



State of Mobile Security

Troy H. Vennon

Manager, Juniper Global Threat Center



Juniper Global Threat Center

- The Juniper Global Threat Center brings proven, methodology-driven analysis of security concepts to mobile devices and operating systems:
 - **Malware Research Team:** Tasked with identifying new Malware threats and device exploits
 - **Exploit Resolution and Integration Team:** Works with the Malware Research Team and Juniper development teams to identify means to mitigate discovered risks and incorporate those solutions into Juniper products
 - **Device Analysis Team:** Analyzes new devices as they are released to identify platform vulnerabilities. Where necessary, this team will ethically disclose any findings or research to the appropriate vendor as a means to address platform or application vulnerabilities that could lead to exploit or compromise.
 - **Device Testing Team:** Conducts testing of threat resolutions, new virus signatures and performance testing of Juniper products across various device platforms.



Mobile Threat Landscape

Malware - Viruses, Worms, Trojans,
Spyware

Direct Attack - Attacking device interfaces,
browser exploits, etc.

Loss and Theft- Accessing sensitive data

Data Communication Interception -
Sniffing data as it is
transmitted and received

Exploitation and Misconduct -
Online predators, pornography,
inappropriate communications

Advances in Malware Development

Symbian/WinMo holds lion's share of mobile malware

- Has seen pirated apps, polymorphic, SMS, spyware, rootkits, similar complexity as PC

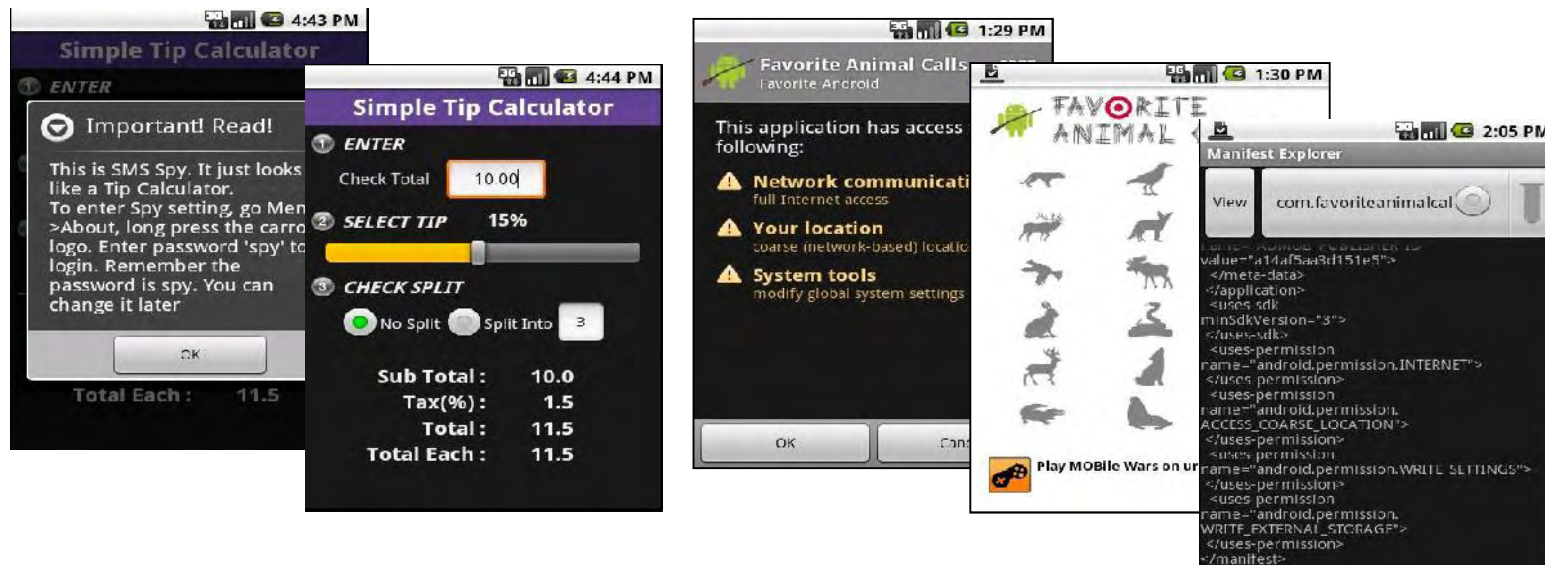
Android currently leading the way in malware research

- Took less than a year to reach complexity of legacy platforms

Android's open approach invites malware developers



The Affect of App Stores



SMS Spy masquerades as “Simple Tip Calculator”

Soundboard app requests unnecessary permissions. Why?



No Platform is Immune

BlackBerry

Commercial Spyware

Threat to
Enterprise/Gov't/SMB

BES Not a Viable Solution

iPhone/iPad

Commercial Spyware

Storm8 Currently Being Sued

3GS Encryption Weaknesses

iPhone 4/iPad Credentials
Stolen in 6 Minutes

NDSS Conference Reveals
Half of iOS Apps Steal Data

iOS Logs Location Data

High Profile Threats



2010/2011 are tough years for Android

Droid 09

Manufacturer Threats

Commercial/App Store Spyware

Tap Snake – First to report

Fake Players

Angry Birds (Oberheide)

High Profile Threats

3rd Party App Stores

Pirating Legitimate Apps

Geinimi

ADRD

PJApps

Myournet – Zero Day Detection



Android Pirated, Arghhh!

Breaking Security Models

Continuing Android Embarrassment

Soundminer

Oberheide & Angry Birds



What to Expect

Research from < 2010 Coming to Fruition

Complex Malware Requires Complex Detection Capabilities

Rootkits

Covert Communication Channels

NFC Payments

Mobile Browser

More Attention on Personal Data Leakage

Direct Attacks at Comm Ports

Lack of Platform Support for Mobile Security

Increased Push into Enterprise

