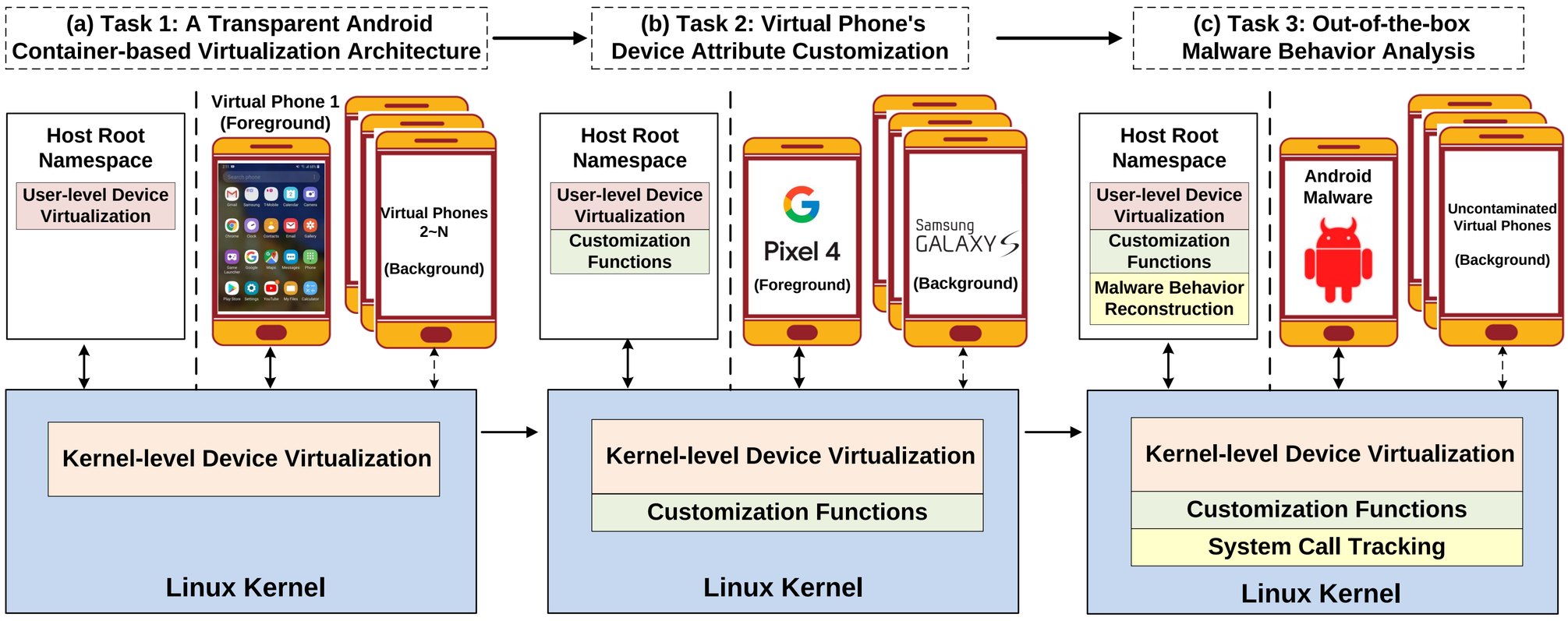
SaTC: CORE: Small: A Transparent and Customizable Android Container-Based Virtualization Architecture for Dynamic Malware Analysis

Jiang Ming, University of Texas at Arlington

Figure 1: The overview of our proposed research tasks and the "out-of-the-box" design.



Challenge:

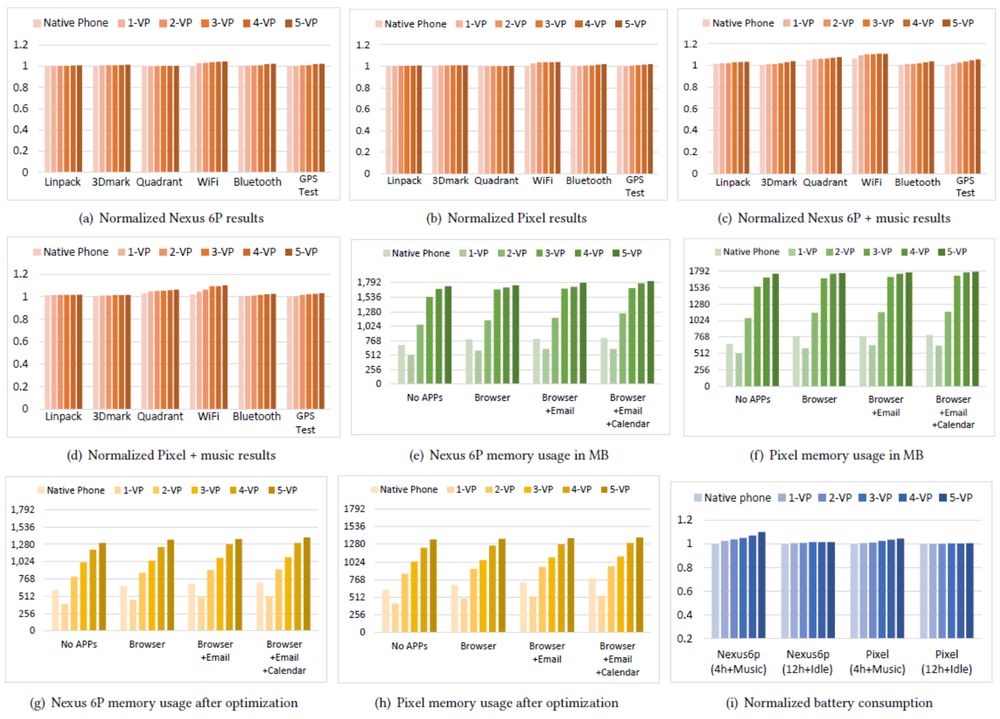
- Efficiently analyzing evasive malware behavior remains an urgent but unsolved problem.
- Current Android malware dynamic analysis platforms (i.e., Android emulators and bare-metal machines) have their specific limitations.
- Android emulators' virtualization techniques are not transparent, and evasive malware have adopted various anti-emulation heuristics to evade Android emulators.
- Bare-metal machines lack the capabilities in customizing device attributes and producing semantics-rich results.

Solution:

- Innovatively employ container-based virtualization to analyze evasive malware.
- Integrate the principle of anti-evasion into the design of a transparent and customizable malware sandbox.
- Reconstruct semantics-rich malware behaviors from low-level system events.

Scientific Impact:

- Apply container-based virtualization to address the long-standing challenge of efficiently analyzing evasive malware.
- Our work shows stronger resilience to evasive malware than Android emulators, and it also has better stealthiness, analysis flexibility, and productivity than bare-metal machines.
- Utilizing our architecture, future researchers can develop various techniques to boost more effective and efficient malware analysis approaches.



(a) Normalized Nexus 6P results (b) Normalized Pixel results (c) Normalized Nexus 6P + music results
(d) Normalized Pixel + music results (e) Nexus 6P memory usage in MB (f) Pixel memory usage in MB
(g) Nexus 6P memory usage after optimization (h) Pixel memory usage after optimization (i) Normalized battery consumption

Figure 2: Gegenees's superior performance data

Broader Impact (impact on society-who will care)

- Pave the way for efficiently analyzing evasive malware.
- Contribute to the system security research community.
- Improve the synergy between mobile systems, virtualization, and security.
- Benefit numerous smartphone users.

Broader Impact (education and outreach)

- Transform the proposed prototypes into three hands-on labs with increasing difficulties
- Develop a new seminar course: Android Malware Analysis
- Incorporate research findings into extracurricular activities, such as HackUTA and CTF.
- Collaborate with industry partners on technology transfer.

Broader Impact and Broader Participation (quantify potential impact)

- The global mobile virtualization market is expected to reach $12.7 billion by 2026.
- McNair scholar and GAANN fellowship students are participating in the project.
- Hundreds of undergraduate and graduate students will benefit from the courses.