Understanding Human Misperception of Cyber Risks and Integrative Design of Human-Centered Intervention Mechanisms to Secure Critical Infrastructures NSF 2122060:

Human Behavior and Infrastructure Component for Connected and Autonomous Vehicles

Lead PI: Emily Balcetis
Quanyan Zhu, Co-PI
Rae Zimmerman, Co-PI (slide submitter)
rae.zimmerman@nyu.edu

CHALLENGE AND OVERALL PROJECT APPROACH SUMMARY

Understanding Human Vulnerabilities:

- Experimental and quantitative methods to study and mode human errors in personal risk assessments of cyber-attacks within interdependent infrastructures.

Monitoring and Detection of Attacks:

- Determine the type of the cyberattack being launched against a particular sub-system or component in order to derive learning patterns from existing attack data sets.

Mitigation Analysis through Multi-Modal Resource Planning:

- Determine how we can use multi-modal networks to promote resilience.

IMPACTS AND SELECTED SOLUTIONS (Use Behaviors)

COMPONENT - CYBER ATTACK SCENARIOS (CASES) ASSOCIATED WITH HUMAN VULNERABILITIES AND ACTIONS FOR RISK AVOIDANCE: HUMAN BEHAVIOR AND CONNECTED AND AUTONOMOUS INFRASTRUCTURE

Collision attacks

- Attacker takes control of vehicle (CAV) causing collisions
- Vehicle user risk perceptions and sociocultural context can promote risk-minimizing pattern to avoid attacker control

Denial-of-Service (DoS) attacks

- Attacker can disrupt vehicle communication system through the internet thereby disrupting vehicle automation systems and communication among vehicles
- Vehicle user risk perceptions can encourage users to avoid vulnerable communications

Traffic manipulation attacks

- Attacker creates misinformation potentially resulting in traffic disruption
- Infrastructure designers can invoke verification and trust mechanisms to detect inconsistencies

For more information see: https://www.nsf.gov/awardsearch/showAward?AWD_ID=2122060&HistoricalAwards=false