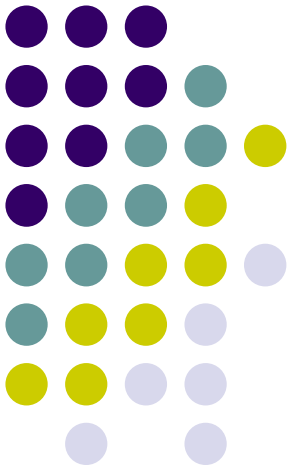
Mobile and Ubiquitous Computing CS 525M: A Survey of Mobile Malware in the Wild

Hiromu Enoki

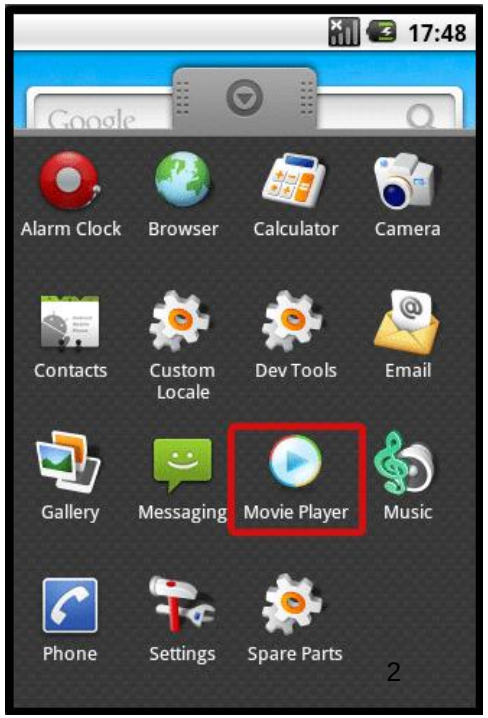
Computer Science Dept.

Worcester Polytechnic Institute (WPI)

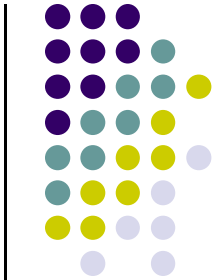


Introduction

- Mobile Malware is fairly recent
  - July 2004 – *Cabir* virus came out on Symbian
  - August 2010 – *Fake Player* on Android
  - July 2012 – *Find and Call* on iOS
- Evolving rapidly
  - Amusement
  - Credential Theft
  - SMS spam
  - Ransomware

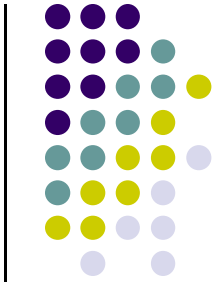


Introduction



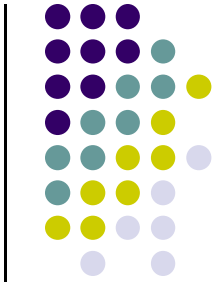
- Sensitive personal information on mobile device
  - E-mail, contacts, passwords…
- Root exploits and Jailbraking
  - Exploits used by both users and adversaries
- Any easy way of defending against malwares?
  - Permissions?
  - OS features?
  - App reviews?

Related Work



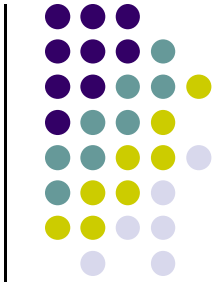
- Extensive research done on PC malwares
- Feasibility and profitability of mobile malware has been researched since 2004
  - Spam, Identity theft, DDoS, wiretapping were predicted
- Malware on other mobile platforms

Background – Application Markets



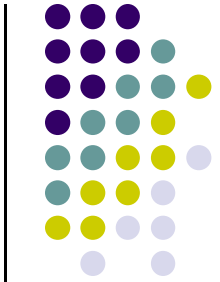
- Apple App Store
  - All applications are reviewed by human
  - iOS devices can only obtain apps through here, unless jailbreaked
- Google Play (Android Market)
  - Some applications may be reviewed
  - Does not restrict installing apps from other markets
- Symbian Ovi
  - Security automatically reviewed by program
  - Risky applications are reviewed by human
  - Can install apps from other markets

Methodology



- Analyzed information about 46 malwares that spread between Jan. 2009 – June 2011
  - 4 – iOS
  - 24 – Symbian
  - 18 – Android
- Information from anti-virus companies and news sources
- Omitted spyware and grayware

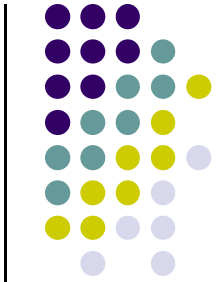
Methodology



- Analyzed permissions of 11 Android malwares
  - Categorized and counted how many permissions they require
  - Attempted to determine malware from permission requests

- Researched on 6 Android devices of root exploits
  - Compared firmware release dates with root hack information on xda-developers

Results



Exfiltrates user information	28
Premium calls or SMS	24
Sends SMS advertisement spam	8
Novelty and amusement	6
Exfiltrates user credentials	4
Search engine optimization	1
Ransom	1

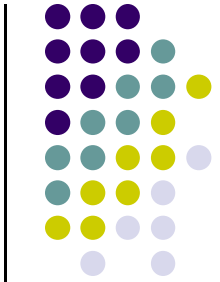
Table 1: We classify 46 pieces of malware by behavior. Some samples exhibit more than one behavior, and every piece of malware exhibits at least one.

Novelty and Amusement

- Minor damage
  - Changing wallpapers, sending annoying SMS

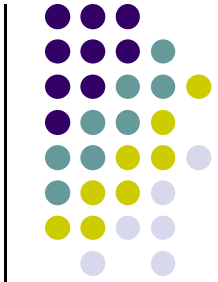
- A preliminary type of malware
  - Expected to decrease in number

Selling User Information



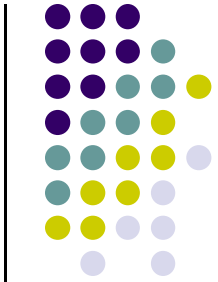
- Personal information obtained via API calls
  - Location, contacts, history, IMEI
- Information can be sold for advertisement
  - $1.90 to $9.50 per user per month
- IMEI information can be used to spoof blacklisted phones

Stealing User Credentials



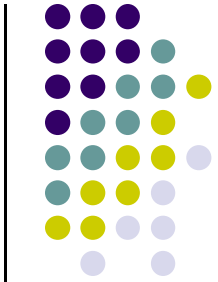
- Malwares can intercept SMS to circumvent two-factor authentication
  - Done in conjunction with phishing on desktops
- Keylogging and scanning documents for passwords
- Application sandboxing prevents most of these

Premium-Rate Calls and SMS



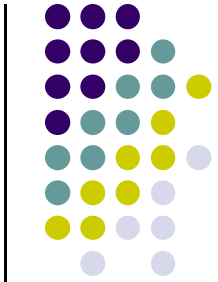
- Premium-rate calls and SMS directly benefits adversaries
  - Few dollars per minute or SMS
- 24 of the 46 malwares send these
  - Mostly on Android and Symbian
- iOS avoids this by always showing confirmation for outgoing SMS messages

SMS Spam



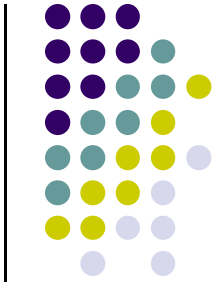
- Distributing spam origin makes blocking harder
- Less noticeable when having unlimited SMS
- Phone numbers are more “reliable” than e-mail
- Can be prevented by enforcing SMS to be sent from a designated confirmation window

Search Engine Optimization (SEO)



- Clicks on a certain link on a search query to increase visibility
- Phishing websites use this technique, along with desktop malware
- Can be prevented with affixing an application-unique tag on the HTTP request
  - Privacy concerns?

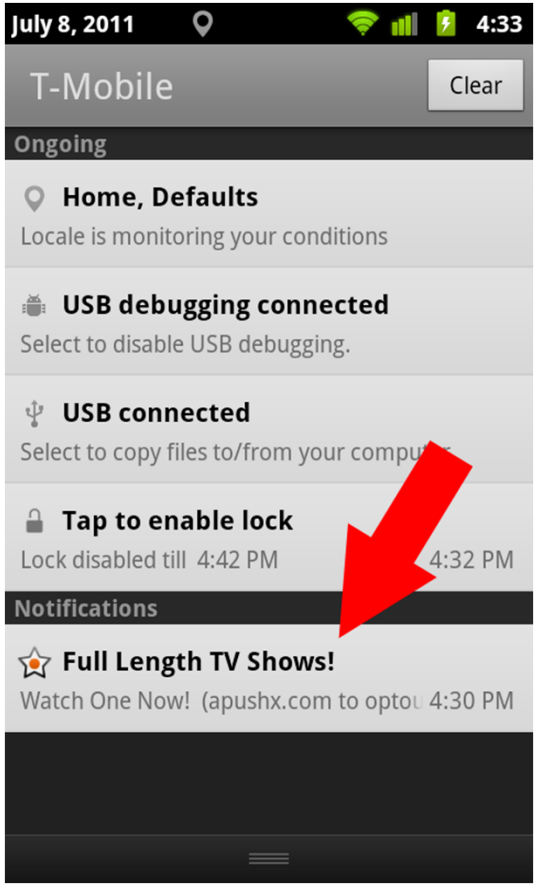
Ransomware



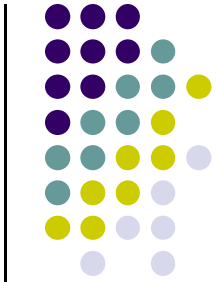
- *Kenzero* – Japanese virus included in pornographic games distributed on the P2P network
  - Asked for Name, Address, Company Name for "registration" of software
  - Asked **5800 Yen** (~$60) to delete information from website (Paper information is wrong)
  - About 661 out of 5510 infections actually paid (12%)
- Not many Ransom malwares on mobile yet….

Possible Future Malware Types

- Advertising Click Fraud
- Invasive Advertising (AirPush)
- In-Application Billing Fraud
- Government spying
- E-mail Spam
- DDoS
- NFC and Credit Cards

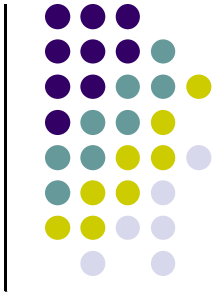


Android Malware Growth



- →Trend Micro PDF
- http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt-evolved-threats-in-a-post-pc-world.pdf

Android Malware Permissions

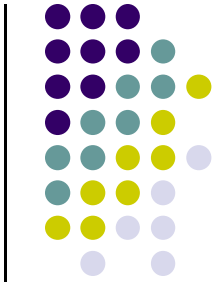


- 8 out of 11 malwares request to send SMS (73%)
  - Only 4% of non-malicious apps ask for this
- READ_PHONE_STATE is used by 8/11 malwares
  - Only 33% for non-malicious apps
- Malware asks on average 6.18 dangerous permissions
  - 3.46 for Non-malicious apps

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%)	-

Table 2: The number of "Dangerous" Android permissions requested by 11 pieces of malware and 956 non-malicious applications [28].

Root Exploits



- *Rooting* allows higher level of customization
  - Installing from unofficial markets
  - System Backups
  - Tethering
  - Uninstalling apps

- However, malwares can take advantage of root commands to obtain permissions

Root Exploits

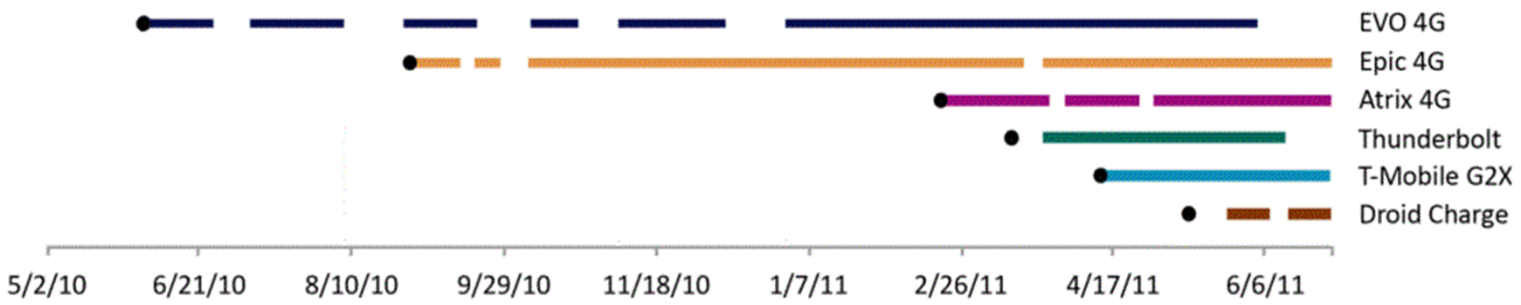
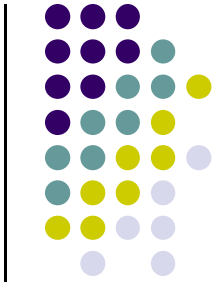


Figure 2: A timeline displaying the dates that known root exploits were available for 6 popular Android phones. Circles mark the release dates of the phones.

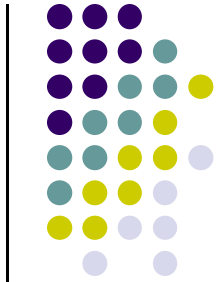
- Root exploits available for 74% of device lifetime
- Malware authors do not need to investigate them, but the community does

Conclusion



- Mobile malware rapidly grew in number
- Profitability is the current trend for malwares
- Defense against mobile malware requires more research
- Human review are effective methods to prevent malware
- Rooting benefits both users and malware producers

Thank You!



- Questions?

References

- *A survey of mobile malware in the wild Adrienne Porter Felt, Matthew Finifter, Erika Chin, Steve Hanna, and David Wagner. in Proc. SPSM 2011.*
- *World's First Android Virus, Nikkei ITPro, http://itpro.nikkeibp.co.jp/article/NEWS/20100816/351137/*
- *Bluetooth-Worm:SymbOS/Cabir, F-Secure Threat Description, http://www.f-secure.com/v-descs/cabir.shtml*

References

- *Find and Call: Leak and Spam, Securelist, http://www.securelist.com/en/blog/208193641/*
- *Kenzero: 40 times more successful than traditional spoofs, http://internet.watch.impress.co.jp/docs/news/20100401_358380.html*
- *AirPush : la publicité dans les notifications qui ressemble à du malware, http://www.frandroid.com/applications/92449_airpush-la-publicite-dans-les-notifications-qui-ressemble-a-du-malware*