Final Edge of Poster

Introduction to Android Security & Malware

Intern: Arthur Miller
Mentors: Kurt Derr, Sam Ramirez
Idaho National Laboratory

Objectives

- **Explore the Android O.S. security model**:
  - Security architecture
  - Security vulnerabilities and enhancements
- **Examine Android's defense against malware**:
  - Determine effectiveness of Android's built-in malware scanner.
  - Determine what user information is vulnerable to malicious attacks.

Methods

Method 1: Perform a malware attack

- Two known malicious applications were chosen for testing (AndroRAT and Android Metasploit).
- These applications were installed onto a test device (Galaxy Nexus v4.3) with Android's malware scanner running.
- The applications were then opened on the device, which allowed communication to a remote server.
- Experiments using the application's malware tools were then run.

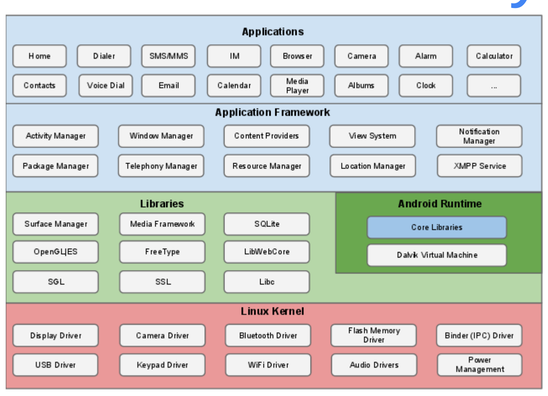
Method 2: Implement an open source mobile device management system (M.D.M.)

- Enforcement policies: password settings, disable camera, disk encryption, data wipe, Wi-Fi settings.
- Other enforcement policies were not allowed without system permissions.

Results

- Deeper understanding of the security architecture of Android O.S.
- SELinux can potentially diminish harm of system and root exploits.
- Android's built in malware scanner did not detect either AndroRAT or Android Metasploit as malware.
- Determined what information an application can gather with app, system, and root permissions.
- Determined capabilities and limitations of Android's Device Admin A.P.I.

Android Security Model



- *Permissions*
- Device Admin A.P.I.

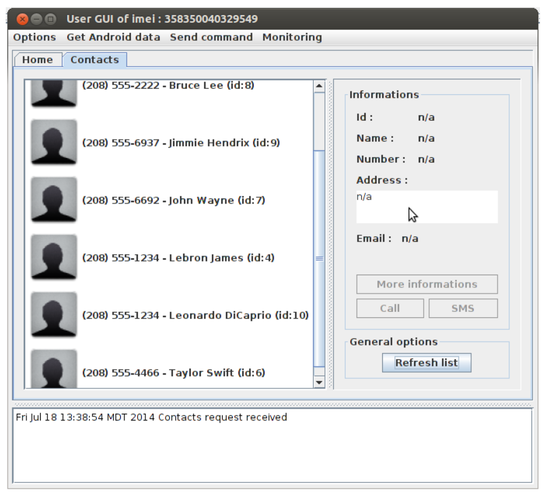
- *Sandboxing**
- SELinux (M.M.A.C.)
- Password's
- Crypto Services

- *SELinux (M.A.C.)***
- Memory Space Protection
- Disk Encryption

Source: Android Security Overview, source.android.com, July 2014.

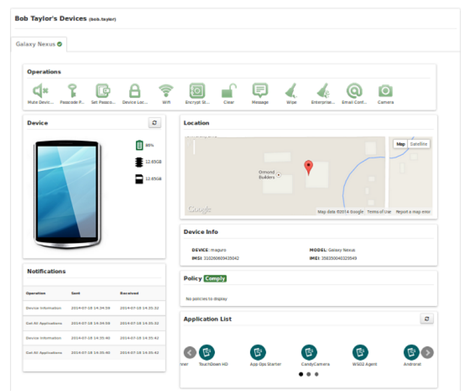
*Each application runs on its own process and is assigned a unique user ID. Inter process communication is handled by the kernel on a permissions allowed basis.
**SELinux implements mandatory access control (M.A.C.) permissions policies. These policies defend against privilege escalation attacks.

Method 1



The AndroRAT server is able to retrieve the contact list of the infected device.

Method 2



WSO2 Enterprise Mobility Manager was the M.D.M. that was implemented. This is the device manager console, as seen in a desktop browser.

Security Enhancements by O.S. Version

	April 30, 2009	September 15, 2009	October 26, 2009	May 20, 2010	December 6, 2010	February 22, 2011	October 19, 2011	(4.1) July 9, 2012 (4.2) November 13, 2012 (4.3) July 24, 2013	October 31, 2013
	Cupcake (1.5)	Doughnut (1.6)	Éclair (2.0-2.1)	Froyo (2.2-2.2.3)	Gingerbread (2.3-2.3.7)	Honeycomb (3.0-3.2.6)	Ice Cream Sandwich (4.0-4.0.4)	Jelly Bean (4.1-4.3.1)	KitKat (4.4-4.4.4)
	Memory Management Enhancements (M.M.E.)	None	None	Device Management A.P.I.	M.M.E.	Full Disk Encryption	M.M.E.	M.M.E., Malware Scanner, Premium SMS Notification, Keystore / Crypto / Certificate Enhancements, Root Processes Limited	M.M.E., SELinux Enforced, Per User VPN, Keystore Additions, Certificate Pinning

Source 1: Security Enhancements, source.android.com, July 2014. Source 2: Android Security Enhancements, androidtamer.com, July 2014.

Final Edge of Poster