EAGER: SaTC-EDU:
Teaching Security in Undergraduate AI
with Transparency and Contextualization

THE UNIVERSITY OF UTAH

Challenge:

- When AI and ML are taught abstractly, students can't identify security implications
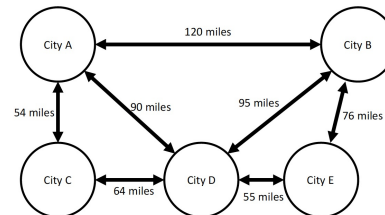
Solution:

- **Contextualization:** integrate security issues into technical assignments
- **Transparency:** show the human impacts of technical choices

Focus on choosing or modifying algorithms

Identify harms from rote use of algorithms

Jessie is traveling from City A to City B. Jessie requires hospital treatment at random intervals. Hospitals are in the cities but not along the roads.

Which objective function would meet Jessie's needs, and which search algorithms could use it?

Student think-alouds, instructor co-design

Analyze student work for technical misconceptions

Scientific Impact:

- Instructional design process
- Improved assessment validity and instructor pedagogical content knowledge

Broader Impact and Broader Participation:

- Implemented in two offerings of intro AI
- Instructor Workshop
- Ug. Thesis; REU; Honorable Mention CRA Outstanding Ug. Researcher
- Invited talks for instructors and community