SaTC: CORE: Small: Collaborative: Enabling Precise and Automated Insecurity Analysis of Middleware on Mobile Platforms

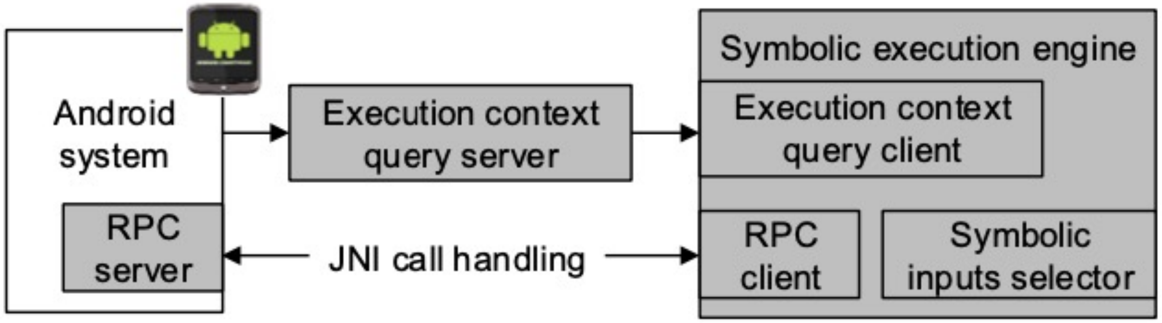
UNIVERSITY OF South Carolina

Challenge:

- Middleware of a mobile platform (such as Android Framework) has a huge code base and is difficult to analyze
- Existing symbolic execution is not scalable

Scientific Impact:

- The developed tools are used to find Android Framework vulnerabilities and generate exploits
- Tainting and heap snapshots can boost the scalability of symbolic execution


Android system
RPC server
Execution context query server
JNI call handling
Symbolic execution engine
Execution context query client
RPC client
Symbolic inputs selector

Solution:

- Instead of analyzing the code as a whole, our solution analyzes system service methods separately
- Tainting is used to identify framework variables under the control of a malicious app
- Heap snapshots assisted symbolic execution

CNS-1856380
University of South Carolina
Penn State University
Lead PI: Qiang Zeng (zegn1@cse.sc.edu)

Broader Impact and Broader Participation:

- Improved the trustworthy of smartphones
- Open-sourced the tools
- Funded the research of students from underrepresented groups
- Published papers in MobiSys’17, TMC, TDSC, etc.