

Mobile Pickpocketing

Exfiltration of Sensitive Data through NFC-enabled Mobile Devices

Ryan Caney, Christopher Dorros, Stuart Kennedy, Gregory Owens
Carnegie Mellon University

May 10 2012

1 Introduction

2 Building a Mobile Pickpocketing App

3 Attack Model

4 App Observations

5 Defenses

5.1 Short-term

5.2 Long-term

6 Future Work

7 Conclusions

8 Acknowledgements

References

- [1] Amazon appstore for android. <http://www.amazon.com/b?node=2350149011>. Amazon, [Online; accessed 7-May-2012].
- [2] Identity stronghold. <http://www.idstronghold.com/>. [Online; accessed 7-May-2012].

- [3] The lookout blog: Search results for: chinese data phone. <http://blog.mylookout.com/?s=chinese+data+phone>. Lookout Mobile Security, [Online; accessed 7-May-2012].
- [4] Open nfc: Developer site: Features. <http://open-nfc.org/wp/home/features/>. Open Source, Sponsored by Inside Secure, [Online; accessed 7-May-2012].
- [5] University of pittsburgh: Panther card. <http://www.pc.pitt.edu/card/services.html>. [Online; accessed 7-May-2012].
- [6] Curated app markets could help android security. <http://www.informationweek.com/news/security/mobile/231300342>, August 2011. InformationWeek, [Online; accessed 7-May-2012].
- [7] Electronic pickpocket apps. <http://www.11alive.com/news/article/198946/3/Electronic-pickpocket-apps->, July 2011. WXIA-TV Atlanta, Gannett.
- [8] Farebot: Read data from public transit cards with your nfc-equipped android phone. <http://codebutler.com/announcing-farebot-for-android>, February 2011. posterous SPACES.
- [9] McAfee: Android malware surges 76%, iphone untouched. <http://www.electronista.com/articles/11/08/23/mcafee.shows.android.facing.huge.spike.in.malware>, August 2011. electronista.
- [10] A definitive list of nfc phones. <http://www.nfcworld.com/nfc-phones-list/>, May 2012. Near Field Communications World.
- [11] No more virtual pickpocketing of credit cards, thanks to new tap and pay technology. http://www.eurekalert.org/pub_releases/2012-02/uop-nmv021712.php, February 2012. EurekaAlert!
- [12] BALANZA, M., ALINTANAHIN, K., ABENDAN, O., DIZON, J., AND CARAIG, B. Droiddream-light lurks behind legitimate android apps. In *Malicious and Unwanted Software (MALWARE), 2011 6th International Conference on* (oct. 2011), pp. 73 –78.
- [13] BOULTON, C. Google augments nfc api in android 2.3. <http://www.eweek.com/c/a/Application-Development/Google-Refreshes-NFC-ReaderWriter-API-in-Android-23-739296/>, February 2011. eWeek.
- [14] EMVX. Mastercard aligns with visas u.s. emv migration plans by publishing its own emv implementation roadmap. <http://blog.level2kernel.com/mastercard-us-emv-migration-roadmap/>, February 2012. EmvX Blog, [Online; accessed 7-May-2012].
- [15] GOOGLE. Android developers: Advanced nfc. <https://developer.android.com/guide/topics/nfc/advanced-nfc.html>. [Online; accessed 7-May-2012].

- [16] GOOGLE. Android developers: Nfc basics. <http://developer.android.com/guide/topics/nfc/nfc.html>. [Online; accessed 7-May-2012].
- [17] GOOGLE. Android developers: Sample code: Nfcdemo. <http://developer.android.com/resources/samples/NFCDemo/index.html>. [Online; accessed 7-May-2012].
- [18] GOOGLE. Beaming ndef messages to other devices. <https://developer.android.com/guide/topics/nfc/nfc.html#p2p>. [Online; accessed 7-May-2012].
- [19] GOOGLE. Google wallet: How it works: Security. <http://www.google.com/wallet/how-it-works-security.html>. [Online; accessed 7-May-2012].
- [20] GOOGLE. Coming soon: make your phone your wallet. <http://googleblog.blogspot.com/2011/05/coming-soon-make-your-phone-your-wallet.html>, May 2011. Google: Official Blog.
- [21] GREENBERG, A. Hacker's demo shows how easily credit cards can be read through clothes and wallets. <http://www.forbes.com/sites/andygreenberg/2012/01/30/hackers-demo-shows-how-easily-credit-cards-can-be-read-through-clothes-and-wallets/>, January 2012. Forbes.
- [22] HANCKE, G. Eavesdropping attacks on high-frequency rfid tokens.
- [23] JOHNSONPHONE. Ash (flannelette lint card holder) case pouch bag for samsung nexus s i9020. http://www.ebay.com/itm/Ash-Flannelette-Lint-Card-Holder-Case-Pouch-Bag-For-Samsung-Nexus-S-I9020-/320805691237?pt=PDA_Accessories&hash=item4ab1825f65#ht_2658wt_1038. ebay, [Online; accessed 7-May-2012].
- [24] JUELS, A., MOLNAR, D., AND WAGNER, D. Security and privacy issues in e-passports. In *Proceedings of the First International Conference on Security and Privacy for Emerging Areas in Communications Networks* (Washington, DC, USA, 2005), SECURECOMM '05, IEEE Computer Society, pp. 74–88.
- [25] KEVIN. The lookout blog: Update and clarification of analysis of mobile applications at blackhat 2010. <http://blog.mylookout.com/blog/2010/07/29/mobile-application-analysis-blackhat/>, July 2010. Lookout Mobile Security.
- [26] KFIR, Z., AND WOOL, A. Picking virtual pockets using relay attacks on contactless smartcard. In *Proceedings of the First International Conference on Security and Privacy for Emerging Areas in Communications Networks* (Washington, DC, USA, 2005), SECURECOMM '05, IEEE Computer Society, pp. 47–58.
- [27] KIRSCHENBAUM, I., AND WOOL, A. How to build a low-cost, extended-range rfid skimmer. In *In Proceedings of the 15th USENIX Security Symposium* (2006), pp. 43–57.

- [28] LIFCHITZ, R. Hacking the nfc credit cards for fun and debit. <http://2012.hackitoergosum.org/blog/wp-content/uploads/2012/04/HES-2012-rlifchitz-contactless-payments-insecurity.pdf>, April 2012. Hackito Ergo Sum 2012.
- [29] O’NEIL, Y. T., AND CHIN, E. Seven ways to hang yourself with google android. <https://media.defcon.org/dc-19/presentations/0%27Neil-Chin/DEFCON-19-0%27Neil-Chin-Google-Android.pdf>. [Online; accessed 7-May-2012].
- [30] RAMOS, A., SCOTT, W., SCOTT, W., LLOYD, D., O’LEARY, K., AND WALDO, J. A threat analysis of rfid passports. *Commun. ACM* 52, 12 (December 2009), 38–42.
- [31] SAMMARCO, A. J. Nfc enabling technology. Tech. rep., Device Solutions Inc, November 2010.
- [32] STRONGHOLD, I. Google play: Electronic pickpocket rfid. <https://play.google.com/store/apps/details?id=com.idstronghold.CCReaderMkt&hl=en>. Google, [Online; accessed 7-May-2012].
- [33] TAKAHASHI, D. Updated: Android wallpaper app that takes your data was downloaded by millions. <http://venturebeat.com/2010/07/28/android-wallpaper-app-that-steals-your-data-was-downloaded-by-millions/>, July 2010. Venture Beat.
- [34] WOLFE, H. Are cell phones safe? In *Risk Analysis VII & Brownfields V*, WIT Transactions on Information and Communication Technologies Series. WIT Press, 2010.