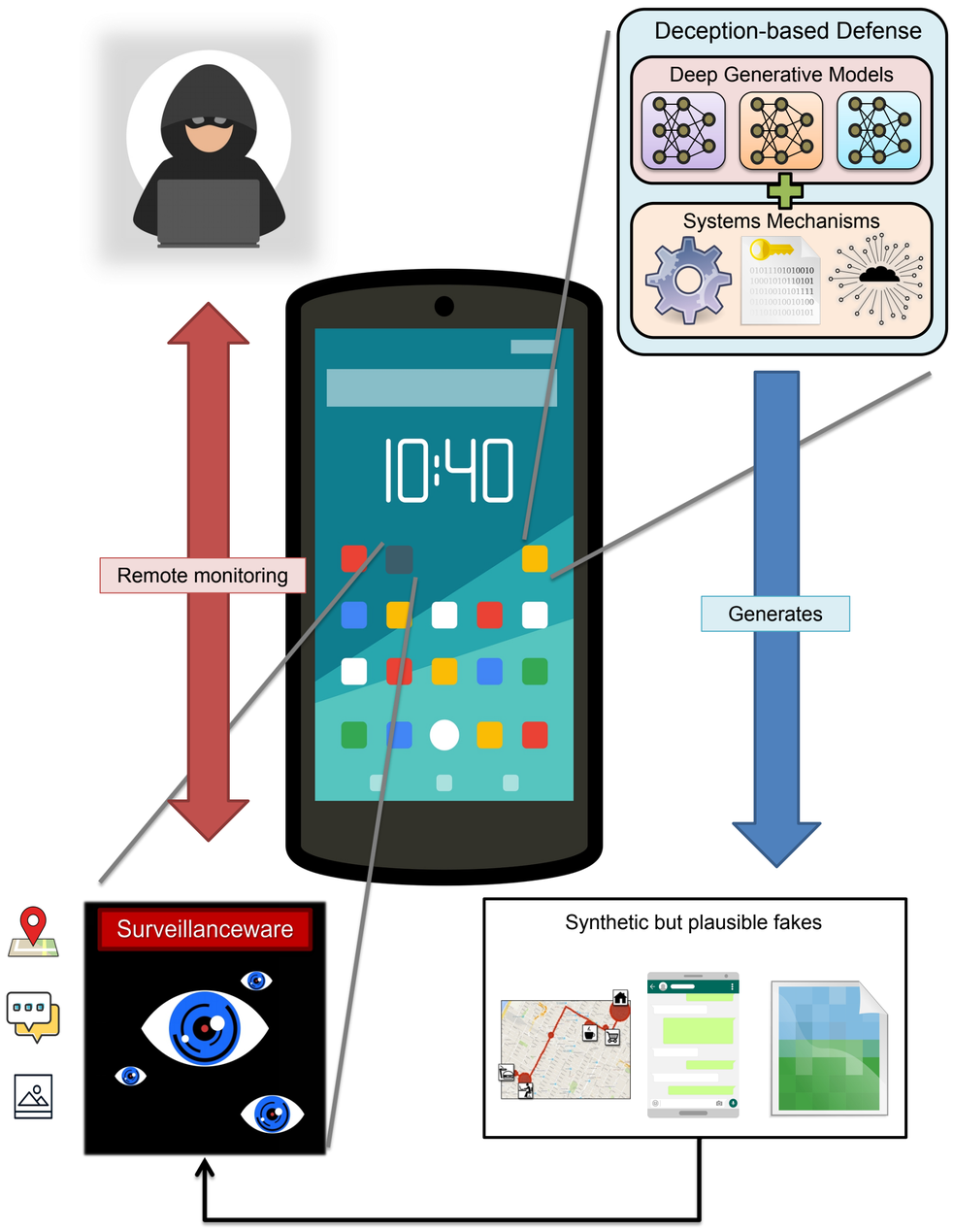
SaTC: CORE: Medium: Countering Surveillanceware Using Deception-Based Generative Models and Systems Mechanisms

Vincent Bindschaedler (PI), Kevin Butler (Co-PI) — University of Florida

Overview:



Challenges:

- Surveillanceware (i.e., stalkerware, spyware) is increasingly common
- Traditional malware defenses (e.g., antivirus) may not work; For example victims may be unable to uninstall surveillanceware due to coercion or threats of violence
- Surveillanceware is poorly understood and new defenses are needed

Scientific Impact:

- Studying surveillanceware adversaries will improve our understanding of the threat and possible mitigations both legal and technical
- Use of deep generative models for synthesizing fake but plausible data highlights new applications of ML for security and privacy

Broader Impact and Broader Participation:

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

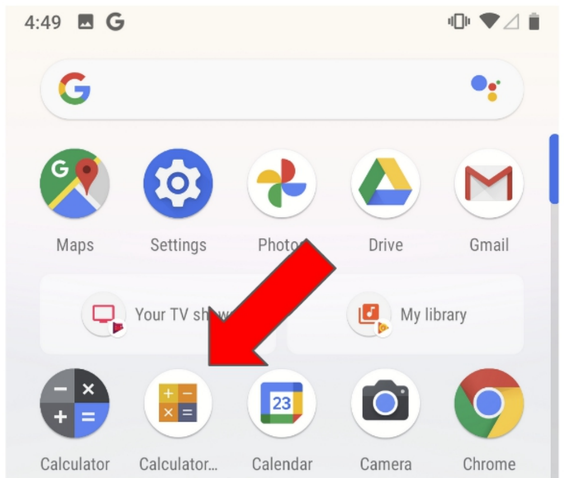
Roadmap:

- Thrust 1: Characterizing the surveillanceware adversary
- Thrust 2: Deception using ML-based fakes
- Thrust 3: Systems integration and protection mechanisms

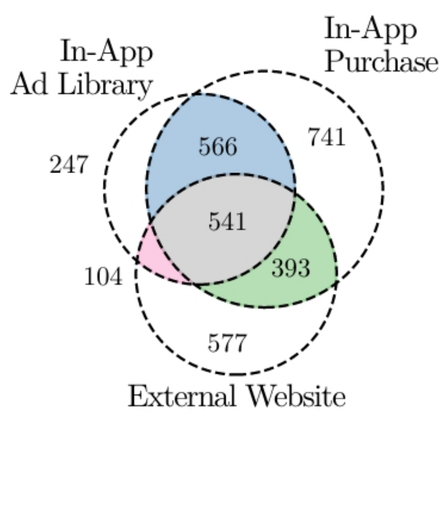
Preliminary work: "Analyzing the Monetization Ecosystem of Stalkerware."*

**Joint work with: Cassidy Gibson, Vanessa Frost, Katie Platt, Washington Garcia, Luis Vargas, Sara Rampazzi, Patrick Traynor. (Conditionally accepted at PETS 2022.)*

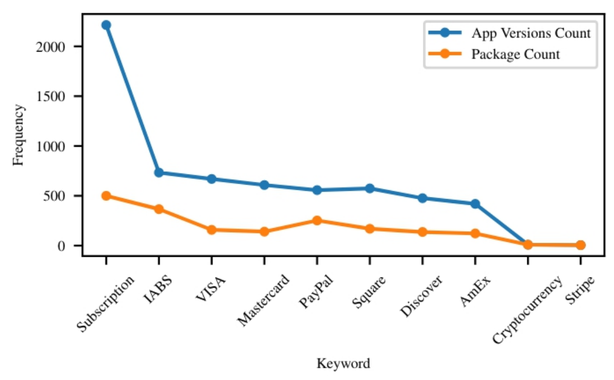
Example of camouflage



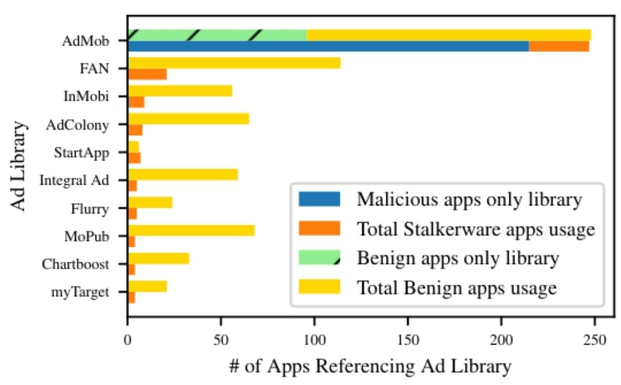
Monetization types:



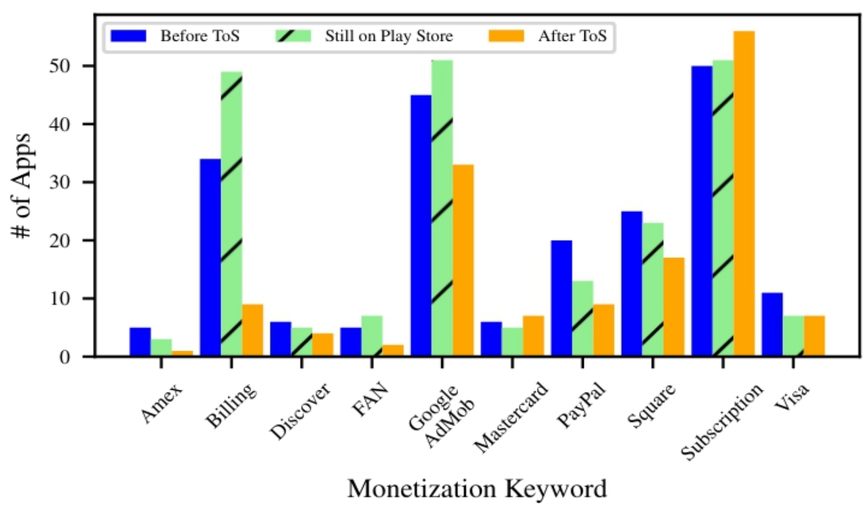
In-app monetization keywords:



Use of ad libraries:



Effect of policy change (Google Playstore):



Summary & Findings:

- We analyze monetization strategies of 6,400 apps collected by the Coalition Against Stalkerware
- We find significant differences in monetization strategies of stalkerware apps (compared to benign apps)
- Also: stalkerware apps continue to be monetized despite Google Playstore policy changes
- Our results suggest a multi-pronged approached involving many stakeholders is needed