International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

COPY RIGHT

ELSEVIER
SSRN

IJIEMR Transactions, online available on 18th Dec 2017. Link
:http://www.ijiemr.org/downloads.php?vol=Volume-06&issue=ISSUE-12

Title: **DISTINGUISH THE USER ACTIVITIES BY ANALYZING THE ANDROID ENCRYPTED NETWORK TRAFFIC**

Volume 06, Issue 12, Pages: 576–581.

Paper Authors

V.RAMU
Chaitanya Colleges(Autonomus)

USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

To Secure Your Paper As Per UGC Guidelines We Are Providing A Electronic Bar Code

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

DISTINGUISH THE USER ACTIVITIES BY ANALYZING THE ANDROID ENCRYPTED NETWORK TRAFFIC

V.RAMU
Assistant Professor, Dept. of Computer Science, Chaitanya Colleges(Autonomus)
sriramresearch2019@gmail.com

ABSTRACT: Mobile devices can be maliciously exploited to violate the privacy of people. In most attack scenarios, the adversary takes the local or remote control of the mobile device, by leveraging a vulnerability of the system, hence sending back the collected information to some remote web service. In this paper, we consider a different adversary, who does not interact actively with the mobile device, but he is able to eavesdrop the network traffic of the device from the network side (e.g., controlling a Wi-Fi access point). The fact that the network traffic is often encrypted makes the attack even more challenging. In this paper, we investigate to what extent such an external attacker can identify the specific actions that a user is performing on her mobile apps. We design a system that achieves this goal using advanced machine learning techniques.We built a complete implementation of this system, and we also run a thorough set of experiments, which show that our attack can achieve accuracy and precision higher than 95%, for most of the considered actions. We compared our solution with the three state-of-the-art algorithms, and confirming that our system outperforms all these direct competitors.

INTRODUCTION: The amount of sensitive data that users handle with their mobile devices is truly staggering. People continuously carry these devices with them and use them for daily communication activities, including not only voice calls and SMS, but also emails and social network interactions. A typical user gains access to her savings and checking account by using her smartphone. She installs and uses several apps to communicate with friends or acquaintances. Through her smartphone, she gets information about sensitive topics such as diseases, sexual or religious preferences, etc. As a consequence, several concerns have been raised about the capabilities of these portable devices to invade the privacy of users actually becoming "tracking devices". In this context, an important aspect is related to the possibility of continuously spying and locating an individual. Solutions to identify and isolate malicious code running on smartphones as well as to protect against attacks coming from the network might significantly reduce current threats to user privacy. While people become more familiar with mobile technologies and their related privacy threats, users have started adopting good practices that better adapt to their privacy feeling and understanding. Unfortunately, we believe that even adopting such good practices would not

close the door to malicious adversaries willing to trace people. Indeed, several attacks may violate the privacy of the user even when the adversary does not physically or remotely control the user device. In this paper, we consider a passive attacker that is able to sniff the network traffic of the devices from the network side. Obviously, if the network traffic is not encrypted, the task of such an attacker is simple: he can analyze the payload and read the content of each packet. However, many mobile apps use the Secure Sockets Layer (SSL) – and its successor Transport Layer Security (TLS) – as a building block for encrypted communications. Even when such solutions are in place, the adversary can still infer a significant amount of information from the analysis of the properly encrypted network traffic. For example, work leveraging analysis of encrypted traffic already highlighted the possibility of understanding the apps a user has installed on her device, or identify the presence of a specific user within a network.

This work focuses on understanding whether the user profiling made through analyzing encrypted traffic can be enhanced to understand exactly what actions the user is doing on her phone: as concrete examples, we aim at identifying actions such as the user sending an email, receiving an email, browsing someone profile on a social network, publishing a post or a tweet. The underlying issue we leverage in our work is that SSL and TLS protect the content of a packet, while they do not prevent the detection of networks packets patterns that instead may reveal some sensitive information about the user behavior. An adversary may use our approach in several practical ways to threaten the privacy of the user.

In the following, we report some possible scenarios:

- A censorship government may try to identify a dissident who spreads anti-government propaganda using an anonymous social network account. Comparing the time of the public posts with the time of the actions (inferred with our method), the government can guess the identity of that anonymous dissident.
- By tracing the actions performed by two users, and taking into account the communication latency, an adversary may guess (even if with some probability of error) whether there is a communication between them.Multiple observations could reduce the probability of errors.
- An adversary can build a behavioral profile of a target victim based on the habits of the latter one (e.g., wake up time, work time). For example, this could be used to improve user fingerprinting methods, to infer the presence of a particular user in a network, even when she accesses the network with different types of devices.

EXISTING SYSTEM:

Mobile devices can be maliciously exploited to violate the privacy of people. In most attack scenarios, the adversary takes the local or remote control of the mobile device, by leveraging a vulnerability of the system, hence sending back the collected information to some remote web service.

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

There are disadvantages in existing system they are

- Security is less

PROPOSED SYSTEM: In this paper, we investigate to what extent such an external attacker can identify the specific actions that a user is performing on her mobile apps. We design a system that achieves this goal using advanced machine learning techniques. We built a complete implementation of this system, and we also run a thorough set of experiments, which show that our attack can achieve accuracy and precision higher than 95%, for most of the considered actions. Advantages of our system are:

- Security is more

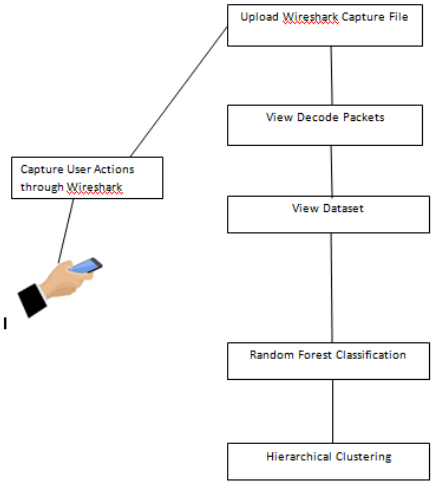

Fig: System Architecture

IMPLEMENTATION: Every implementation is having its own uses. We discussed about the implementation of opinion mining in this paper. They are:

Privacy attacks via traffic analysis: In the literature, several works proposed to track user activities on the web by analyzing unencrypted HTTP requests and responses. With this analysis it was possible to understand user actions inferring interests and habits. More recently, Neasbitt et al. proposed ClickMiner, a tool that reconstructs user-browser interactions. However, in recent years, websites and social networks started to use SSL/TLS encryption protocol, both for web and mobile services. This means that communications between endpoints are encrypted and this type of analysis cannot be performed anymore.

Traffic analysis of mobile devices: Focusing on mobile devices, traffic analysis has been successfully used to detect information leaks, to profile users by their set of installed apps, to find their position, and to generate network profiles to identify Android apps in the HTTP traffic. Traffic analysis has also been used to understand network traffic characteristics, with particular attention to energy saving. It is possible to identify the set of apps installed on an Android device, by eavesdropping the 3G/UMTS traffic that those apps generate. An automatic app profiler that creates the network fingerprint of an Android app relying on packet payload inspection.

CONCLUSION:

The framework proposed in this paper is able to analyze encrypted network traffic and to infer which particular actions the user executed on some apps installed on her mobile-phone. We demonstrated that despite the use of SSL/TLS, our traffic analysis approach is an effective tool that an eavesdropper can leverage to undermine the privacy of mobile users. With this tool an adversary may easily learn habits of the

target users. The adversary may aggregate data of thousands of users in order to gain some commercial or intelligence advantage against some competitor. In addition, a powerful attacker such as a Government, could use these insights in order to deanonimize user actions that may be of particular interest. We hope that this work will shed light on the possible attacks that may undermine the user privacy, and that it will stimulate researchers to work on efficient countermeasures that can also be adopted on mobile devices. These countermeasures may require a kind of trade-off between power efficiency and the required privacy level.

REFERENCES:

1. Androidrank. [Online]. Available: http://www.androidrank.org/, accessed Apr. 1, 2015.
2. (Jan. 2014). Top 15 Most Popular Social Networking Sites. [Online]. Available: http://www.ebizmba.com/articles/social-networking-websites
3. R. Abir. (Mar. 2014). iphone 5s Can Track User's Every Move Even After the Battery Dies. [Online]. Available: http://guardianlv.com/2014/03/iphone5s-can-track-users-every-moveeven-after-the-battery-dies/
4. C. A. Ardagna, M. Conti, M. Leone, and J. Stefa, "An anonymous endto-end communication protocol for mobile cloud environments," IEEE Trans. Services Comput., vol. 7, no. 3, pp. 373–386, Jul./Sep. 2014.
5. G. Ateniese, B. Hitaj, L. V. Mancini, N. V. Verde, and A. Villani, "No place to hide that bytes won't reveal: Sniffing location-based encrypted traffic to track a user's position," in Proc. NSS, 2015.
6. R. Atterer, M. Wnuk, and A. Schmidt, "Knowing the user's every move: User activity tracking for website usability evaluation and implicit interaction," in Proc. ACM WWW, 2006, pp. 203–212.
7. F. Benevenuto, T. Rodrigues, M. Cha, and V. Almeida, "Characterizing user navigation and interactions in online social networks," Inf. Sci., vol. 195, pp. 1–24, Jul. 2012.
8. L. Breiman, "Random forests," Mach. Learn., vol. 45, no. 1, pp. 5–32, Oct. 2001.
9. X. Cai, X. C. Zhang, B. Joshi, and R. Johnson, "Touching from a distance: Website fingerprinting attacks and defenses," in Proc. ACM CCS, 2012, pp. 605–616.
10. S. Chen, R. Wang, X. Wang, and K. Zhang, "Side-channel leaks in Web applications: A reality today, a challenge tomorrow," in Proc. IEEE SP, May 2010, pp. 191–206.
11. M. Conti, N. Dragoni, and S. Gottardo, "MITHYS: Mind the hand you shake—Protecting mobile devices from SSL usage vulnerabilities," in Security and Trust Management. New York, NY, USA: Springer-Verlag, 2013.
12. M. Conti, L. V. Mancini, R. Spolaor, and N. V. Verde, "Can't you hear me knocking: Identification of user actions on Android apps via traffic

analysis," in Proc. ACM CODASPY, 2015, pp. 297–304.
13. S. E. Coull and K. P. Dyer, "Traffic analysis of encrypted messaging services: Apple iMessage and beyond," ACM SIGCOMM Comput. Commun. Rev., 2014, pp. 5–11.
14. S. Dai, A. Tongaonkar, X. Wang, A. Nucci, and D. Song, "NetworkProfiler: Towards automatic fingerprinting of Android apps," in Proc. IEEE INFOCOM, Apr. 2013, pp. 809–817.
15. T. Dierks and E. Rescorla, The Transport Layer Security (TLS) Protocol Version 1.2, document RFC 5246, Aug. 2008.
16. K. P. Dyer, S. E. Coull, T. Ristenpart, and T. Shrimpton, "Peek-a-boo, i still see you: Why efficient traffic analysis countermeasures fail," in Proc. IEEE SP, May 2012, pp. 332–346.
17. W. Enck et al., "TaintDroid: An information-flow tracking system for realtime privacy monitoring on smartphones," in Proc. USENIX OSDI, 2010, pp. 1–6
18. H. Falaki, D. Lymberopoulos, R. Mahajan, S. Kandula, and D. Estrin, "A first look at traffic on smartphones," in Proc. ACM IMC, 2010, pp. 281–287.
19. M. Georgiev, S. Iyengar, S. Jana, R. Anubhai, D. Boneh, and V. Shmatikov, "The most dangerous code in the world: Validating SSL certificates in non-browser software," in Proc. ACM CCS, 2012, pp. 38–49.
20. Y. Go, D. F. Kune, S. Woo, K. Park, and Y. Kim, "Towards accurate accounting of cellular data for TCP retransmission," in Proc. ACM HotMobile, 2013, pp. 1–2.
21. T. Hastie, R. Tibshirani, and J. Friedman, The Elements of Statistical Learning, 2nd ed. New York, NY, USA: Springer-Verlag, 2009.
22. D. Herrmann, R. Wendolsky, and H. Federrath, "Website fingerprinting: Attacking popular privacy enhancing technologies with the multinomial Naïve-Bayes classifier," in Proc. ACM CCSW, 2009, pp. 31–42.
23. B. Krishnamurthy, "Privacy and online social networks: Can colorless green ideas sleep furiously?" IEEE Security Privacy, vol. 11, no. 3, pp. 14–20, May/Jun. 2013.
24. M. Liberatore and B. N. Levine, "Inferring the source of encrypted HTTP connections," in Proc. ACM CCS, 2006, pp. 255–263.
25. X. Luo, P. Zhou, E. W. W. Chan, W. Lee, R. K. C. Chang, and R. Perdisci, "HTTPOS: Sealing information leaks with browser-side obfuscation of encrypted flows," in Proc. NDSS, 2011, pp. 1–21.
26. T. Mitchell, Machine Learning. New York, NY, USA: McGraw-Hill, 1997.
27. M. Müller, Information Retrieval for Music and Motion. New York, NY, USA: Springer-Verlag, 2007.
28. C. Neasbitt, R. Perdisci, K. Li, and T. Nelms, "ClickMiner: Towards forensic reconstruction of user-

browser interactions from network traces," in Proc. ACM CCS, 2014, pp. 1244–1255.
29. A. Panchenko, L. Niessen, A. Zinnen, and T. Engel, "Website fingerprinting in onion routing based anonymization networks," in Proc. ACM WPES, 2011, pp. 103–114.
30. J.-F. Raymond, "Traffic analysis: Protocols, attacks, design issues, and open problems," in Designing Privacy Enhancing Technologies. New York, NY, USA: Springer-Verlag, 2001.
31. B. P. S. Rocha, M. Conti, S. Etalle, and B. Crispo, "Hybrid static-runtime information flow and declassification enforcement," IEEE Trans. Inf. Forensics Security, vol. 8, no. 8, pp. 1294–1305, Aug. 2013.
32. R. Schlegel, K. Zhang, X. Zhou, M. Intwala, A. Kapadia, and X. Wang, "Soundcomber: A stealthy and context-aware sound trojan for smartphones," in Proc. NDSS, 2011, pp. 1–17.
33. F. Schneider, A. Feldmann, B. Krishnamurthy, and W.Willinger, "Understanding online social network usage from a network perspective," in Proc. ACM IMC, 2009, pp. 35–48.
34. D. X. Song, D. Wagner, and X. Tian, "Timing analysis of keystrokes and timing attacks on SSH," in Proc. USENIX SSYM, 2001, pp. 1–17.
35. C. Staff. (Oct. 2014). Germany: U.S. Might Have Monitored Merkel's Phone. [Online]. Available: http://edition.cnn.com/2013/10/23/world/europe/germany-us-merkel-phonemonitoring

V.Ramu
Assistant Professor,
MCA, M.Tech
Dept. of Computer Science
Chaitanya Colleges(Autonomus)
E-Mail :
sriramresearch2019@gmail.com