The Misuse of Android Unix Domain Sockets and Security Implications

PI: Z. Morley Mao, University of Michigan (zmao@umich.edu)

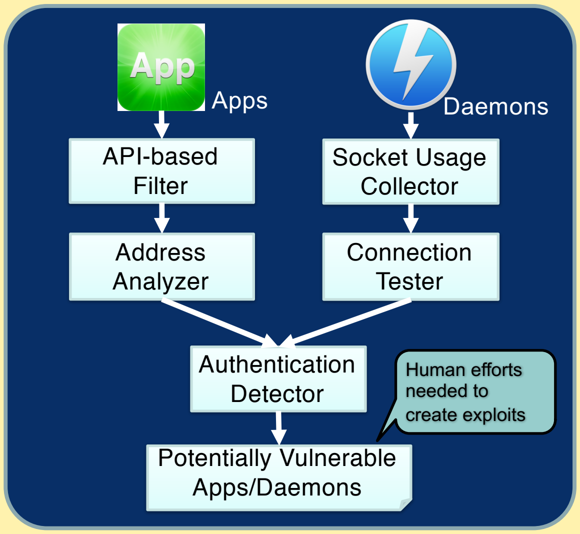
COMPUTER SCIENCE AND ENGINEERING
UNIVERSITY of MICHIGAN

Security properties of the usage of Unix domain sockets on Android remain unstudied

- **Unix domain sockets** is the only Linux IPC that is widely used by both the Android system and apps
- **Inadequate documentation** leaves developers to use them as they see fit
- There is **no systematic study** on security properties of their usage in the wild

Why Unix domain sockets?

- Android is a multi-layered system, cross-layer IPCs are needed
- Unix domain sockets are the first choice
  - Native/Java APIs provided
  - Straightforward client-server model
  - Only INTERNET permission required


App
Apps
Daemons
API-based Filter
Socket Usage Collector
Address Analyzer
Connection Tester
Authentication Detector
Human efforts needed to create exploits
Potentially Vulnerable Apps/Daemons

Approach

Automated analysis

- Performs static analysis on apps to detect potential misuse
- Conducts dynamic testing on daemons' socket channels to discover insecure ones

Key components

- Address Analyzer is able to
  - Find out insecure socket addresses
  - Help classify libraries apps include
- Authentication Detector identifies strong/weak checks that are being enforced

Peer authentication

- Strong checks cannot be bypassed
  - UID/GID/Username/Permission checks
  - Token-based checks
- Weak checks are not reliable
  - PID checks (PIDs are non-deterministic)
  - Proc name checks (Proc name can be spoofed)

Unix domain sockets usage

- There are other purposes in addition to IPC
- Realizing *singleton services/global locks*
  - Addresses are exclusively used by processes
  - **Can be DoS'd**
- Implementing watchdog

Some serious vulnerabilities we found

- KingRoot exposed a socket channel that allowed arbitrary apps to gain root access
- LG AT daemon can be exploited to factory reset the device, and turn on/off SIM card
- ES File Explorer allowed arbitrary file access, including system files on rooted devices

Possible defense solutions

- More fine-grained SEAndroid policies and domain assignment are desired
- Deny direct access to daemons and use a system service as proxy
- Employ token-based checks at both client and server sides

Interested in meeting the PIs? Attach post-it note below!

NSF
National Science Foundation
WHERE DISCOVERIES BEGIN

NSF Secure and Trustworthy Cyberspace Inaugural Principal Investigator Meeting
Nov. 27 -29th 2012
National Harbor, MD