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

UNIVERSITY OF TEXAS ARLINGTON

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.
- Bare-metal machines lack the customization flexibility.

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.

NSF CNS #2128703,

University of Texas at Arlington ,
Computer Science and Engineering Department,
Jiang Ming

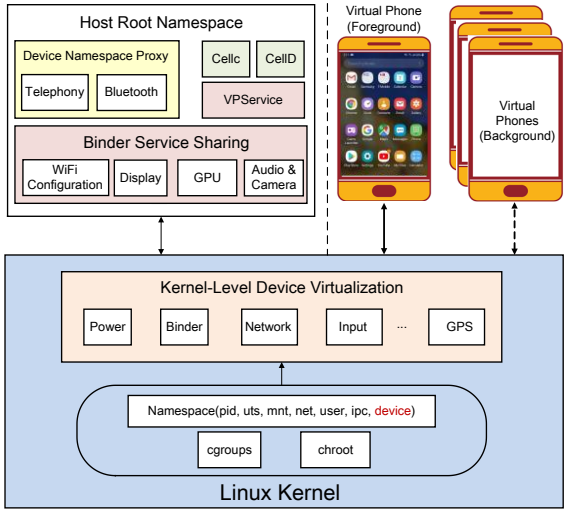

Figure 1: **Gegenees**'s virtualization architecture

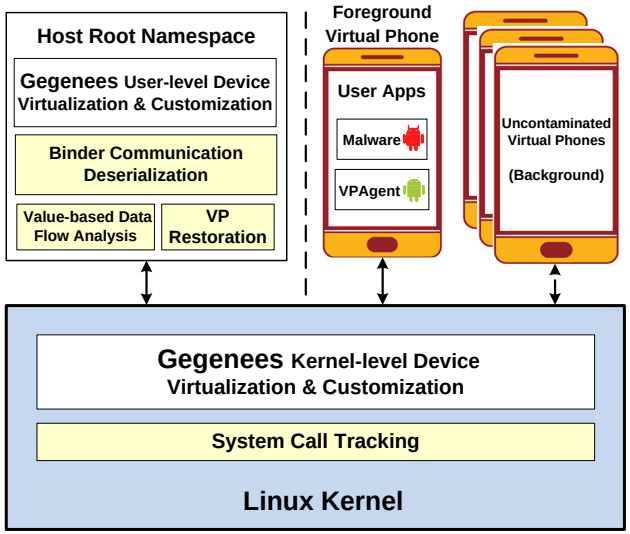

Figure 2: Gegenees's malware analysis components

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

Broader Impact:

- Pave the way for efficiently analyzing evasive malware.
- Benefit numerous smartphone users.
- Improve the synergy between mobile systems, virtualization, and security.
- Collaborate with industry partners on technology transfer.
- Develop hands-on courses to enhance UTA security courses.
- McNair scholar and GAANN fellowship students are participating in the project.