Stealth File Systems for Proactive Forensics Support in Custom Android ROMs

Guide: Dr. Prabhakar Mateti[1]   Sudip Hazra[2]

[1]Wright State University

[2]Amrita Centre For Cyber Security Systems and Networks
Amrita University

15 November 2016

Outline

1. Background
   - Forensic Rom
   - Shortfalls
   - Possible Solutions

2. Proposed Framework
   - File System in User Space
   - Linux Cloud Drive
   - Android Rootkits
   - Stealth File Systems

Outline

1. Background
   - Forensic Rom
   - Shortfalls
   - Possible Solutions

2. Proposed Framework
   - File System in User Space
   - Linux Cloud Drive
   - Android Rootkits
   - Stealth File Systems

Forensic Rom

Work Done Till Now

- Features of Aiyappan Et.al [1] and Karthik Et.al [2] Forensic Rom:
- Captures All User Activities.
- Key-logging and Call Tapping Facility.
- Opportunistically Uploads In Cloud.
- Hiding the Process using hidepid =2.
- Data Stored in /forensic partition only accessible to Root.

Outline

1. Background
   - Forensic Rom
   - Shortfalls
   - Possible Solutions
2. Proposed Framework
   - File System in User Space
   - Linux Cloud Drive
   - Android Rootkits
   - Stealth File Systems

Shortfalls

- What if The Suspect Roots the Phone ?
- Can Find the /forensic Partition.

Outline

1. Background
   - Forensic Rom
   - Shortfalls
   - Possible Solutions
2. Proposed Framework
   - File System in User Space
   - Linux Cloud Drive
   - Android Rootkits
   - Stealth File Systems

Posible Solutions

- Encrypting The /forensic partition can Still arise Suspicion.
- Creating A Fuse File System and enable Stealth Features and Copy all Forensically Relevant Data in that File System.

Outline

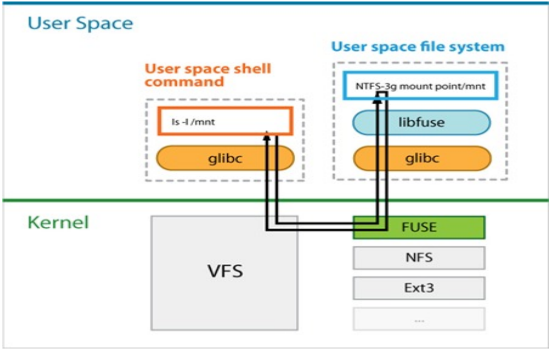
1. Background
    - Forensic Rom
    - Shortfalls
    - Possible Solutions

2. Proposed Framework
    - File System in User Space
    - Linux Cloud Drive
    - Android Rootkits
    - Stealth File Systems

File System in User Space

- The Filesystem in Userspace (FUSE) is a special part of the Linux kernel that allows regular users to make and use their own file-systems without needing to change the kernel or have Root privileges.

Figure : A Fuse Filesystem.



Source:en.wikipedia.org/wiki/Filesystem in Userspace

Outline

1. Background
   - Forensic Rom
   - Shortfalls
   - Possible Solutions

2. Proposed Framework
   - File System in User Space
   - Linux Cloud Drive
   - Android Rootkits
   - Stealth File Systems

Linux Cloud Drive

- Using FUSE we can mount Cloud Drive in Our System and Use it Like a Local File System.
- Gcsfuse: A user-space file system for interacting with Google Cloud Storage.
- Wingfs: A debian Package to mount various cloud storage drives as user-space file systems.
- Azurefs: A python package to mount Azure blob storage as Local File system.

Outline

1 Background

- Forensic Rom
- Shortfalls
- Possible Solutions

2 Proposed Framework

- File System in User Space
- Linux Cloud Drive
- Android Rootkits
- Stealth File Systems

Android Rootkits

- Dong-Hoon Et.al [3] has listed the various ways Rootkits can infect Android Kernel Like:
  - sys_call_table hooking through /dev/kmem access technique.
  - exception vector table modifying hooking techniques.
- Our Objective is to Make the /Forensic Partition a Fuse File system and Hide it using Rootkits.

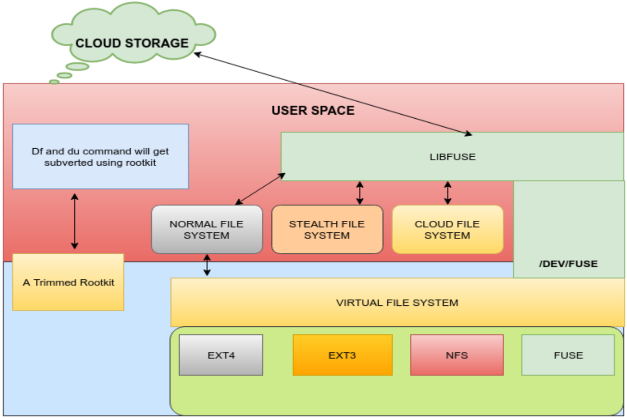
Outline

1. Background
   - Forensic Rom
   - Shortfalls
   - Possible Solutions
2. Proposed Framework
   - File System in User Space
   - Linux Cloud Drive
   - Android Rootkits
   - Stealth File Systems

Stealth File Systems

Proposed Framework

Figure : The Stealth File System Framework.



Summary

Summary

This Framework can effectively Hide the forensic as well as the cloud file system so that even if the Suspect is connecting to adb to check the internal state , He will not be able to find the hidden File systems.

Summary

- Process Hiding can also be Implemented Using this Technique
- The Stealth File-system will periodically copy the forensically relevant data from the normal file system
- This data will be moved to the Mounted Cloud Drive and opportunistically uploaded to the cloud server.
- Outlook
  - Have Developed a High-Level Overview of the Framework.
  - Implementation Needs to be done.

References I

- *Android forensic support framework*, Aiyappan.P Advisor:Prabhaker Mateti, M.Tech thesis, Amrita Vishwa Vidyapeetham,2015
- *Proactive Forensic Support for Android Devices*, Karthik K. Advisor:Prabhaker Mateti M.Tech thesis, Amrita Vishwa Vidyapeetham,2016
- *Android platform based linux kernel rootkit*, Dong-Hoon You, Bong-Nam Noh, Malicious and Unwanted Software (MALWARE), 2011 6th International Conference ,IEEE