

Security and Privacy in Mobile Cloud Under a Citizen's Perspective

Dimitris Geneiatakis^{1(✉)}, Ioannis Kounelis^{1,2}, Jan Loeschner¹,
Igor Nai Fovino¹, and Pasquale Stirparo^{1,2}

¹ Institute for the Protection and Security of the Citizen,
Joint Research Centre (JRC), European Commission, Ispra, VA, Italy

² Royal Institute of Technology (KTH), Stockholm, Sweden

{dimitrios.geneiatakis, ioannis.kounelis, jan.loeschner, igor.nai-fovino,
pasquale.stirparo}@jrc.ec.europa.eu

Abstract. Cloud usage has become a reality in users' everyday habits (even if sometimes unconsciously), and security and privacy issues in this context have already been subject of consideration by scientific, business and policy-makers communities. However, the increasing use of mobile phones, and, generally speaking mobile smart devices, to access the Cloud, introduced recently in the area the concept of Mobile Cloud. Scope of this paper is to address the security and privacy aspects of the mobile cloud phenomenon, under the citizen perspective, taking as driving example the context of commercial mobile transactions.

Keywords: Cloud · Cyber-security · Mobile devices · Mobile cloud

1 Introduction

Cloud usage has become a reality in users' everyday habits (even if sometimes unconsciously) and security and privacy issues in this context have already been subject of consideration by scientific, business and policy-maker communities. However, the increasing use of mobile phones, and, generally speaking, mobile smart devices to access the Cloud, introduced recently in the area the concept of Mobile Cloud. According to a generally well-accepted vision, mobile cloud refers to an infrastructure where both the data storage and data processing happen outside of the mobile device [1]. This view does not indeed add so much to the common view of cloud, in fact, according to it, smart-phones here are seen only as interfaces to get access to the cloud. In the real world, however, the role of smart devices in cloud operations is a lot more than that of mobile interface: smart-phones in fact can be used as storage resource for the cloud, memorizing data and making it available to the cloud when needed. Moreover, they can simultaneously establish mobile-to-mobile direct connections, share directly information and computation results with other phones, and at the same time interact with the traditional cloud. In that sense, especially considering their computational resources (quad-core processors are not rare in this domain), we

believe that mobile phones can and must be considered as full, even if peculiar, nodes of the cloud infrastructure. The criticality of these “special nodes” is generally due to the following considerations:

1. Being mobile by nature, they are exposed full-time to a potentially adverse environment
2. The need, for mobile applications, to cut the development costs to maintain the price appealing for the mobile-application market, is often translated into a quick-prototyping approach, rather than a careful cyber-security oriented code development
3. Being the smart-phone strongly linked to their owner, a successful exploitation of a smart-phone can directly impact the security and privacy of its owner

Scope of this paper is to address the security and privacy aspects of the mobile cloud phenomenon, under the citizen perspective, taking as driving example the context of commercial mobile transactions. Particularly, we focus on cloud services accessed by mobile devices (SaaS - Software as a Service) and the first-level connection between mobile devices and their access point. The structure of the paper is the following: Section 2 describes the reference use case scenario. In Sect. 3 we categorize mobile cloud vulnerabilities in order to map a set of threats on the use case scenario to which the citizen might be exposed (e.g. profiling, proximity marketing and behavioral analysis). In Sect. 4 we use the scenario to present a set of effective countermeasures. Finally, in Sect. 5 we conclude our findings.

2 Use Case Scenario

In order to better demonstrate the risks and threats for a citizen when using a mobile cloud, we base our explanations on the following scenario.

A citizen, Maria, with a mobile device (e.g. an Android smart-phone) is visiting Milan during her vacation. As she is new to the place, she would like to explore the city and see the most well-known monuments and tourist attractions. In order to do so, she uses the mobile application of her choice and using GSM/3G she connects to the Internet and is able to search for sightseeings. She picks up the most common location as her next place to visit, but she then realises that it is too far to go on foot. As a result she buys a ticket for the subway using the corresponding application.

The ticket mobile application is an interface to a cloud through a mobile device. The payment itself is delegated to a third-party payment service, while the ticket company keeps on their servers proof and details of the ticket purchase. The citizen also receives on her phone a valid barcode and NFC tag to be used for ticket control. As a result, before entering on the subway she swipes her phone at the NFC readers, her ticket is validated and she can proceed on using the means of transport.

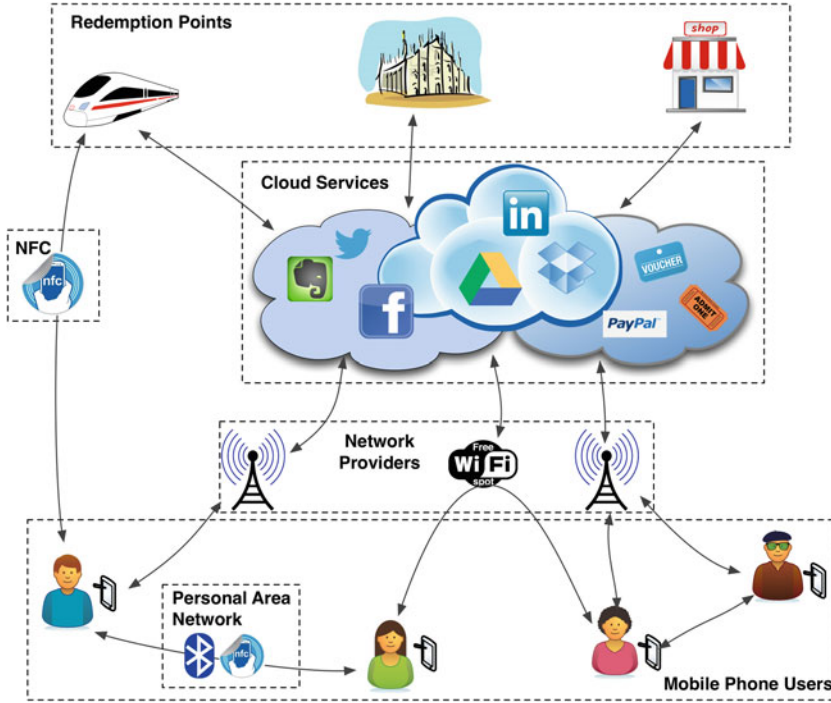


Fig. 1. High level mobile cloud layered interaction scheme

Later that day, she is with her friend in a cafeteria and in order to avoid using the 3G connection, since she has reached the data plan limit, she switches to Wi-Fi connecting to the open wireless network of the shop. While connected she chats with her friends online while in the mean time uses a cloud storage application to send pictures.

Finally, as she had bought by mistake more than one subway ticket, she wants to give one of them to her friend. The tickets are anyway anonymous and no authentication of the user is required. The transfer of the ticket is done over Bluetooth to her friend's device. Her friend can now use the ticket as if she had bought it himself. In this case it is of the ticket provider's interest to be able to verify the validity of the ticket and to also be able not to allow misuse and illegal duplication of the tickets. Figure 1 provides an overview of all the actors, services and infrastructures typically involved in mobile cloud operations.

3 Vulnerabilities and Threats

Scope of this section is to present a general overview of threats and vulnerabilities affecting the mobile cloud infrastructure under a citizen's perspective. We are looking at those vulnerabilities related to the "last mile" of the infrastructure, i.e. the mobile device. As defined by Bishop in his book [2], a threat is a *potential*

violation of security. Such violation does not need actually to occur for there to be a threat. The fact that the violation might occur means that those actions that could cause it to occur must be guarded against (or prepared for). Those actions are called attacks.

3.1 Communication Vulnerabilities

Due to the nature of mobile devices, all communications happen via several wireless communication protocols, and today's smart-phones have deployed on board many different wireless communication capabilities. Unfortunately every (new) feature brings, along with many technological advantages and benefits, a series of vulnerabilities and possible threats. All wireless protocols are prone to the following major classes of threats:

- *Eavesdropping* is the unauthorized interception of information. It is passive, suggesting simply that some entity is listening to the communications. If data is sent unencrypted over any wireless communication channel, eavesdropping becomes very trivial.
- *Spoofing* is the impersonation of one entity by another. It lures a victim into believing that the entity with which it is communicating is a different entity.
- *Tracking* refers to the possibility for an attacker to remotely determine the exact or approximate location of a mobile device. Because mobile devices by their nature emit radio signals and their physical addresses, which have to be both unique and known to communicating parties, that are subject to location-tracking threats.
- *Denial of Service (DoS)*, a long-term inhibition of service, refers to the ability of an attacker to prevent a server from providing a service. The denial may occur at the source or at the destination (by blocking the communications from the server), or along the intermediate path (by discarding messages from either the client or the server, or both).
- *Data Corruption, Manipulation or Insertion* is the result from an entity changing information. Unlike eavesdropping, this threat is active. An example of this could be the man-in-the-middle attack, in which an intruder reads messages from the sender and sends a modified version to the recipient, in hopes that the recipient and sender will not realize the presence of the intermediary.

Although the above listed threats apply to the computer world as well and are not exclusive to the mobile world, the easiness to carry attacks in order to exploit such threats increases drastically in the mobile world, as all wireless communications are broadcasted, therefore lacking of any physical protection mechanism. In the following paragraphs we provide an overview of the major weaknesses affecting the communication channel available in modern smart-phones.

GSM Connections: Vulnerabilities of the GSM protocol are mainly related to serious flaws in the cryptographic algorithms A5/1 and A5/2, other than to the

fact that it authenticates only the subscriber against the network and not vice-versa. Since the first attack against A5/1 proposed by Anderson in 1994 [3], both algorithms A5/1 and A5/2 used for link-level encryption of voice data in GSM have been practically broken [4]. Moreover interception attacks have been shown to be easily possible with off-the-shelf hardware, making feasible to set up a cellular base station to pose as a legitimate one [5]. The price of needed equipment has dropped significantly; with a low budget it is possible to buy the hardware needed such as Universal Software Radio Peripheral (USRP), daughterboard, antennas, etc., while the software to run on top of it is free and open source: OpenBTS and GNURadio. By setting up a fake base station, all the nearby phones could be automatically connected to it, as by default the phones choose to connect to the base station with the most powerful signal. Upon connecting, the attacker can act as a man-in-the-middle, eavesdropping all incoming and outgoing communication and even creating fake ones. It is possible for example, to send a Short Message Service (SMS), SMS Spoofing, or make a call pretending to be a specific number, making the victim believe that someone else is communicating with him/her. In this context, the SMS represents a high risk solution when used as (extra) security feature, e.g. Transaction Authentication Number (mTAN) sent over SMS by the banks to their customers.

Wi-Fi Connections: Wi-Fi is the common name used when referring to the implementation of the standard IEEE 802.11 for wireless local area network (WLAN). Wi-Fi vulnerabilities are mainly related to the authentication method used. Particularly the WEP authentication protocol has been broken due to a flaw found in the RC4 algorithm, which is at the base of WEP. In 2001 Fluhrer et al. [6] demonstrated a weakness in the use of the initialization vectors (IVs) used with RC4, resulting in a passive attack that can recover the RC4 key after eavesdropping on the network.

Near Field Communication Protocol: The NFC is a bidirectional proximity coupling technology, which allows data transfer between devices on a short distance (up to 10 cm). Other than supporting contactless smartcard systems, NFC extends the above with peer-to-peer functionality standardized in [7, 8]. NFC has three operative modes: (1) Reader/Writer, (2) Card Emulation, and (3) Peer-to-Peer. NFC technology, brought to mobile phones, opens new attacks and threats scenarios. According to [9], NFC-enabled devices can be susceptible to threats like eavesdropping, data modification, corruption, insertion, man-in-the-middle (MITM), DoS, and phishing. Although more a design/standard issue than a proper vulnerability, the NFC standard does not offer link level security, a part from NFC-SEC [10] that provides security standard for peer-to-peer NFC communication (does not include reader/writer and card emulation mode [11]), the wireless signal is not encrypted.

3.2 Application Layer Vulnerabilities

According to [1] mobile Internet is expected to overwhelm the usage of land line Internet. This is not only because of evolution of smart-phones and underlying infrastructure, but also due to easy management of the mobile applications. This is supported by mobile applications stores, such as *Google play store*, *Itunes*, etc., which follow the one-stop shop model, where a user can acquire the desired application and install it directly on his phone without any interventions. These stores gain users' trust. Each of these stores before publishing an application scrutinize it for identifying possible malicious activities by using particular security techniques, such as Google's Bouncer.

However, on a side, it's almost impossible to be 100 % secure on the safeness of an application. For instance, in 2012 was presented a technique to bypass *Google's Bouncer* security checks [12]. A similar problem was faced also by *Apple's store* [13]. These facts show that even the existence of security mechanisms at the store side do not guarantee the security (e.g., lack of malicious operations) in the provided applications. On the other side, to make things even worst, end-users can in any case try to install applications from non-verified repositories.

Malicious software (malware) [14] is a type of software designed to manipulate users' data depending on its attributes. Under the umbrella of malware can be found multiple types of malicious software such as backdoors, rootkits, spyware, etc., that might violate users' privacy. In the past malware was affecting mainly the availability or/and the integrity of the information system, while currently it can affect the confidentiality as well. Without loss of generality, mobile malware applications can be classified in two main categories:

Trojanized applications: In this type of malware the attacker is able to modify the application's code and insert the malicious code as illustrated in Fig. 2. Afterwards, the attacker uploads the new modified application in the store, where unsuspecting users can install and use it, without recognizing the malicious operations executed by it. This can be accomplished by using the Soot framework instrumentation tool [15] that enables the reverse engineering Android applica-

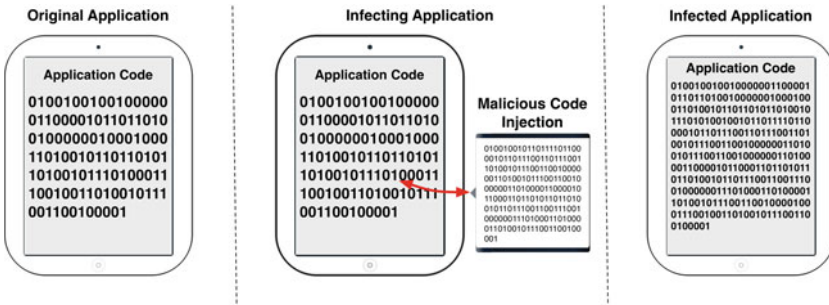


Fig. 2. An example of mobile *trojanized* application

tions. As a result a malicious user can modify the provided application in order to add particular type of code.

Malicious applications: In this type of malware the attacker develops a particular application which is able to manipulate personal data or execute other malicious functionalities on the smart-phone by design (e.g., send out users' photos).

The plethora of personal information managed (created, modified, deleted) by mobile applications, the always online nature of mobile devices and their integration with the cloud, makes the smart-phones, especially in the cloud context, an interesting target for attackers. For example, spying applications can collect user's position or steal his personal contacts and sell them to marketing companies. A detailed analysis for existing mobile malware can be found in [16].

According to Kaspersky security bulletin for 2012 [17] malware main target is smart-phones and particularly those which run Android OS. Consequently, the mobile users have to face the following threats in the context of mobile application security:

Privacy invasion and data loss: the fact that mobile applications manage a wide range of personal information such as unique identifiers, location, call history, text messages, emails, etc., generates new opportunities for profiling users' preferences. Legitimate applications can use personal information to provide powerful features and benefits. However, the opportunity to misuse that information exists as well. This is, for instance, the case of *Twitter application*, which was sending out users' personal information (contacts), without notifying the user [18]. In the worst case scenario personal information can be totally lost if the malware is allowed to execute the corresponding operations. In other cases mobile malware takes the advantage of the fact that applications can be granted with more permissions than what they actually need and consequently can manipulate personal information stored in the phone.

Toll fraud: The malware developers create such software driven by different aims, however, as reported in [16] among main incentives is financial return. In these cases, malware achieves profit by leveraging the mobile phone billing system mainly by sending sms to premium rate services without the users' consent. Alternatively, malware can focus on other financial related applications for exploitation. As illustrated in [19], applications include personal information in different states, which a malicious user is able to extract with existing tools.

Furthermore, considering the fact that smart-phones are becoming the central repository of user's personal data, there is an urgent need for mechanisms protecting the content of mobile devices as high number of phones are lost or stolen. In [19] Stirparo et al. show different techniques in order to extract personal information when you have physical access to a smart-phone. For instance, if a smart-phone is lost a malicious user can root it and data can be extracted via the android device bridge (adb) using the following command.

```
adb pull /system/app/data.dem /tmp/
```

In this example, the malicious user is able to store the file *data.dem* to the */tmp* directory in his computer. Even if the stored information is encrypted

other tools for analyzing operating system's memory can be used in order to identify personal data. Alternatively, this information can be extracted and then decrypted *off-line* using well-know decryption tools, such as the Cain and Abel tool.

3.3 Attack Scenarios

The above mentioned vulnerabilities and threats are not just theoretical but as a matter of fact are in most cases easy to replicate and provide a good investment/profit ratio from the attacker's point of view.

Taking the use case scenario described in Sect. 2, an attacker could be eavesdropping on the GSM network, and therefore interfering with the communication of our character. The attack could either be passive in order to gather information for the victim's physical movements or active altering data of the transaction on the attacker's benefit. In the first case, the attacker could be interested to find out that the victim bought a subway ticket. He may for example be interested in locating the victim and stealing her laptop. In the second case the attack has no physical encounters. It may be a financial attack, stealing the victim's credit card or making her buy tickets from a fake website. Of course, the same two attacks can also occur in the case of the open Wi-Fi network by monitoring the internet traffic or over a Bluetooth local area network in order by sniffing on the transferred files (steal the subway ticket in this case).

Besides financial gain, the attacker may be interested in more indirect attacks. Performing session hijacking to the victim's personal social sites, may result into taking in control her personal digital life. The attacker may be able to alter personal and sometime private information of the victim that will result in harming her public profile. Although these attacks don't have direct economical gain, they occur during personal rivalries or even more important business intelligence.

The passive version of this attack is to monitor the user and profile her. Profiling can also be used for the purposes described above with the only difference that the user usually does not understand that she is been profiled. Profiling refers to collecting user's habits, interests and in general preferences in everyday choices; from the music someone listens to, to the cafeteria she prefers to hang out, etc. This information can be then used combined in order to perform a specific personalised attack on the victim, using in most cases social engineering skills, to gain the victim's trust and then exploit it according to the attacker's interest.

Another attack that can take place is a phishing attack on the NFC tags. An attacker can replace a legitimate NFC tag (the one for ticket validation for example) with a rogue one that injects code on the user's phone and then manages to take control.

Finally, eavesdropping can be performed in a physical way as well. As shown in [20] with a mobile application and a normal camera of an average phone, a user can monitor all the letters the victim is typing from a not so close distance. As a result stealing credentials, personal information or just messages can be

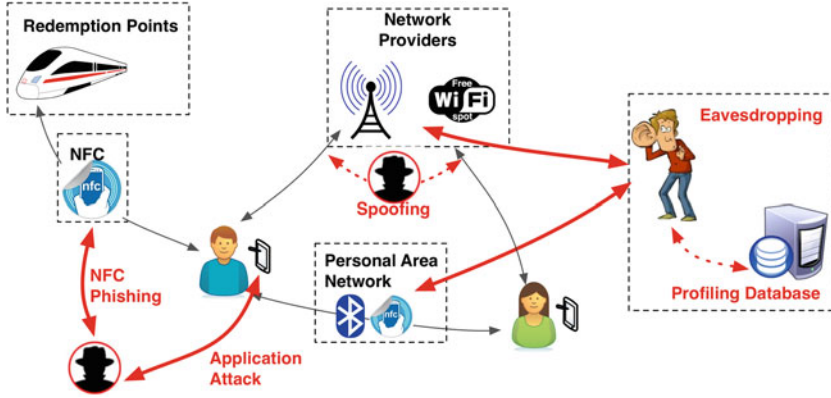


Fig. 3. Attack scenarios

achieved in this way especially in crowded places like means of transport or tourist attractions. All the attack scenarios are illustrated in Fig. 3.

4 Countermeasures

Successful countermeasures aim at preserving the three pillars of security services, also known as the CIA model: confidentiality, integrity, and availability. *Confidentiality* refers to preventing the disclosure of information to unauthorized individuals or systems. Data *integrity* means maintaining and assuring the accuracy and consistency of data over its entire life-cycle and, finally, *availability* refers to the ability to use the information or resource desired. For any information system to serve its purpose, the information must be available when it is needed, therefore the communication channels used to access it must be functioning correctly.

4.1 Communication Layer

To minimize the risk of being victim of attacks targeting vulnerabilities that affect communication protocols, it is important to determine a priori in the design phase which communication protocols will be used in the Cloud architecture that has to be developed and deployed, and therefore applying the proper countermeasures. For example, in order to avoid connecting to a compromised base station, 3G (or 4G if available) connection should always be used. As the 3G protocol allows mutual authentication, the base station will have to be authenticated and thus a compromised base station will not be accepted as a legitimate one.

When moving to Wi-Fi connection, WPA2 must be enforced as compulsory authentication method, since it uses AES-based encryption mode with strong security. As underlined in Sect. 3.1, the specification do not envisage link-level

encryption except for the peer-to-peer mode, therefore it is fundamental that developers implement cryptography in their solutions.

4.2 Applications Layer

To eliminate the risk of personal data manipulation Android and iOS operating systems follow different approaches. Particularly, Android OS provides strong application isolation. By default applications are not allowed to execute functions that affect other applications or the user. Applications have to declare in a manifest all sensitive operations that can be accomplished during their execution, which the user should endorse during installation. Android does not offer any capacity to users for dynamically enabling permissions.

On the other hand, iOS since version five, does not incorporate any functionality to avoid data manipulation. iOS in fact, protects users' data through developer license agreement. In the latest release iOS enables users to enhance the control of their personal data by requiring applications to get explicit permission before accessing them.

However, as described in Sect. 3.2 the underlying security mechanism can be by-passed, thus various researches have been published in order to enhance the security and privacy levels in the mobile platforms. Particularly, [21] focus on the static analysis of the executable part of the mobile application to identify any permission manipulation. An alternative approach is followed by [22–24] in which users are able to define their policies for accessing personal data. Other solutions such as [25] focus on application repackaging. In this approach the compiled applications are analyzed and injected with particular code at the bytecode level in order to monitor all the access of personal data.

4.3 User Behavior

Security measures and mechanisms are developed with the aim to provide protection to the end user. However, it is very often the case that the end user is the weakest link in the security chain. Especially in the case of mobile devices, where the users tend to forget that the smart-phone they are using is not just a telephone but a computer with powerful capabilities. This is either due to the fact that they are not aware of the security risks of mobile applications and how to manage their security and privacy settings [26] or because the extra security features change their user experience and interface in such a way that it makes the original application hard to use. The latter is completely aligned with Saltzer and Schroeder principle of “*psychological acceptability*” [2].

5 Conclusions

Mobile Cloud is the new *frontier* of modern ICT. It represents the most evident proof of the technology convergence that is in act in the telecommunication and, more in general, in the ICT world. On one side the massive use of mobile

devices to get access to the Internet and to perform cloud oriented operations constitutes a great opportunity to deliver new and more advanced services to the citizen. On the other side, the economic model on which the mobile cloud is built, based on cheap mobile applications development, rarely fits with the need for high security level in a field in which citizen's privacy and security should be indeed the most important parameter to be taken under consideration. On top of this, the scarce attention of the end-user to the security issues (in average a smart-phone, for the end-user, is still "only" a phone), is an amplifier for the threats described. In this paper we provided an overview of these threats and of the vulnerabilities affecting the mobile world, under a cloud perspective, providing a set of "best practices" which should help the end-user in mitigating the exposure to the described threats.

References

1. Mobithinking: Global mobile statistics 2013 part a: Mobile subscribers; hand-set market share; mobile operators (2013) [Online]. <http://mobithinking.com/mobile-marketing-tools/latest-mobile-stats/a#subscribers>
2. Bishop, M.: Computer Security: Art and Science. Addison Wesley Professional, Boston (2003)
3. Anderson, R.: A5 (was: Hacking digital phones), Usenet communication on sci.crypt, alt.security and uk.telecom (1994)
4. Barkan, E., Biham, E., Keller, N.: Instant ciphertext-only cryptanalysis of GSM encrypted communication. In: Boneh, D. (ed.) CRYPTO 2003. LNCS, vol. 2729, pp. 600–616. Springer, Heidelberg (2003)
5. Meyer, U., Wetzels, S.: On the impact of gsm encryption and man-in-the-middle attacks on the security of interoperating gsm/umts networks. In: Proceedings of 15th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, PIMRC 2004, vol. 4, pp. 2876–2883 (2004)
6. Fluhrer, S., Mantin, I., Shamir, A.: Weaknesses in the key scheduling algorithm of RC4. In: Vaudenay, S., Youssef, A. (eds.) SAC 2001. LNCS, vol. 2259, pp. 1–24. Springer, Heidelberg (2001)
7. ISO/IEC 18092 / ECMA-340: Near Field Communication Interface and Protocol (NFCIP-1), ECMA International Std. (2004)
8. ISO/IEC 21481 / ECMA-352: Near Field Communication Interface and Protocol (NFCIP-2), ECMA International Std. (2004)
9. Haselsteiner, E., Breitfuß, K.: Security in near field communication (nfc). In: Workshop on RFID Security (2006)
10. NFCIP-1 Security Services and Protocol - Cryptography Standard using ECDH and AES, ECMA International Std. (2008)
11. Coskun, V., Ok, K., Ozdenizci, B.: Near Field Communication (NFC): From Theory to Practice. Wiley, New York (2012)
12. Miller, C., Oberheide, J.: Dissecting the android bouncer (2012) [Online]. <http://jon.oberheide.org/blog/2012/06/21/dissecting-the-android-bouncer/>
13. Ducklin, P.: Apple's app store bypassed by russian hacker, leaving developers out of pocket (2012) [Online]. <http://nakedsecurity.sophos.com/2012/07/14/apple-app-store-bypassed-by-ussian-hacker-leaving-developers-out-of-pocket/>
14. Mell, P., Kent, K., Nusbaum, J.: Guide to Malware Incident Prevention and Handling [Online]. <http://csrc.nist.gov/publications/nistpubs/800-83/SP800-83.pdf>

15. Bartel, A., Klein, J., Le Traon, Y., Monperrus, M.: Dexpler: converting android dalvik bytecode to jimple for static analysis with soot. In: Proceedings of the ACM SIGPLAN International Workshop on State of the Art in Java Program Analysis, SOAP '12, pp. 27–38. ACM, New York (2012)
16. Felt, A.P., Finifter, M., Chin, E., Hanna, S., Wagner, D.: A survey of mobile malware in the wild. In: Proceedings of the 1st ACM Workshop on Security and Privacy in Smartphones and Mobile Devices, SPSM '11, pp. 3–14. ACM, New York (2011)
17. Kaspersky security bulletin 2012. The overall statistics for 2012 [Online]. https://www.securelist.com/en/analysis/204792255/Kaspersky_Security_Bulletin_2012_The_overall_statistics_for_2012
18. Mobile apps take data without permission [Online]. <http://bits.blogs.nytimes.com/2012/02/15/google-and-mobile-apps-take-data-books-without-permission/>
19. Stirparo, P., Kounelis, I.: The mobileak project: forensics methodology for mobile application privacy assessment. In: Proceedings of the International Conference for Internet Technology and Secured Transactions, pp. 297–303. IEEE (2012)
20. Maggi, F., Gasparini, S., Boracchi, G.: A fast eavesdropping attack against touchscreens. In: Proceedings of 7th International Conference on Information Assurance, IAS' 12, pp. 320–325. IEEE December 2011
21. Bartel, A., Klein, J., Le Traon, Y., Monperrus, M.: Automatically securing permission-based software by reducing the attack surface: an application to android. In: Proceedings of the 27th IEEE/ACM International Conference on Automated Software Engineering, ASE, pp. 274–277. ACM, New York (2012)
22. Schreckling, D., Kstler, J., Schaff, M.: Kynoid: real-time enforcement of fine-grained, user-defined, and data-centric security policies for android. Inf. Secur. Tech. Rep. **17**(3), 71–80 (2013)
23. Kodeswaran, P., Nandakumar, V., Kapoor, S., Kamaraju, P., Joshi, A., Mukherjee, S.: Securing enterprise data on smartphones using run time information flow control. In: Proceedings of the 13th International Conference on Mobile Data Management, MDM '12, pp. 300–305. IEEE Computer Society, Washington (2012)
24. Xiao, X., Tillmann, N., Fahndrich, M., De Halleux, J., Moskal, M.: User-aware privacy control via extended static-information-flow analysis. In: Proceedings of the 27th IEEE/ACM International Conference on Automated Software Engineering, ASE, pp. 80–89. ACM, New York (2012)
25. Berthome, P., Fecherolle, T., Guilloteau, N., Lalande, J.F.: Repackaging android applications for auditing access to private data. In: Proceedings of the 7th International Conference on Availability, Reliability and Security (ARES), pp. 388–396 (2012)
26. Felt, A.P., Ha, E., Egelman, S., Haney, A., Chin, E., Wagner, D.: Android permissions: user attention, comprehension, and behavior. In: Proceedings of the Eighth Symposium on Usable Privacy and Security, SOUPS '12, pp. 3:1–3:14. ACM, New York (2012)

Cyber Security and Privacy

Trust in the Digital World and Cyber Security and Privacy

EU Forum 2013, Brussels, Belgium, April 2013, Revised

Selected Papers

Felici, M. (Ed.)

2013, XIV, 177 p. 44 illus., Softcover

ISBN: 978-3-642-41204-2