SaTC: CORE: Medium: Countering Surveillanceware Using Deception-Based Generative Models and Systems Mechanisms

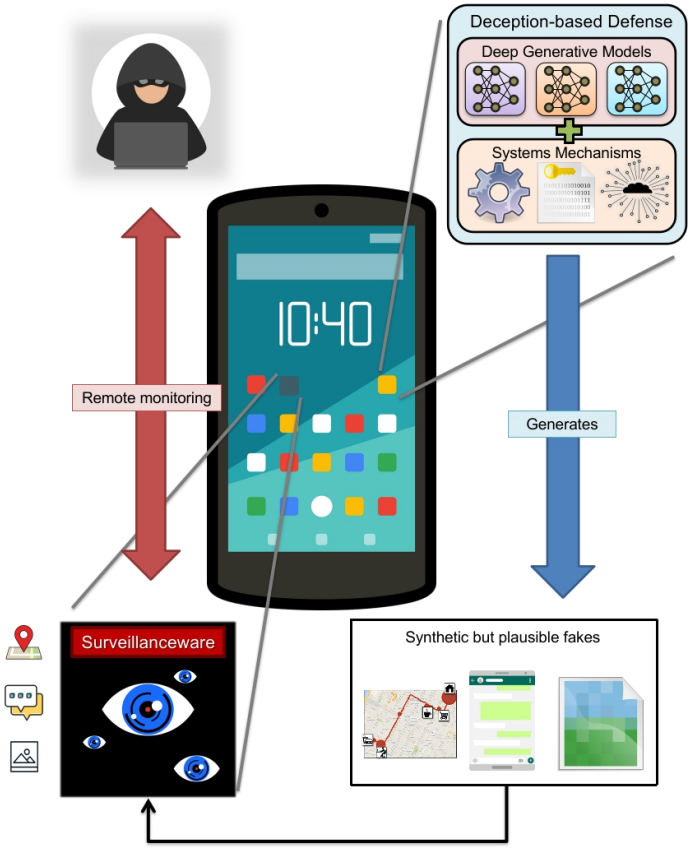
UF UNIVERSITY of FLORIDA

Challenge:

- Surveillanceware is increasingly common; Victims are unable to uninstall it due to coercion or violence, so traditional defenses (e.g., antivirus) may not work
- We need better understanding of surveillanceware and new directions for defenses

Solution:

- Generate synthetic data and feed it to surveillanceware to fool it
  - Building on our prior work synthesizing location trajectories and our past experience with mobile platforms
- Novel combination of systems mechanisms and deep generative models



Scientific Impact:

- Studying surveillanceware adversaries will improve understanding of the threat and highlight mitigations
- Deep generative models for synthesizing fake but plausible data will highlight new applications

Broader Impact and Broader Participation:

- Tackling surveillanceware helps broaden cybersecurity research to include concerns of vulnerable individuals/groups
- Collaborations with local organizations (e.g., domestic abuse shelters) and international partners (e.g., the Coalition Against Stalkerware)

Project #: 2055123
Vincent Bindschaedler (PI) and Kevin Butler (Co-PI)
University of Florida