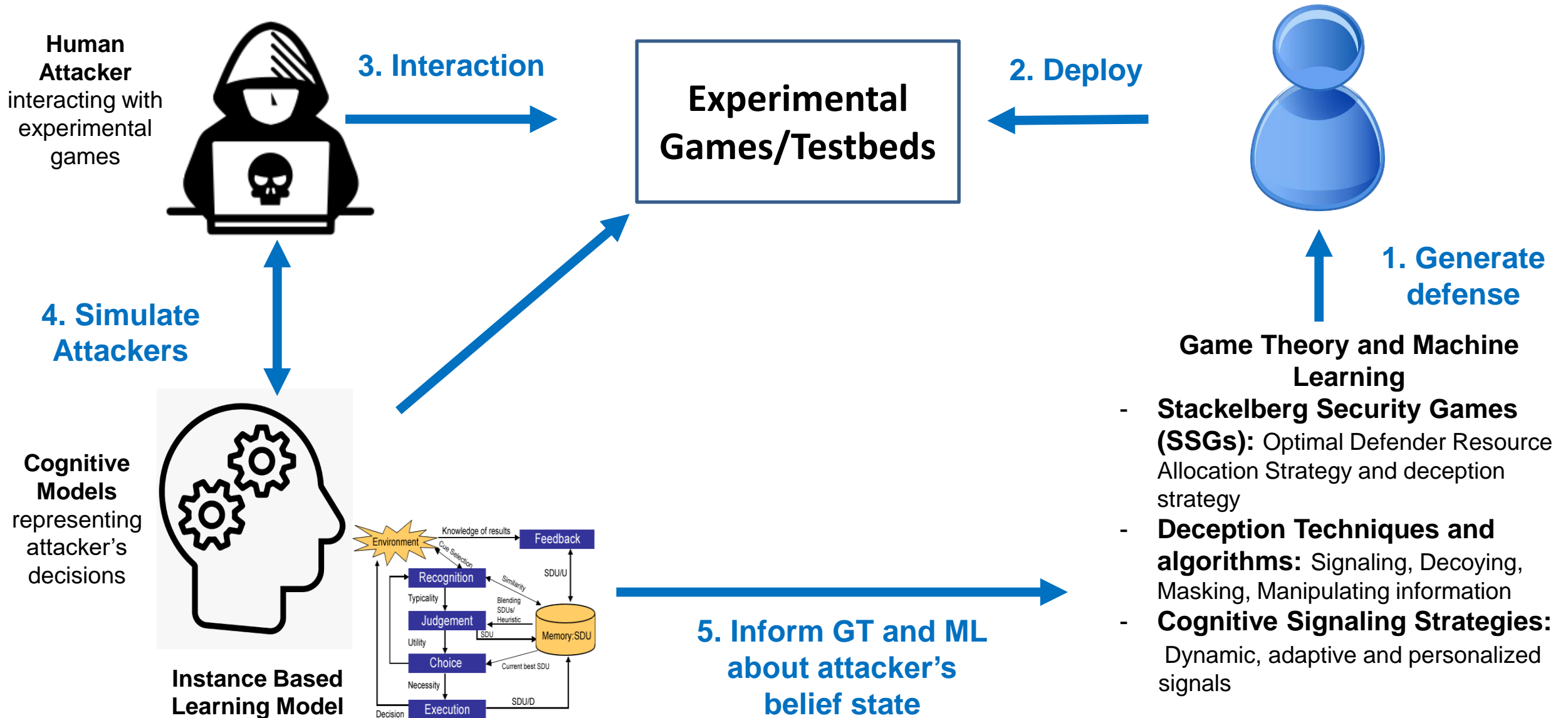
Department of Computer Science

University of Texas, El Paso, USA

Human-AI Cognition in Cyber Protection Teams



Research Framework for Cyber Deception



Increasing Complexity and Fidelity of experimental games

Fidelity (Realism)

Abstract

Simplicity

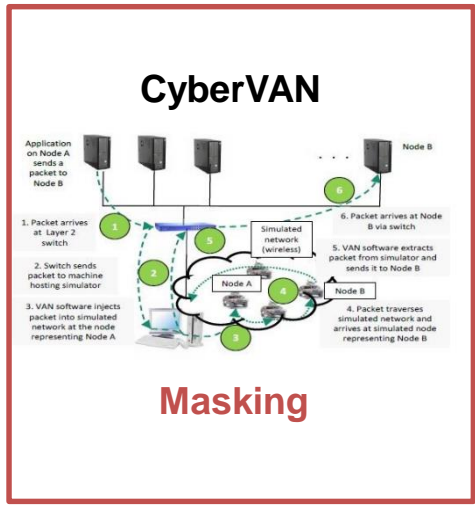
Complexity



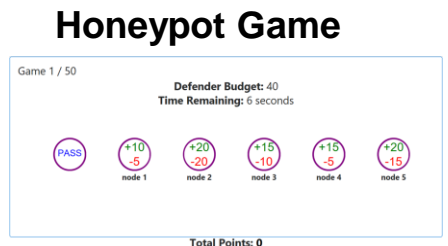
Information Manipulation



Decoying and Masking

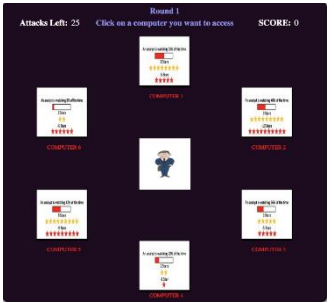


Masking



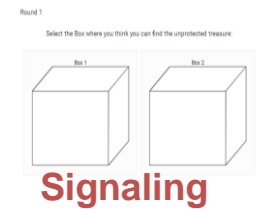
Decoys

Insider Attack Game



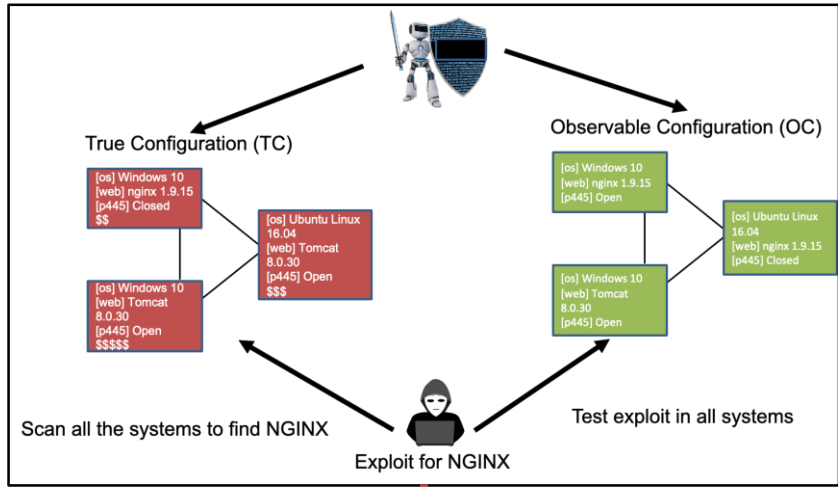
Signaling

The Box Game

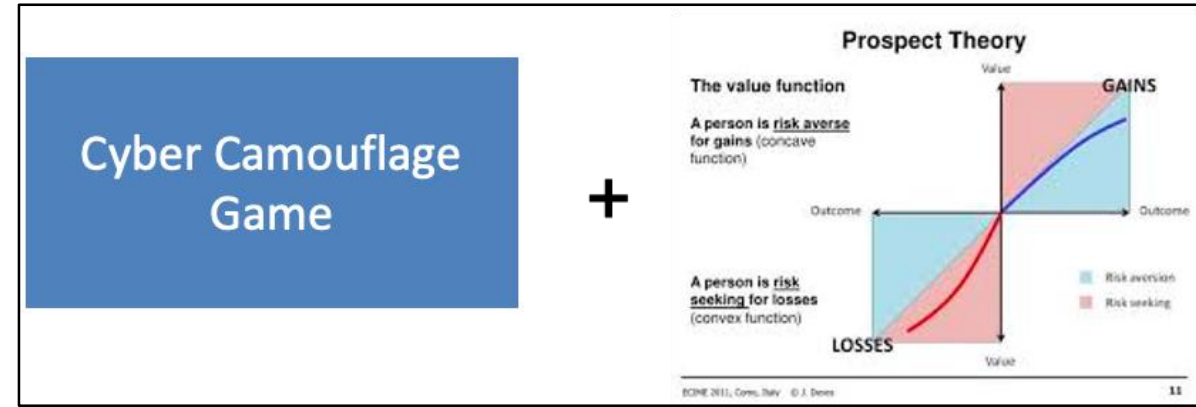


Signaling

Attacker's Behavior in Cyber Camouflage Game



Risk Based Cyber Camouflage Games (RCCG)

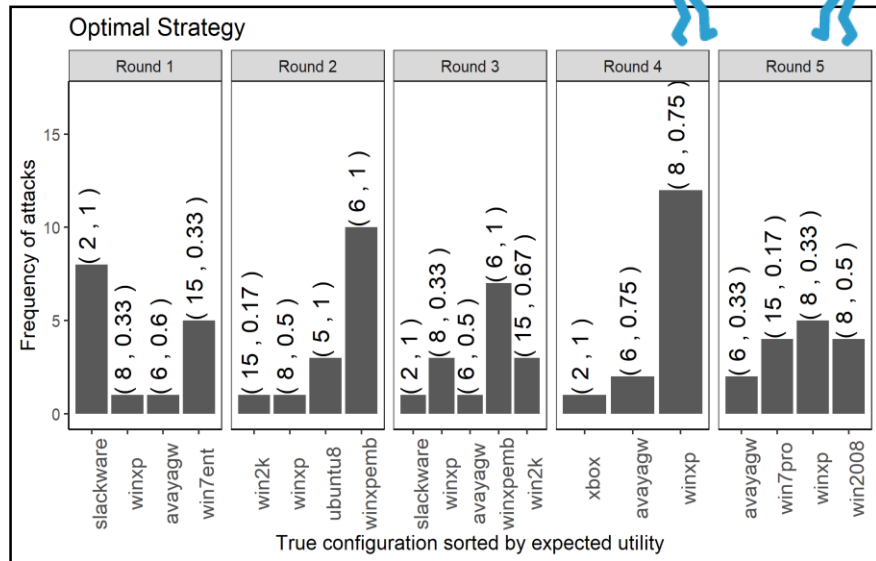


Generate new defense scheme

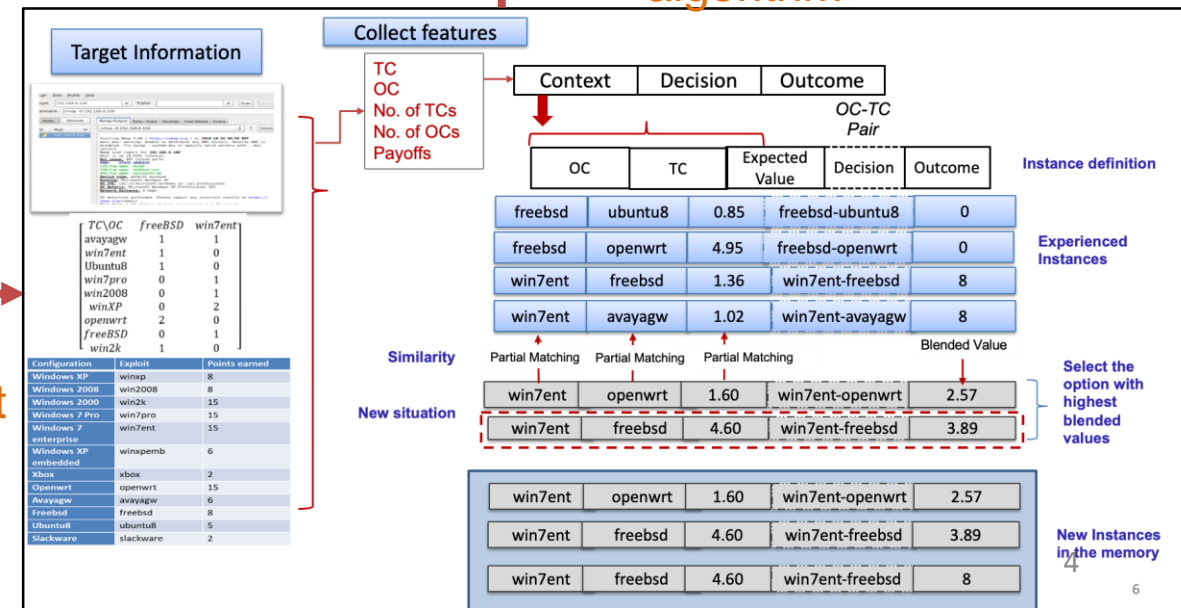
Risk Aversion



Adapt the defense algorithm



Developing Cognitive Agent



Thank you!

Contact: pagggarwal@utep.edu