The Center for Cyber Defenders

Expanding Computer Security Knowledge

Santeria

An Android Debug Framework

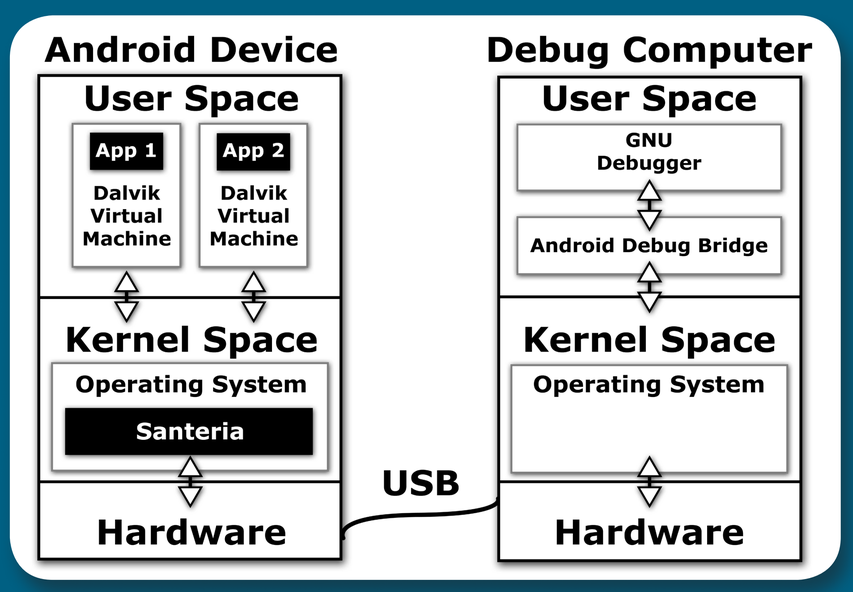
Daming Dominic Chen, Arizona State University;
Alex Bertels, Missouri University of Science and Technology

SAND2012-6017C

Project Mentors: Brandon Eames, 5638; Robert Bell, 5634; Brian Gaines, 5629

Problem Statement:

As the Android mobile platform has proliferated, the need for on-device debugging of applications and system binaries has become more and more important. The development of a hypervisor or kernel-based debug platform assists in achieving this goal.



Overview diagram of the Santeria system

Technical Challenges:

Development of a hypervisor requires low-level debug capabilities, frequently requiring the use of dedicated hardware and software platform emulators. Similarly, kernel modification of ARM interrupt vectors is complex and error-prone.

Tasks on Android Device:

Platform development occurred through several distinct steps, each of which was important to the overall effort.

Task 1: Develop full-duplex USB communication capabilities between debug host and Android device.

Task 2: Develop mobile GDB stub on Android as interpreter for host debug commands.

Task 3: Develop Android kernel module capable of debugging all executable code on the system.

Task 4: Develop ARM-based ELF parser and loader to enable additional plugin development.

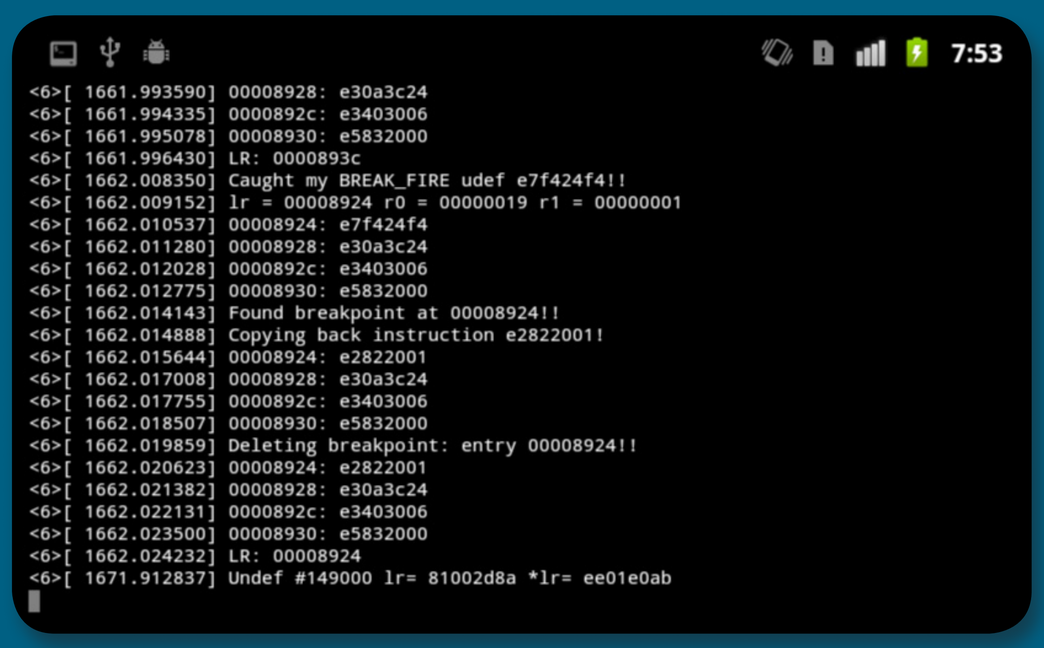
Results:

Task 1: Using built-in socket tunneling functionality, successful full-duplex communication was achieved.

Task 2: An Android application capable of communicating over the GDB remote protocol was developed.

Task 3: A hooker kernel module capable of inserting breakpoints and modifying memory addresses was developed in C and ARM assembly.

Task 4: An external parser and loader was written to load plugins into the debug framework.



Breakpoint being placed and removed from the kernel.

Impact and Benefits:

By providing on-device debugging functionality, malicious software can be easily detected and analyzed. These capabilities allow for dynamic analysis of all executable code on the system, and additionally help ensure flexibility by permitting plugins to be loaded. In summary, these efforts have improved mobile security for the Android platform.

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000. SAND2012-XXXXP.