6.857 Final Project Proposal: Mobile Device Security

Elizabeth Fong, David Lam, David Wang, & Mark Yen
{lizfong, d_lam201, wang4, markyen}@mit.edu

March 16, 2011

1 Introduction

Mobile devices such as smartphones are becoming increasingly popular, and are set to outstrip sales of PCs for the first time this year. This means that they are also becoming bigger targets for hackers and criminals. One study found that from May to December 2009, malware and spyware on mobile phones doubled from 4% to 9%. Still, consumers are not treating smartphones with the same care as they do with their PCs (few users bother to install anti-virus software on their phones, for instance).[1]

However, the number of vulnerabilities in mobile devices is no less than their desktop counterparts. A test conducted by viaForensics found that 10 out of 12 e-mail applications tested failed to store usernames and other information in a secure way.[2] Also, when communicating over the network, a security professor at Rice University found that Android apps like Facebook and Google Calendar send their information in the clear over the network, even if the accounts are set to always use SSL on the desktop versions.[3]

Finally, loopholes have been discovered in the Android Market which allow malicious applications to automatically download other more malicious apps.[4] Even after the loopholes

[1] Richmond, Riva. "Security to Ward Off Crime on Phones", *The New York Times*, February 23, 2011. http://nyti.ms/f4LQDi

[2] Kolesnikov-Jessop, Sonia. "Hackers Go After the Smartphone", *The New York Times*, February 13, 2011. http://nyti.ms/e0uVmi

[3] Goodin, Dan. "Security shocker: Android apps send private data in clear", *The Register*, February 24, 2011. http://www.theregister.co.uk/2011/02/24/android_phone_privacy_shocker/

[4] Schwartz, Mathew J. "Fake Angry Birds App Exposes Android Vulnerability", *InformationWeek*, November 15, 2010. http://www.informationweek.com/news/security/vulnerabilities/showArticle.jhtml?articleID=228200946

had been patched, it appears that there is little to no screening done on the applications uploaded to the store, and on March 5, Google saw 58 malicious apps uploaded to the Android Market. These apps were corrupted versions of legitimate products, and so they carried names such as Super Guitar Solo, Advanced Barcode Scanner, and Bubble Shoot. Downloaded to around 260,000 devices before Google removed them from the Market, the applications contained malicious code that could compromise personal data such as the IMSI number of the phone.[5] This incident led Google to exercise its previously unused ability to remotely remove applications from its users phones, in order to protect them from the dangerous applications. Google has stated it will be making changes to prevent similar malicious applications from being distributed through those markets, though it did not go into detail on what those changes were.[6]

Another problem is the lack of quality-control in third-party app stores. Google has not officially launched their Android Market in China, so a number of third-party app stores have popped up to fill the void. However, an analysis of those markets found only 61% of those apps to be unique, 36% to be redistributed, and 2% to be pirated.[7] A number of those apps distributed on these third-party app stores are in fact apps repackaged as trojans, which can then hijack certain functions of your phone.[8]

The trend is set to continue. Ed Amoroso, chief security officer at AT&T, has remarked that 2011 is the "eye of the storm", as 4G network speeds start to make hacking more and more attractive to criminals.[9] According to a report from ICSA Labs, "while most hackers heavily focused on Nokia's mobile phones [in 2010], mobile malware will increasingly target non-Nokia devices including Apple, Blackberry, Android, and Microsoft." And according to Adam Powers, CTO of Lancope, "perimeter-based defenses, such as firewalls and IPS, aren't enough anymore. Corporations must think about how they will deal with smart phones, WiFi devices, and other consumer-oriented mobile devices."[10]

---

[5] Ante, Spencer E. and Efrati, Amir. "Google Takes Heat Over App Security", *Wall Street Journal*, March 8, 2011. `http://on.wsj.com/ga73Tn`

[6] Menn, Joseph. "Google disables Android malware", *Financial Times*, March 7, 2011. `http://www.ft.com/cms/s/0/f04a88b8-48ea-11e0-af8c-00144feab49a.html`

[7] Lookout Mobile Security. "App Genome Report", February 2011. `http://bit.ly/idg1tI`

[8] Rothman, Wilson. "Smart phone malware: The six worst offenders", *MSNBC Technolog*, February 16, 2011. `http://technolog.msnbc.msn.com/_news/2011/02/16/6063185-smart-phone-malware-the-six-worst-offenders`

[9] Messmer, Ellen. "Do wireless providers like Verizon and AT&T crimp mobile security?", *Network World*, February 18, 2011. `http://www.networkworld.com/news/2011/021811-verizon-att-mobile-security.html`

[10] Wilson, Tim. "For Hackers, 2011 Looks Like a Prosperous New Year", *Darkreading*, January 3, 2011. `http://www.darkreading.com/security/vulnerabilities/228901590/for-hackers-2011-looks-like-a-prosperous-new-year.html`

For our final project, we have three areas that we plan to investigate:

1. **Network information leakage**: data and personal info that can be gained by a network eavesdropper without direct access to the device
2. **App-to-app security**: protection of sensitive application data from hostile apps residing on the same device
3. **App marketplace security**: determine what types of malware can pass Google's and Apple's checks and become available for download at the official marketplace

2 Network information leakage

For this task, we intend to build on the findings that Dan Wallach (professor of computer security at Rice University) posted on his blog in February.[11] Using Wireshark and Mallory, Wallach tested Facebook, Twitter, several Google apps, and a couple other applications. He found that while Gmail and Google Voice encrypt your traffic, Google Calendar, Google Reader, Google Maps, Google Googles, Twitter, and Facebook send all of their data in the clear, and the data you are currently working with can be intercepted by others monitoring the network traffic.

We plan to start with Facebook, and break down exactly what calls are being made when. From preliminary data gathering, we have determined that several of the calls to the Facebook server are using undocumented parts of the API. We would like to see if we can reconstruct the entire API and make requests against it ourselves. We would also like to see if we can spoof notifications to the mobile device, for instance, chats, messages, or wall posts from arbitrary Facebook users. We would also like to compare the differences between the iOS version of the Facebook application and the Android version of the application. We know from preliminary testing that they use different versions of the API and in some cases different protocols.

The next application we would like to test would be Google Maps, which communicates not only the user's current fine GPS location every few seconds, but also all of the user's friends' locations on Google Latitude. It would be very interesting to see exactly how much and under what conditions this location data is sniffable.

[11] Wallach, Dan. "Things overheard on the WiFi from my Android smartphone, February 22, 2011. `http://shar.es/3UVsP`

3 App-to-app security

4 App marketplace security