Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 12, December 2014, pg.16 – 22

RESEARCH ARTICLE

USABLE SECURITY AND PRIVACY IN SMART PHONES

Gousiya Begum[1], P Ram Mohan Rao[2], Dr. K Venkateswara Reddy[3]

[1]CSE Department, MGIT, Hyderabad, INDIA, gousiyabegum@gmail.com
[2]CSE Department, ACE, Hyderabad, INDIA, rammohan04@gmail.com
[3]Principal, MLRITM, Hyderabad, INDIA, drkvreddy2k3@rediffmail.com

Abstract-- In curent Information Security Domain, Usable Privacy is one of the most anticipated area. In this paper we analysed and experimented with a case study to prove the importance and need for usability, privacy and security in a great detail. The main objective of this paper is to emphasize security measures in relevance to usability. We also gathered various experts views and opinions expressed in first International Symposium on Usable Privacy and Security. In this regard we implemented a case study to understand and guide the importance of usable privacy in user interface design with adequate information relevance to security attributes.

Index Terms-- Privacy, Security, Usability, User Interface Design, Android, Permissions

I. INTRODUCTION

Security is the mechanism of protecting data from unauthorized access. Conventionally Security means providing defense against attacks like Interruption, Modification, Integrity, Authentication, Availability etc., where as privacy is the ability of individuals to control the terms under which their personal information is shared. Usability can be defined as the ease of use of a product with effectiveness and efficiency. Today human's personal life relies on Information and Communication Technologies(ICT) in the form of Social networking, communication with friends and colleagues, E-Commerce, banking, Retail etc. Larger part of the society is now dependent on the ICT. It is very clear that the users of ICT need not be Computer Professionals and security becomes hard to understand for these users and also every user expects ease of use. To understand the essence of usable security and privacy, let us consider the following example.

Let us assume there is an email application which is asking its users to change their passwords once in a month for the sake of additional security. Changing of passwords monthly is tedious for the user because they cannot use old passwords and they have think of new passwords and also remember them. Now the usability comes into picture as the user may not feel comfortable with the security feature imposed on him. Since the user has to change passwords regularly, the user may start using dictionary words so that he can remember easily. Using dictionary words as passwords will not enhance security rather it is easy to break such passwords. Hence in the process of increasing the security for the application we end up making it more insecure. As a result when security becomes clumsy, end users may knowingly or unknowingly compromise the computer systems and contribute to the release of private and confidential information.

Challenges in usable privacy and security

Security is not limited to computer systems. Today user base of computer systems has drastically increased because of the availability of Internet and Smart Phones. Emergence of social networks has increased attention of all kinds of people towards information systems. Internet banking, E-commerce have become part of our life. So the people started using Internet and other web applications. Many of them are not aware of any security or privacy issues.

Some of the key challenges in Usable Privacy are

a. Conventional Security Framework is to be changed since the availability of information is not just limited to computers. There is a need for new methodologies and enough economy allocation.
b. Generally when an application is developed the user interface design is carried out by Design Experts whose goal is to provide easy to use environment. Their interest towards security attributes is very less. Security Providers and User Interface Designers they do not work together.
c. Lack of awareness among users in maintaining privacy. Sometimes added security makes application difficult to use.
d. There is an immense need of understanding the Psychology of the users and as well as the Psychology of the attackers because firewalls, passwords and other security measures are proved to be inadequate.
e. No standards and policies for website and web application development.
f. No metrics of how usable and secure a system is

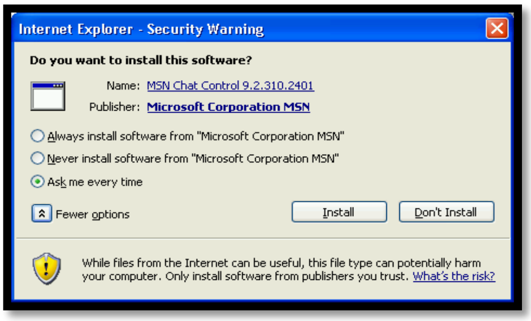
Abbreviations and Acronyms

ICT Information and Communication Technology
CUPS CyLab Usable Privacy and Security Laboratory

II. RELATED WORK

The challenges mentioned above were framed based on the experiments done to identify the need for Usable Security and Privacy.

1. **Not Privacy Sensible:** A group of 120 Engineering students from various streams were asked to fill in a registration form in order to get their email id. We made an attempt to crack their passwords. Before this we have gone through the Orkut and Facebook profiles of these students. We could crack one password by using profile information. One student was using her pet's name followed by year of birth. which we found in her orkut profile and we were able to crack the password. Hence it is very clear that the users are not privacy sensible.
2. **SQL Injection and XSS attacks:** These are still used to get some useful information of users. Now-a-days people are registering their information in many web applications and web sites. It has been noticed that all web applications and websites are not safe and secure enough, a SQL Injection attack can be made to retrieve personal information of the users which in turn can be used to access other web sites where lot of sensible data is stored. Here there is a need for universal standards.
3. **Lack of Awareness:** Many end Users are not aware of security threats and may unknowingly become victim of a security attack which may lead to information theft. For example, every day people download many software's which are free to use but many of them don't know what exactly that software is doing in the background. It may steal personal information and send to some remote server.



Internet Explorer - Security Warning

Do you want to install this software?

Name: MSN Chat Control 9.2.310.2401
Publisher: Microsoft Corporation MSN

○ Always install software from "Microsoft Corporation MSN"
○ Never install software from "Microsoft Corporation MSN"
● Ask me every time

While files from the Internet can be useful, this file type can potentially harm your computer. Only install software from publishers you trust. What's the risk?

Fig. 1 Security Warning

In this context it is not in correct to suspect even an antivirus program since it can also access the memory

4. Psychological impact: End users of any application always expect an easy to use interface which is also proved to be a cause for stealing private information. For example little attention is paid to the URL's. An end user will always prefer to click the URL which is sent as part of an email without checking its authenticity. It is safe practice to type URL's manually rather than using URL's found in email attachment. Unfortunately end users feel comfortable in clicking the URL. The following URL was sent to four people asking them to update their profile information. The URL below is routed to a local web server and successfully collected usernames and passwords of the four users. http://www.okrut.com/servicauthlogin/675898765543333 . So user's psychology is also an important factor in developing a secure usable interface.

Modern Threat in the form of SMART PHONE

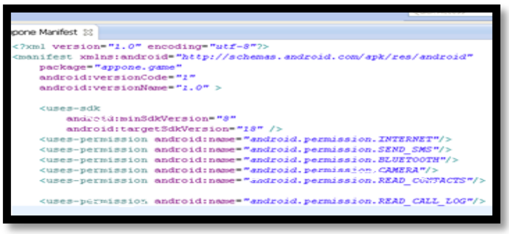
Today computer system is almost replaced by Smart Phones. Smart Phones are used in E-commerce, retail, online gaming, Banking services and many more. All these things are achieved with the help of Internet and apps. Day in – day out thousands of apps are being developed and delivered for free. Users obviously download them and use. Maximum Smart Phone users do not know the technical details of the Phone and its memory hierarchy. It has been observed that the young students form a major user base of Smart Phones especially for gaming purpose. Phone contains lot of personal information like contacts, pictures, videos etc. so ensuring privacy and providing security to the personal data is highly required. Many of the Smart Phone Users are not aware of the risk involved in downloading apps specifically which are free.

Many users don't even know the permissions that an app requests before getting downloaded. When an app is downloaded, users show least interest in reading the license agreements or any other notifications also. Previous research shows that only 15 – 17% of android users are aware of the permission that an app demands [1].

Typical Permissions in any mobile OS include

1. *Network Access*
2. *Access to call log*
3. *Access to internal storage*
4. *Access to external storage*
5. *Access to contacts and media*

Very common type of access that gaming apps use are location tracking and sharing [2] [3] [4]. Most often the users are not aware of it. Many apps do not give proper notifications about the permissions. If some apps request some types of permissions the users may misinterpret them. For example SEND_SMS request is made by an app, the user may think that this app will allow him to send SMS messages. But the fact is the app is requesting to access text messages and in turn forward them to the app developer.



```
<?xml version="1.0" encoding="utf-8"?>
<manifest xmlns:android="http://schemas.android.com/apk/res/android"
    package="appone.game"
    android:versionCode="1"
    android:versionName="1.0" >

    <uses-sdk
        android:minSdkVersion="8"
        android:targetSdkVersion="18" />
    <uses-permission android:name="android.permission.INTERNET"/>
    <uses-permission android:name="android.permission.SEND_SMS"/>
    <uses-permission android:name="android.permission.BLUETOOTH"/>
    <uses-permission android:name="android.permission.CAMERA"/>
    <uses-permission android:name="android.permission.READ_CONTACTS"/>

    <uses-permission android:name="android.permission.READ_CALL_LOG"/>
```

Fig. 2 Android Manifest File

Dangerous Permissions in ANDROID

So it is difficult to ensure security and privacy to personal data in smart phone especially when user's awareness towards privacy preservation is less. Apart from this, Stealing information from Smart Phone is much easier as there are no enough standards and regulations monitoring these apps. Conventional security mechanisms followed by Network Administrators and System Administrators cannot be applied to Smart Phones.

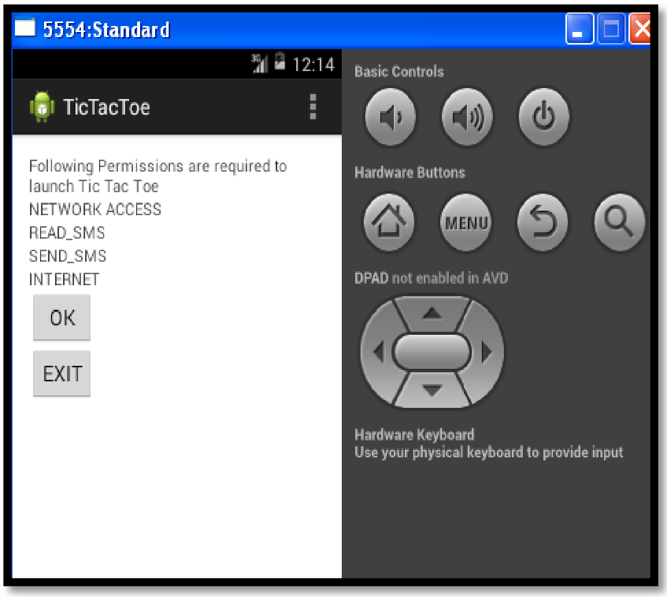
Android API is also a vulnerable to variety of security threats. Users and even developers may not be aware of the Android API framework. Android API contains a public library and private interface which is based on Remote Procedure Calls. Using Java Reflection API one can access the hidden and private classes of Android Framework.[5]

III. DESIGN AND IMPLEMENTATION

CASE STUDY

It is highly required to provide a user friendly interface while ensuring the security and privacy for user data residing in the memory. There is need to carry out research in a new dimension i.e. Usable Privacy.
Security and Usability should go hand in hand. We have done an experiment on 174 engineering students as participants and found surprising results. Our work is described below.

We developed an app using Android SDK and the .apk file was distributed to 174 students. The app was basically a Tic TacToe game for the user and internally it contains code which will access the text messages and forward them to our email account. We gave clear instructions before launching the game regarding permissions.



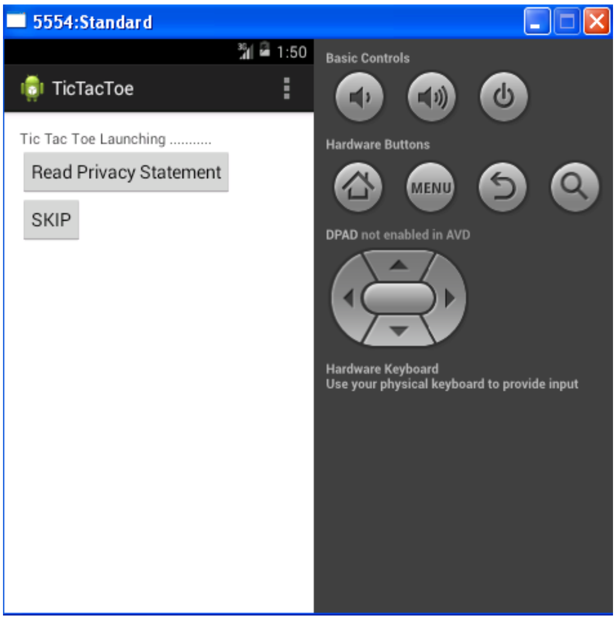
Following Permissions are required to launch Tic Tac Toe
NETWORK ACCESS
READ_SMS
SEND_SMS
INTERNET

Fig. 3 TicTacToe Launching

The above screen is the initial screen before the TICTACTOE game launches. It has got two buttons. Read Privacy Statement and SKIP.

When User Clicks on Read Privacy Statement

Button it will show the list of all permissions the app demands. If user agrees for the same then the app will be loaded otherwise not.



Tic Tac Toe Launching ....

Fig. 4 Permissions requested by TICTACTOE App

If the user does not want to read privacy statement, can also skip them using SKIP button. Out of 174 participants, only 32 participants have clicked the Read Privacy Statement button and remaining have skipped.32 participants who have clicked the Read Privacy Statement button, only 28 participants have read each and every permission request out of which only 13 participants did not agree for the permissions demanded by the app.

142 participants ignored reading privacy statement reflects the kind of the attitude user show towards downloading apps. Users typically do not have patience to read the license agreements and privacy statements. The participants in our case study are computer literates and had enough awareness on security and privacy issues, still the participants were reluctant in reading the privacy statement. It is very clear user always wants a simple usable interface and does not like to read any license agreements or privacy statements. In our case study our app was able to access the text messages of the users. The

text messages of the users were also forwarded to our email account. If the users are not aware of any security and privacy issues then it becomes very easy to steal data from their smart phones. Many of these attacks are passive attacks.

Various trends of user's behavior towards our case study is described in the graph below.

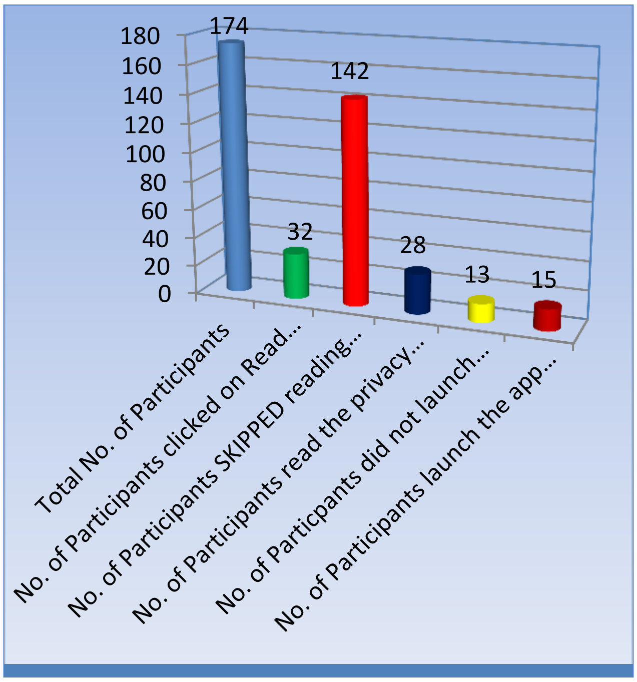


Fig. 5 Participants Behaviour

Fig. 6Participants Playing TICTACTOE APP

The results are really surprising as 81.6% participants have skipped reading the privacy statement. Only 16% of participants have read the privacy statement and 53% of it have launched the app even after reading the privacy statement.

IV. CONCLUSION

Based on the results of the case study following Observations and recommendations are made

1. User Interface Design should be carried out by considering all security and privacy attributes. User Interface Designers, Security Professionals and Psychology experts should work together in providing a user friendly application simultaneously providing privacy controls to the user. This is a new area of research which enables Usable Privacy.

2. Creating Awareness among Users: It is immediate requirement to spread awareness among the users of smart phones regarding the data leak that can occur due to improper handling of the apps. Users should realize that they are carrying Hacker in their pocket.

3. Notifications: Many apps do not give proper notifications regarding the resources they are going to access. It should be made mandatory that an app should provide complete list of permissions and resources it demands.

4. Universal Standards: All Mobile Operating Systems should provide a standard API interface for the app developers by considering all possible security attributes.

REFERENCES

[1] M. Hettig, E. Kiss, J.-F. Kassel, S. Weber, M. Harbach, Visualizing Risk by Example: Demonstrating Threats Arising From Android Apps, *M. Smith Symposium on Usable Privacy and Security (SOUPS), Newcastle, UK*, July 24–26, 2013,

[2] L. Barkhuus and A. Dey. Location-based services for mobile telephony: a study of users' privacy concerns, *Proceedings of the International Conference on Human-Computer Interaction*, 2003.

[3] A. P. Felt, M. Finifter, E. Chin, S. Hanna, and D. Wagner. A Survey of Mobile Malware in the Wild, *Proceedings of the ACM Workshop on Security and Privacy in Mobile Devices (SPSM)*, 2011.

[4] A. P. Felt, K. Greenwood, and D. Wagner. The Effectiveness of Application Permissions, *Proceedings of the USENIX Conference on Web Application Development (WebApps)*, 2011.

[5] Adrienne Porter Felt, Erika Chin, Steve Hanna, Dawn Song, David WagnerUniversity of California, Berkeley, Android Permissions Demystified, *CCS'11, Chicago, Illinois, USA. Copyright 2011 ACM 978-1-4503-0948-6/11/10 ...$10.00*, October 17–21, 2011

Gousiya Begum has received M.Tech Degree in Computer Science and Engineering from JNTU, Hyderabad. She is currently working as Assistant Professor in Computer Science and Engineering Department in Mahatma Gandhi Institute of Technology, Hyderabad. She is a Life Member of **ISTE**. She has published 6 papers in International Journals and presented 1 paper in International Conference. Her interested areas of research are Data Mining, Natural Language Processing, Network Security,

P Ram Mohan Rao has received M.Tech Degree in Computer Science and Engineering from JNTU, Hyderabad. He is a Life Member of **ISTE**. He is currently working as Assistant Professor in Department of Computer Science, ACE Engineering College, Ghatkesar, Hyderabad. He was a Resource Person in one of the workshops conducted by JNTU, Hyderabad.. on Intranet Applications using Java. He has published papers in International Journals. His areas of research are Web Security, Mobile Application Security, Application Layer Security Services, Cloud Security, and Web Mining.

Dr. K Venkateswara Reddy is principal of MLRITM, Hyderabad. He received his PhD from Osmania University, Hyderabad and M.Tech from JNTU, Hyderabad. He chequered a dynamic career in various reputed Engineering Colleges as a Professor, Head of the Department and Vice-Principal and is found to be disciplinary and dynamic personality in academic and administrative spheres. He bagged several national and international journals to his credit in 20 years length of his service. He is life member of **ISTE**. His areas of research are Cloud computing, Network security, MANET and other emerging fields of computer science.