INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 4 ISSUE 2 (2018) PAGES 3245 - 3250
RECEIVED : 10.03.2018 PUBLISHED : 11.04.2018
April 11, 2018

UNDERSTANDING SMARTPHONE SENSORS AND APLLICATION DATA FOR ENHANCING THE SECURITY OF SECRET QUESTIONS

D.Madhan Kumar[1], S.Mohamed Munaff[2], P.Rajesh[3]

Department of Computer Science and Engineering , Final year B.E,[1,2],Assistant Professor[3], Kingston Engineering College, Vellore, India.

ABSTRACT

In smart city, all kinds of users' data are stored in electronic devices to make everything intelligent. A smartphone is the widely used electronic device and it is the pivot of all smart systems. However,current smart phones are not competent to manage users' sensitive data, and they are facing the privacy leakage caused by data over-collection. Data over-collection, which means smartphones apps collect users' data more than its original function while within the permission scope, is rapidly becoming one of the most serious potential security hazards in smart city. In this paper, we study the current state of data over-collection and study some most frequent data over-collected cases. We present a mobile-cloud framework, Many web applications provide secondary authentication methods, i.e., secret questions (or password recovery questions), to reset the account password when a user's login fails. However, the answers to many such secret questions can be easily guessed by an acquaintance or exposed to a stranger that has access to public online tools we present a Secret-Question based Authentication system, called "Secret- QA", that creates a set of secret questions on basic of people's Smartphone usage. which is an active approach to eradicate the data over-collection. By putting all users' data into a cloud, the security of users' data can be greatly improved. We have done extensive experiments and the experimental results have demonstrated the effectiveness of our approach.

I. INTRODUCTION

Smart city will be the next generation of urbanization. However, it brings some new challenges to be solved, such as security and privacy. The most arduous challenge about the cyber security and privacy of smart city is to ensure sensitive data secure. People living in a smart city and they use all kinds of electronic devices. To make the whole smart city efficiently, almost all these electronic devices need to be smart enough to recognize different users.This project allows the user to provide the security and privacy of smart phone data. The security can be enhanced by understanding the smart phone sensor and app data and also by providing the secret questions. Go Green in the City project of Schneider Electric. The aim of Go Green in the City project is improving and integrating traditional systems into a smart city. Consequently, data are the core of a smart city, because they consist of all users' information, which is invaluable in the Big Data age. Nevertheless, users are suffering the potential privacy leakage when they are enjoying the convenience brought by the smart city.

II. EXISTING SYSTEM

Existing research has revealed that such blank-filling questions created upon the user's long-term history may lead to poor security and reliability. The "security" of a secret question depends on the validity of a hidden assumption: A user's longterm personal history/information is only known by the user himself. A stranger can figure out the answers leaked from public user profiles in online social networks or search engine results. To use various kinds of smart systems in a smart city, residents must offer their personal information to these smart systems. Residents must offer the information of their bank accounting numbers and passwords to shop online.

As a result, the security and privacy of data becomes an important issue to achieve the blueprint of smart city. Current smart phones are not competent to manage users' sensitive data, and they are facing the privacy leakage caused by data over-collection. Data over-collection, which means smartphones apps collect users' data more than its original function while within the permission scope, is rapidly becoming one of the most serious potential security hazards in smart city. In a typical smart city, the security and privacy issue contains several aspects, including security service, sensitive data organization, communication protocol, key management, and authorization.

III. DISADVANTAGES

However, there may be a lot kinds of data leakage in smart city. Consequently, a smart phone is the most widely used electronic devices in smart city, because of its portability. Using smart phones, residents can access to the Internet via everywhere Wi-Fi, take online courses, pay their bill online, sign a contract online, and receive medical treatment by tele -health. The smart phone not only stores users' data, but also generates data. These data may consist of users' accounting numbers and passwords, emails and house addresses, photos, and other kinds of sensitive information.

The "reliability" of a secret question is its memorability, the required effort or difficulty of memorizing the correct answer. Without a careful choice of a blank filling secret question, a user may be declined to log in, because he cannot remember. There is no security for the user data. Sensitive data's are easily get by apps permission. Anyone can access the user mobile. So data's are not secured. The objective is to provide security to smart phone users that we can secure our data by two types password so that hacker cannot retrive data such passwords are image based and sensor based password.

IV. LITERATURE SURVEY

[1] A Study Of Android Application Security, The fluidity of application markets complicate smartphone security. Although recent efforts have shed light on particular security issues, there remains little insight into broader security characteristics of smartphone applications. However, we did not find evidence of malware or exploitable vulnerabilities in the studied applications. We conclude by considering the implications of these preliminary findings and offer directions for future analysis. Constant pool structure, Java applications replicate elements in constant pools within the multiple .class files, e.g., referrer and referent method names. The dx compiler eliminates much of this replication. Additionally, dx eliminates some constants by inlining their values directly into the byte code. Because Dalvik bytecode reuses

registers whose variables are no longer in scope, we must evaluate the register type within its context of the method control flow. Note further that ded type inference is also method-local. Because the types of passed parameters and return values are identified by method signatures, there is no need to search outside the method.

[2] Mobile malware is rapidly becoming a serious threat. In this paper, we survey the current state of mobile malware in the wild. We analyze the incentives behind 46 pieces of iOS, Android, and Symbian malware that spread in the wild from 2009 to 2011. We also use this data set to evaluate the effectiveness of techniques for preventing and identifying mobile malware. After observing that 4 pieces of malware use root exploits to mount sophisticated attacks on Android phones, we also examine the incentives that cause non-malicious smartphone tinkerers to publish root exploits and survey the availability of root exploits. People use smartphones for many of the same purposes as desktop computers: web browsing, social networking, online banking, and more. Smartphones also provide features that are unique to mobile phones, like SMS messaging, constantly-updated location data, and ubiquitous access. As a result of their popularity and functionality, smartphones are a burgeoning target for malicious activities. In order to understand the motives of real mobile malware, we classify the malware in our data set by behavior. We find that the most common malicious activities are collecting user information (61%) and sending premium-rate SMS messages (52%), in addition to malware that was written for novelty or amusement, credential theft, SMS spam, search engine optimization fraud, and ransom. We describe the incentives that promote each type of malicious behavior and present defenses that disincentivize some of the behaviors. We consider whether these mechanisms are effective defenses against the malware in our data set.

[3] A number of web service firms have started to authenticate users via their social knowledge, such as whether they can identify friends from photos. We investigate attacks on such schemes. First, attackers often know a lot about their targets; most people seek to keep sensitive information private from others in their social circle. Against close enemies, social authentication is much less effective. We formally quantify the potential risk of these threats. Second, when photos are used, there is a growing vulnerability to face-recognition algorithms, which are improving all the time. Network analysis can identify hard challenge questions, or tell a social network operator which users could safely use social authentication; but it could make a big difference if photos weren't shared with friends of friends by default. This poses a dilemma for operators: will they tighten their privacy default settings, or will the improvement in security cost too much revenue?

We proposed several ways to mitigate the threats we found. Community based challenge selection can significantly reduce the insider threat; when a user's friends are divided into well-separated communities, we can select one or more recognition subjects from each. We can also avoid subjects with common names or who are known in multiple communities could give a real security improvement.

V. PROPOSED SYSTEM

We develop a prototype on Android Smartphone, and evaluate the security of the secret questions by asking the acquaintance/stranger who participate in our user study to guess the answers with and without the help of online tools. A Secret-Question based Authentication system, called "Secret-QA", taking

advantage of the data of smartphone sensors and apps violating the user privacy user authentication system with a set of secret questions created based on the data of users' short-term smartphone usage.

We evaluated the reliability and security of the three types of secret questions. the combination of multiple lightweight true-false and multiple choice questions required less input effort with the same strength provided by blank-filling questions In a smart city, people needn't to hold a ring with many kinds of keys or to manage various kinds of cards, such as ID card, driving licensee card, and credit card. It can be recognized automatically by smart systems.

Smartphones play irreplaceable role in a smart city. Currently, they can be used as not only communication devices, but also health assistants, work secretaries, entertainment mate, and electronic ID. Putting all users' data into a cloud, the security of users' data can be greatly improved. We present a mobile-cloud framework to solve the data over-collection problem, which immensely improves the security and saves storage space of smart phones. We solve the problem of quantifying security risk and design a benchmark to score apps mainly focusing on data over-collection behaviors. Using this benchmarks, we prove that our framework improves the security of smart phones significantly.

VI. ADVANTAGES

This project allows the user to provide the security and privacy of smart phone data. The secret questions related to motion sensors, calendar, app installment. Part of legacy apps (call) have the best performance in terms of memorability and the attack resilience. the conventional secret-question based approaches that are created based on a user's long-term history/information. Data's are secured. Any where to access user data. Easy to access all user. By using the proposed system ,it is difficult to hack the user data and also hacker cannot fine the secret question also, it improve the security of the user data . The "security" of a secret question depends on the validity of a hidden assumption: So a user's long term personal history/information can be secured efficiently.

VII. ARCHITECTURE DIAGRAM

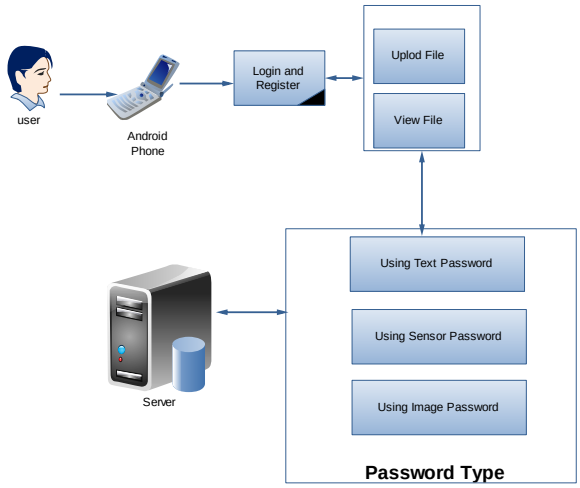

Fig. Architecture diagram

INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 4 ISSUE 2 (2018) PAGES 3245 - 3250
RECEIVED : 10.03.2018 PUBLISHED : 11.04.2018
April 11, 2018

VIII. ALGORITHMS

Every app that wants to use users' data sends its request to the cloud. The cloud access control service provides fine-grained permission authorizations for every app and is in charge of authorizing different permissions for various operations of apps. Smartphone users' data are stored in the cloud storage which can provide various levels of storage solutions for sensitive or normal data. Via en/decryption service, users' encrypted data can be decrypted and sent back to apps.

Algorithm 1 An app stores data into cloud

Input: $appID$, $userID$, $data$.

1: Judge the type of this access request by $appID$, get the result T;
2: **if** $T == hardware$ **then**
3: UR authorize the permission to this app;
4: **else**
5: Send request to Access Control Service including $appID$, $userID$ and $data$;
6: Access Control Service judges whether this app has permission by $appID$, $userID$, $data$ and $accessControlList$, get the result P;
7: **if** $P == true$ **then**
8: Encryption Service encrypts $data$;
9: Store $data$ into Cloud Storage with label $appID$;
10: **else**
11: return;
12: **end if**
13: **end if**

IX. CONCLUSION

Data over-collection in smart phone becomes the most severe potential privacy hazard in smart city. Unlike malwares, data over-collection is difficult to be solved, because this kind of behaviors are within permissions authorized by users. To maximize releasing users' operation pressure and eradicating the data over-collection problem, we presented an active approach. Every app that wanted to use users' data sent its request for accessing to the cloud, and the cloud access control service could provide detailed permissions for every app to every block of users' data. Meanwhile the operations of encryption and decryption were achieved by cloud encryption/decryption service that saves computation resource of smart phone for dealing with these complex calculations. Finally, experimental result verifies the feasibility and advantages of our framework.

REFERENCE

1. W. Enck, P. Gilbert, B.-G. Chun, L. P. Cox, J. Jung, P. McDaniel, and A. N. Sheth, "Taintdroid: An information-flow tracking system for realtime privacy monitoring on smart p ones,"inUSENIX9thConference on Operating Systems Design and Implementation, 2010, pp. 1–6.

2. M. Egele, C. Kruegel, E. Kirda, and G. Vigna, "PiOS: Detecting privacy leaks in iOS applications," in Proceedings of the 18th Annual Network & Distributed System Security Symposium (NDSS), 2011.

3.W. Enck, M. Ongtang, and P. McDaniel, "Understanding Android security," IEEE, Security Privacy, vol. 7, no. 1, pp. 50–57, Jan 2009.

4. W.Enck, D.Octeau, P.McDaniel, and S.Chaudhuri,"A study of Android application security," in Proceedings of the 20th USENIX Conference on Security, ser. SEC'11, 2011.

5. P. Gilbert, B.-G. Chun, L. P. Cox, and J. Jung, "Vision: Automated security validation of mobile apps at app markets," in ACM 2nd International Workshop on Mobile Cloud Computing and Services, 2011, pp. 21–26.

6. N. Sadeh, J. Hong, L. Cranor, I. Fette, P. Kelley, M. Prabaker, and J. Rao,"Understandingandcapturingpeo ple'sprivacypoliciesinamobilesocial networkingapplication,"PersonalUbi quitousComput.,vol.13,no.6,pp. 401– 412, 2009.

7. S. Subashini and V. Kavitha, "Review: A survey on security issues in service delivery models of cloud computing," J. Netw. Comput. Appl., vol. 34, no. 1, pp. 1–11, 2011..

8. Z. Zhou and D. Huang, "Efficient and secure data storage operations for mobile cloud computing," in Proceedings of the 8th International Conference on Network and Service Management, 2012, pp. 37–45.