The Center for Cyber Defenders

Expanding Computer Security Knowledge

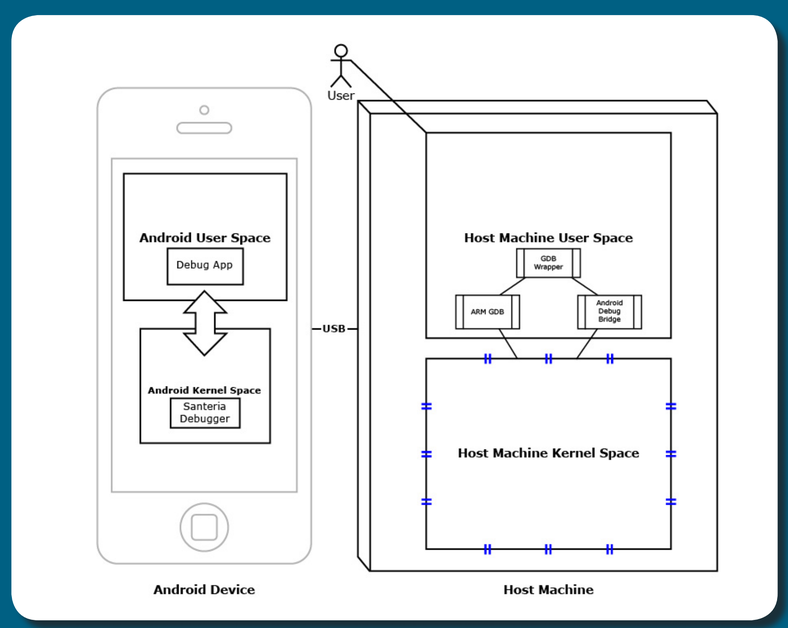
Santeria: An Android Debug Framework

Alex Bertels, Missouri University of Science and Technology;
Wesley Folz, University of Arizona

Project Mentors: Brandon Eames, 5638; Robert Bell, 5634

Problem Statement:

As Android devices are becoming very widely used, the capability to debug the applications and operating system components of these devices is extremely important. A kernel-level debugger, like Santeria, can achieve this capability.



Overview of Santeria system

Objective and Approach:

Task 1: Construct a wrapper for the GNU Debugger (GDB) to send both custom GDB and Android Debug Bridge (ADB) commands to the device.

Task 2: Assemble an environment on a Windows platform to support the execution of the GDB wrapper.

Task 3: Research the use of watchdog timers on an Android device. In particular, learn how to reset the timers and the situations that cause timeouts.

Task 4: Establish communication between the GDB wrapper and the Santeria kernel module on a physical device through USB tethering.

Results:

Task 1: The wrapper can send GDB commands with interpreted symbols as well as send additional modules to the Android device.

Task 2: The GDB wrapper was successfully executed in a Cygwin shell on Windows 7.

Task 3: There is no indication that Android emulators support watchdog timers. Further research is required in order to use watchdog timers on physical devices.

Task 4: The authentication process of kernel modules on a device prevent loading custom modules on some physical devices.

```
wesley@wesley-VirtualBox:~/gdbWrapper$ ./gdbWrapper
840 KB/s (59298 bytes in 0.068s)
Inserting Santeria module
99 KB/s (1137128 bytes in 11.215s)
GNU gdb (GDB) 7.3.1-gg2
Copyright (C) 2011 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.  Type "show copying"
and "show warranty" for details.
This GDB was configured as "--host=x86_64-linux-gnu --target=arm-linux-android".
For bug reporting instructions, please see:
<http://source.android.com/source/report-bugs.html>.
(gdb) Remote debugging using localhost:1024
Remote communication error.  Target disconnected.: Connection reset by peer.
(gdb) Copying output to gdbOutputFile.txt.
(gdb) whereis chmod
c00b1a30 t chmod_common
c00b2538 T sys_fchmod
c00b25a4 T sys_fchmodat
c00b25e0 T sys_chmod
c0104684 T sysfs_chmod_file
c046941c r __ksymtab_sysfs_chmod_file
c046dca0 r __kcrctab_sysfs_chmod_file
c0474d31 r __kstrtab_sysfs_chmod_file
(gdb) whatis c02848b8
dev_watchdog
(gdb) break sys_chmod
Breakpoint 1 at 0xc00b25e0
```

Sample Run of GDB Wrapper Program

Impact and Benefits:

The presence of an in-kernel debugger on a mobile device allows malicious software to be more easily detected and investigated. This capability of dynamic analysis of kernel-level code can drastically increase the security of Android mobile devices.

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. SAND2014-16028D.