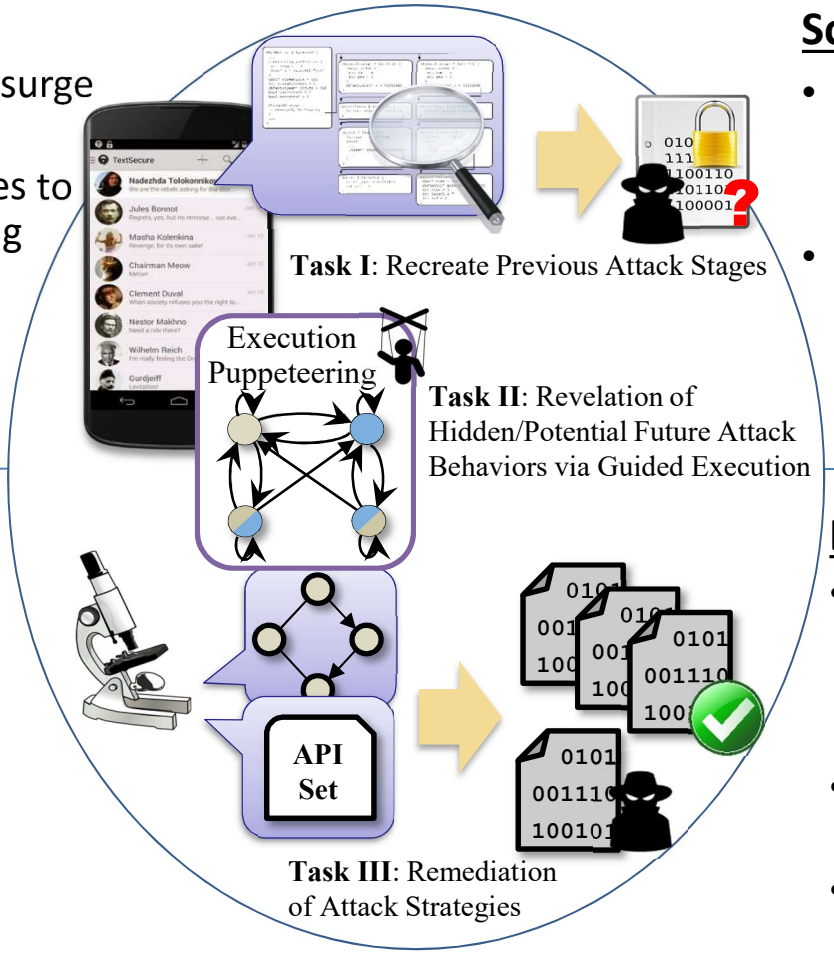
GEMINI: Guided Execution Based Mobile Advanced Persistent Threat Investigation

Challenge:

- Recent years have seen a surge in mobile APT campaigns
- Authorities lack techniques to quickly investigate ongoing attacks
- Prior forensic approaches can take days or months!



Solution:

- Memory forensics is a key technique in time-critical cyber investigation
- GEMINI adapts guided execution techniques to investigate and remediate mobile APT attacks

Scientific Impact:

- GEMINI reveals both previous and potential future attack behaviors
- This project is developing novel Android malware analysis and memory forensics techniques

Broader Impact:

- GEMINI advances national security by developing techniques for mobile cyber forensics
- All findings and code are publicly available
- This work is generating new cyber forensics curriculum materials

CNS-1755721, CRII:SaTC
PI: Brendan Saltaformaggio
brendan@ece.gatech.edu