Rootkits: Now a Threat to Smartphones

Jeffrey Bickford, Ryan O'Hare, Arati Baliga, Vinod Ganapathy, and Liviu Iftode

Department of Computer Science - Rutgers University

Overview

Rootkits Targeting Unique Interfaces in Smartphones

- Few defenses against malware on smartphones exist
- Smartphones run full operating system with phone software on top
- Rootkits are not new however their transfer to smarthphones is new
- The threat of rootkit attacks targeting specific devices becomes more severe

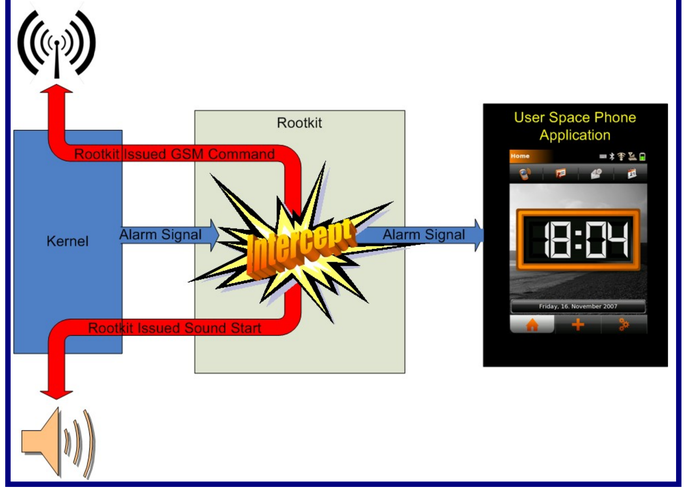
Alarm Attack

Target: Privacy Invasion

- Scenario : You have a meeting
- Attack : Calendar triggers reminder; phone connects to attacker

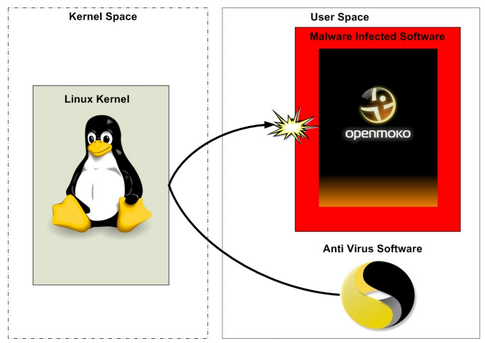
How It Works

- The rootkit watches the system calls issued and waits for one containing the calendar reminder
- When the specific system call is issued the rootkit injects commands that initiate a call to the attacker
- Microphone is able to capture the conversation



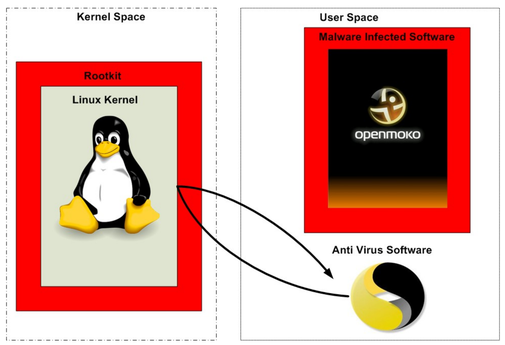
Smartphone Rootkit Concept

User Space Phone Malware



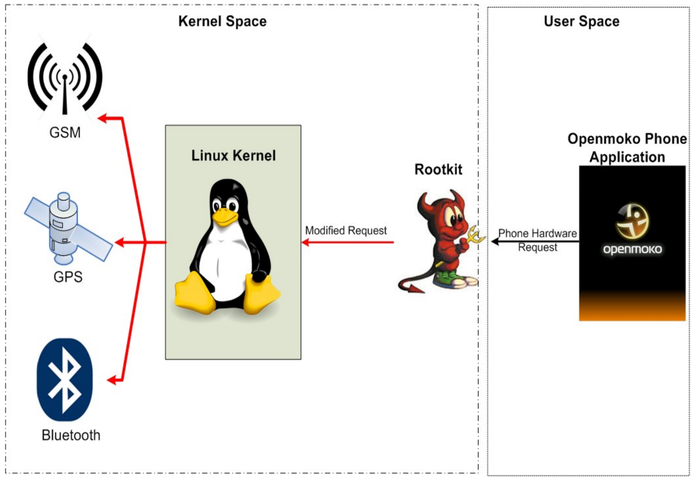
- Traditional malware is detectable by examining the running programs through the kernel

Kernel Space Rootkits



- Rootkits compromise kernel so malware detection is not possible

Smartphone Targeting Rootkits

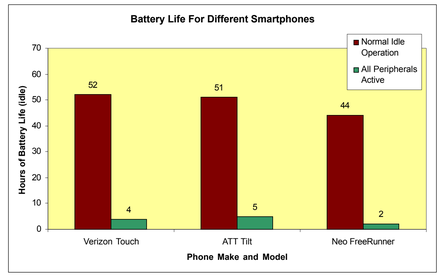


- Rootkits target the kernel by monitoring system calls from within the kernel to filter out the presence of the attack
- User space applications will not be able to detect the rootkits presence
- Rootkit now has direct access the phone's hardware to perform attacks

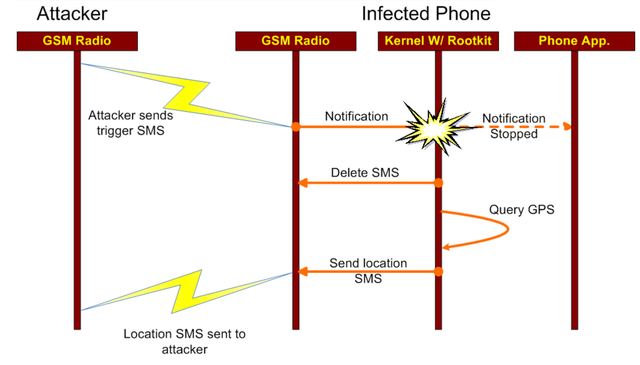
Battery Attack

A phone is only as good as it's battery life

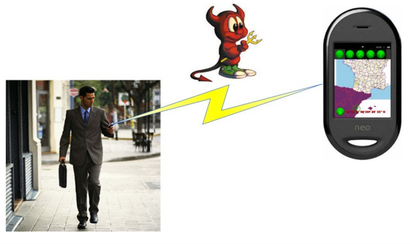
- The rootkit keeps on all the phone's high power devices (Bluetooth and GPS)
- Turns them off temporarily when the user checks their status



GPS Tracking Attack



- Phone receives SMS from attacker



- Rootkit blocks SMS alert
- Location sent to attacker

Reference: "Rootkits on Smart Phones: Attacks, Implications and Opportunities", Proc. HotMobile, February 2010