Ubiquitous and Mobile Computing
CS 403x: Mobile *Malware in the Wild*

Anthony Dresser, Nicholas Kalamvokis, Nicholas Muesch

Computer Science Dept.

Worcester Polytechnic Institute (WPI)

Problem

- Article: A Survey of Mobile Malware in the Wild
- iOS, Android, and Symbian were the largest mobile platforms in 2011
- They were/are all vulnerable to many forms of attack

iPhone 3G (iOS)

Tmobile G2X (Android)

Omnia HD i8910 (Symbian)

Motivation

- Study malware on various mobile platforms
  - iOS, Symbian, Android
- Discuss possible preventions on a per OS basis
  - Permissions
  - Application Signing Process
  - Root privileges/Customization
- Data was used to
  - Understand malware developer's motivation
  - Evaluate how well current defense mechanisms protect phone users
- Propose possible future exploits

Methodology

- Studied 46 Known Mobile Malware
  - 24 Symbian, 18 Android, 4 iOS
  - Public databases of anti-virus companies (At least 2)
  - News releases
- Analyzed the permission of 956 Android 2.2 apps
  - 100 top paid apps
  - 756 most popular free apps
  - 100 most recently uploaded apps

Types of Threats

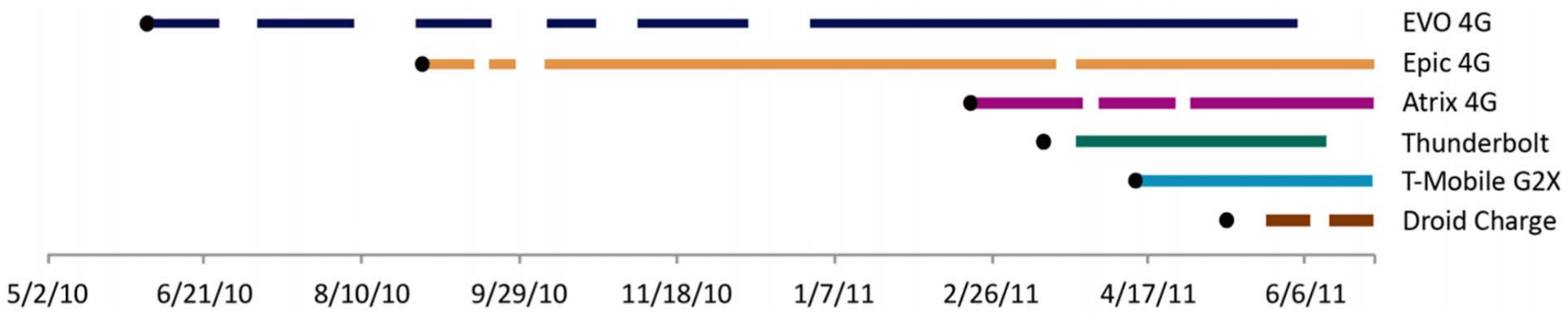
- Malware
  - Gains access through device vulnerabilities
  - Includes Trojans, worms, botnets, and viruses
- Spyware
  - Installed via physical access to the device
  - Collects personal user information
- Grayware
  - Legitimate software that acts as Spyware
  - Barely legal

Malware

- Survey included 24 for Symbian, 18 for Android, and 4 for iOS
- Malware was used to…
  - Collect user information (61%)
  - Send premium-rate SMS (52%)
  - SMS spam (17%)
  - Amusement (13%)
  - Extract user credentials (9%)
  - Search engine optimization fraud (2%)
  - Ransom (2%)

Root Exploits

- Used by consumers to evade phone stock limitations
- Malware developers obtain superuser access in order to bypass security
  - This allows access to parts of the API that are permission protected

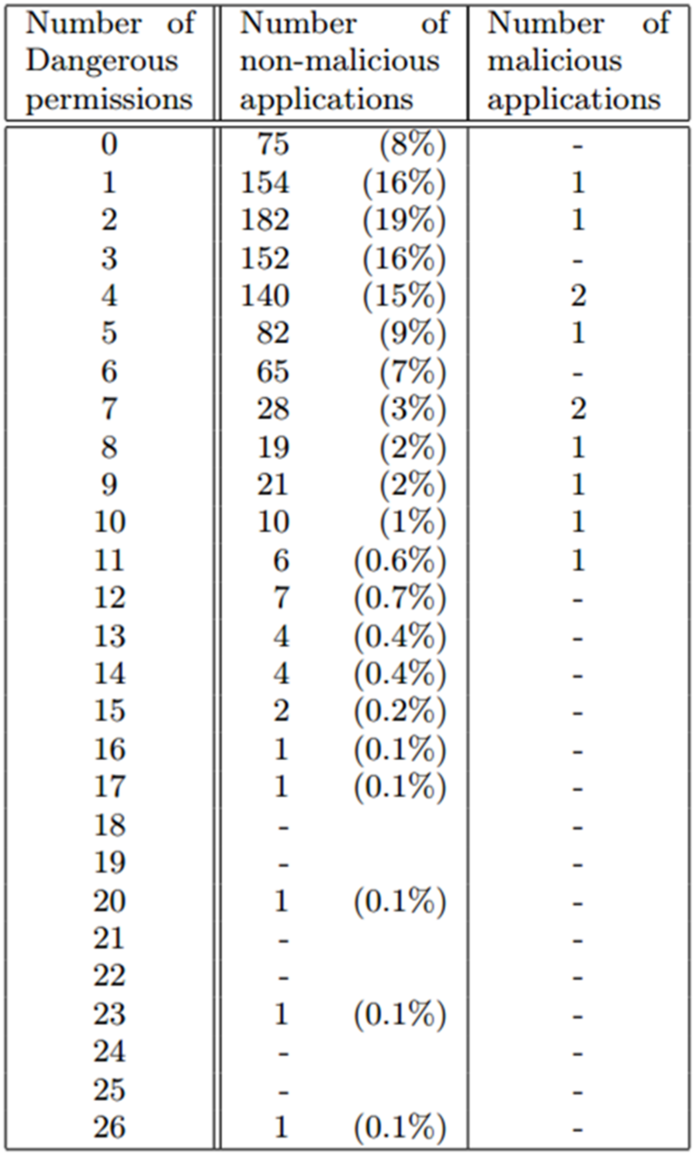


App Marketplaces

- Apple App Store
  - Allows some GrayWare
  - Non-automated app review process (high security)
- Android App Store
  - User complaint driven
  - Unofficial apps can be obtained from other markets
- Symbian (Ovi) App Store
  - Unreliable automated signing process
  - Many other unregulated app markets existed

Android Permissions

- Dangerous Permissions
  - Access to user’s “confidential” data
  - Requires User Auth
  - Camera, Calendar, Location, Contacts, etc
- Hard to correlate number of dangerous permissions to malicious apps



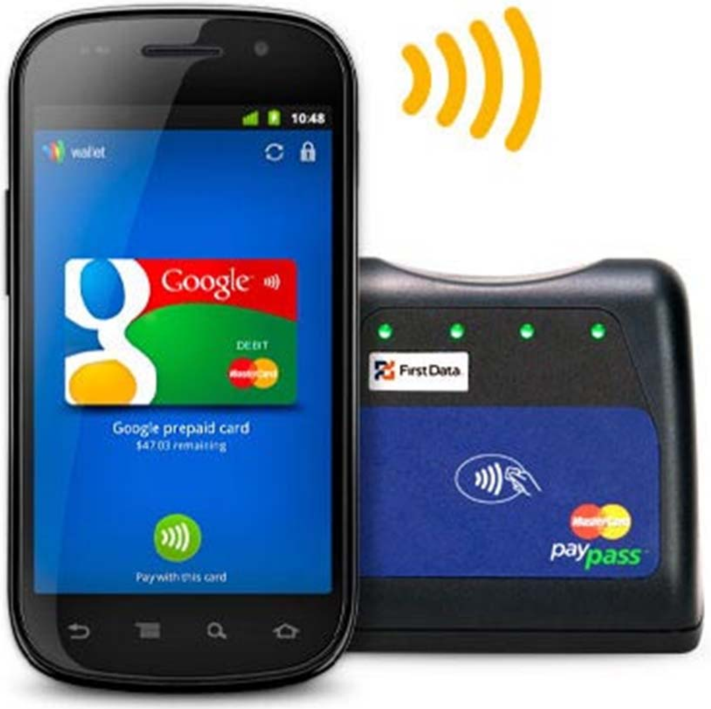
Number of Dangerous permissions	Number of non-malicious applications		Number of malicious applications
0	75	(8%)	-
1	154	(16%)	1
2	182	(19%)	1
3	152	(16%)	-
4	140	(15%)	2
5	82	(9%)	1
6	65	(7%)	-
7	28	(3%)	2
8	19	(2%)	1
9	21	(2%)	1
10	10	(1%)	1
11	6	(0.6%)	1
12	7	(0.7%)	-
13	4	(0.4%)	-
14	4	(0.4%)	-
15	2	(0.2%)	-
16	1	(0.1%)	-
17	1	(0.1%)	-
18	-		-
19	-		-
20	1	(0.1%)	-
21	-		-
22	-		-
23	1	(0.1%)	-
24	-		-
25	-		-
26	1	(0.1%)	-

Suggested Countermeasures

- Allow Users to customize their phones to prevent the need to jailbreak/root
- Use Apple’s review process to deter malware
- Use Android’s Permissions to give the user control over what an application can do.
  - Provide real time permission access over install time
  - Android M does this
- Symbian seems to offer no security valuable features

Future Incentives

- Government - Monitor Citizens
- Distributed Denial of Service (DDoS)
- Advertising Click Fraud
- Invasive Advertising
- In-App Billing Fraud
- Spam
- NFC Credit Card Payments



Related Works

- In 2007, a paper read IRC logs of black market [1]
  - Discovered a compromised desktop sells for $2-$25
- In 2009, researchers estimated 11,750 phones in could reduce network usability by 93% [2]
- In 2011, researchers discussed potential attacks on mobile phones [3]

References/Questions?

- ***A survey of mobile malware in the wild*** Adrienne Porter Felt, Matthew Finifter, Erika Chin, Steve Hanna, and David Wagner in Proc SPSM 2011
- [1] M. Fossi (Editor). Symantec Report on the Underground Economy. Symantec Corporation, 2008.
- [2] P. Traynor, M. Lin, M. Ongtang, V. Rao, T. Jaeger, P. McDaniel, and T. La Porta. On Cellular Botnets: Measuring the Impact of Malicious Devices on a Cellular Network Core. In CCS, 2009.
- [3] M. Becher, F. Freiling, J. Hoffmann, T. Holz, S. Uellenbeck, and C. Wolf. Mobile Security Catching Up? Revealing the Nuts and Bolts of the Security of Mobile Devices. In IEEE Symposium on Security and Privacy, 2011.