IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

*International Journal of Advanced Research in Computer and Communication Engineering*
*Vol. 5, Issue 2, February 2016*

# Security Issues and Social Impacts of Mobile Applications

**Ms. Y Sowjanya[1], Ms. M Nishantha[2]**

Assistant Professor, IT Department, Guru Nanak Institutions Technical Campus, Hyderabad[1,2]

**Abstract:** Information and communication technologies made world easy. Mobile applications are one which rapidly growing the global mobile market. Security and social impacts on the society is an open issue. This paper gives security measures for information access by using a layered approach for applications which downloads data from the server, static and dynamic programs to automatically detect suspicious applications. This paper also presents some effect of mobile application on society from the ethical perspective with statistical data on different domains.

**Keywords:** Android, layered technology, inboxes, social impacts, mobile applications.

## 1. INTRODUCTION

Today's smartphones and tablets are more than communication devices. They are hip-mounted personal computers, with more memory and processing power than your laptop of just a few years ago. They are an integrated part of our lives… personal and professional. The information they provide is so vital that the Army is piloting their use as standard field issue to every soldier, complete with combat-focused applications [1].

However, smartphones and tablets raise new security issues. They are more likely to be lost or stolen, exposing sensitive data. Malware risks are increased because they connect to the Internet directly rather than from behind corporate firewalls and intrusion-protection systems. Security of mobile devices focuses on controlling access through the use of device locks and hardware data encryption. While this may be sufficient for individual users, it is insufficient for defense needs. Many documented examples exist of hacking of the device lock, as well as defeats of the hardware-level encryption. Once the device is unlocked, there is generally unfettered access to all apps and their associated data. Military applications require additional application-level access controls to provide data security.

The mobile enterprise has created vast opportunities— and serious new challenges. Mobile phones, mobile applications, and the network infrastructure are particularly vulnerable to attack and intrusion—and can all too often be the weak link in an otherwise secure enterprise infrastructure. Smartphones and mobile apps are being adopted at a phenomenal rate worldwide, with business users driving uptake in many markets. The burgeoning mobile Internet presents a tempting target for hackers and cybercriminals In this paper, we examine the current threats and realities affecting mobile enterprise security, and evaluate Best Practices in the areas of mobile testing and security. The authors recommend a comprehensive approach to enterprise security, one that addresses the device, network, servers, and the full secure development lifecycle (SDL) of mobile applications.

## 2. LITERATURE SURVEY

According to Nielsen, Google's Android is the most-used mobile OS, followed by Apple's iOS [6]. The threat level varies between the iOS and the Android environments, due to their app-distribution models. Because iOS apps are distributed only through the Apple App Store, the Apple review process substantially reduces the threat of downloading a malicious app. This protection, however, is lost if a user "jailbreaks" the device and installs apps from an alternative site or obtains illegal apps from elsewhere.

**Apple Ios:**Apple's "trust us" model controls security from malicious apps by providing only one outlet for app distribution and by tightly controlling the iOS Software Development Kit (SDK). Developers submitting apps for distribution must register with Apple to obtain certificates to build and deploy apps. All apps must be signed with the certificate assigned by Apple.

**Google Android:** Google took a different approach with the Android OS. Whereas Apple controls everything related to the app development and distribution process, Google developed Android as an open source model. Android developers are free to add to the API, use third-party APIs, and distribute apps through any means they see fit. While all Android apps must be signed with a certificate, developers can create their own certificates without using a certified certificate authority. Android provides the capability for greater application security than iOS, but the security model is definitely "trust them," as in, "do you trust the developer of the app is providing you a legitimate app that will provide its stated service in the manner described by the app developer and not try to steal information from you or try to damage your mobile device?" Still, Android is not without some basic security measures.

**Colonel Rajmohan, CISSP:** Colonel heads the Security CoE practice of TCS Niche Tech. Delivery Group (NTDG). He has led varied security initiatives in emerging areas and architecting end to end security solutions for strategic consulting engagements for many industry verticals.

DOI 10.17148/IJARCCE.2016.52128

**Ruchi Choudhary:** Ruchi leads the Mobile Security initiatives of TCS NTDG group. She is involved in creating awareness on secure application development guidelines on mobile platforms and actively working with customers on addressing their mobile security solutioning requirements.

**Somen Das:**Somen is an Application Security Analyst. Specialized in Static & Dynamic application vulnerability assessment techniques, he is actively involved in spreading awareness on secure application development and related guidelines across industry verticals. He has front ended many solutioning requirements from customers on creating application security frameworks for web and native applications. He is also Local Chapter Leader – OWASP Bhubaneswar.

## 3. SECURITY ISSUES

Massive growth in the mobile ecosystem has transformed operations in the enterprise world with respect to mobile devices. Increasing globalisation and on-the-spot information requirement is also catalyzing the mobile enablement of the global workforce. More and more employees are taking advantage of mobile devices to access emails, spreadsheets, databases, and ERP applications using either personal or company-owned devices. Due to inadequate access control policies and lack of information on securing mobile devices, IT departments had to completely ban such devices or risk insecure access inside the enterprise firewall. But as new mobile devices continue to appear on the enterprise network, a secure mobile enablement framework is a key IT programme requirement. This paper highlights various aspects of security that require extra focus when enabling mobile devices in an enterprise. Emerging trends in usage patterns and evolving models of managing mobile devices are also discussed here. Customised security processes, methodology and solutions are proposed to cover the entire spectrum of issues that need to be addressed.

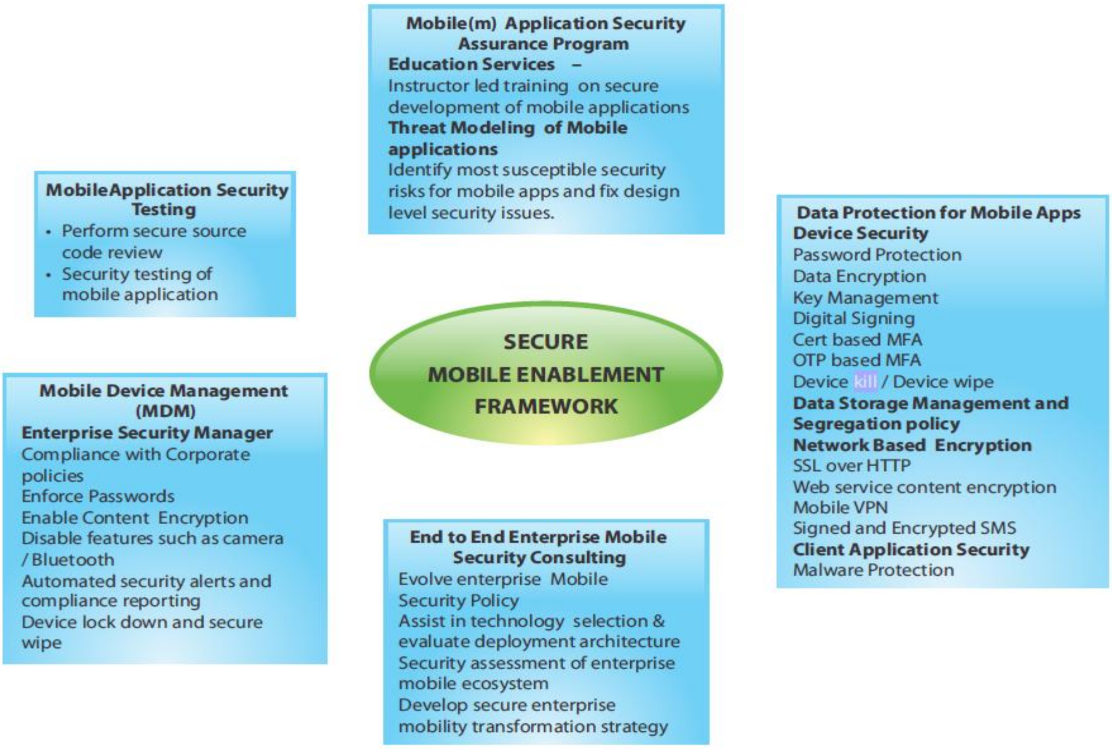

Mobile(m) Application Security Assurance Program
Education Services –
Instructor led training on secure development of mobile applications
Threat Modeling of Mobile applications
Identify most susceptible security risks for mobile apps and fix design level security issues.
MobileApplication Security Testing
• Perform secure source code review
• Security testing of mobile application
SECURE MOBILE ENABLEMENT FRAMEWORK
Data Protection for Mobile Apps
Device Security
Password Protection
Data Encryption
Key Management
Digital Signing
Cert based MFA
OTP based MFA
Device kill / Device wipe
Data Storage Management and Segregation policy
Network Based Encryption
SSL over HTTP
Web service content encryption
Mobile VPN
Signed and Encrypted SMS
Client Application Security
Malware Protection
Mobile Device Management (MDM)
Enterprise Security Manager
Compliance with Corporate policies
Enforce Passwords
Enable Content Encryption
Disable features such as camera / Bluetooth
Automated security alerts and compliance reporting
Device lock down and secure wipe
End to End Enterprise Mobile Security Consulting
Evolve enterprise Mobile Security Policy
Assist in technology selection & evaluate deployment architecture
Security assessment of enterprise mobile ecosystem
Develop secure enterprise mobility transformation strategy

Fig.1. Secure Mobile Framework[2]

Many threat vectors for infecting personal computers arise from social-engineering attacks that bypass anti-virus defenses. Similar techniques are used in the smartphone and tablet world by deceiving users into installing malicious apps. Examples include apps that gather personal information, track location, and charge accounts by sending text messages to premium-rate numbers. Using a mobile device to access corporate email or other resources extends the threat to the organization, including the theft of sensitive data [2]. With the acknowledged role of mobile devices and social networks in the revolutions in Egypt, Libya, and Syria, malware and viruses targeted at intelligence gathering and device-usage denial will increase significantly in the future [3].

While viruses and malware targeting mobile devices would share many of the same goals as on the PC, the enhanced capabilities of these devices present expanded attack surfaces through sensors such as GPS, accelerometer, camera, microphone, and gyroscope. Recently, Kaspersky Lab discovered a new threat involving the photo-scanning of Quick Response (QR) codes [4]. QR codes are 2-D matrix barcodes increasingly used in advertising and merchandising to direct mobile-phone users to a website for further information on the tagged item. In this case, users downloaded what they thought was a legitimate app, but instead was malware that sent Simple Message System (SMS) messages to a premium-rate number that charged for each message [5].

This app could have easily been reconfigured to send covert copies of emails and text messages to an intelligence gatherer instead.

### Application-level Data Protection

As organizations utilize mobile devices as enhancements or replacements for computers, many will soon work to develop custom applications designed for their own needs. These applications may contain confidential, proprietary information that will need additional protections than are offered at the device or hardware level.

The typical method to protect application data is to protect access via a login specifically for the application. We do this on our PCs with applications that need an additional level of protection over and above the OS-level screen lock; sometimes to protect specific information, sometimes to log who is currently using the application, many times for both. The scenarios required for application locking on PCs also exist on mobile devices.

### Data Security vs. User Experience

Computer security is a balance between usability and protection, or more specifically between usability and cryptographic strength. If security controls are too demanding, ample evidence suggests users will circumvent or disable the controls. For example, most users select insecure passwords easy to remember instead of strong passwords they are prone to forget. Smartphones have an added problem in small screens and keyboards that make typing passwords more difficult and add delay. Passwords for email and other accounts are therefore entered once in the device settings and stored, even when the device is powered off. This reduces security to device locking; after a device is unlocked, the user has immediate access to password-protected data and apps. With device locking, it is difficult to guarantee the locking implementation is secure. The Internet contains numerous methods to circumvent device locks.

Smartphones offer the potential for developing new methods of authentication using sensors such as the touch screen, GPS, camera, and accelerometers. Swipe patterns on smartphones are one example; others include picture passwords, tap patterns, and arm motions. Before adopting new authentication methods, there should be a formal analysis of the cryptographic strength to determine the number of pictures, taps, or motions required. The critical question is whether new methods can improve usability for the same level of protection as traditional methods.

Apple’s iOS model provides greater security out-of-the-box given Apple’s total control over the device, the app development environment, and the app-distribution model. Google’s Android provides greater potential for application-level security due to the extensive and open nature of the SDK. Neither OS model currently provides any significant focus for application-level security. To truly allow mobile devices to replace PCs and laptops, further research and development will be necessary to enable true application security within the mobile-device environment.

## 4. SOCIAL IMPACTS

This paper presents the uses and effect of mobile application in individuals, business and social area. In modern information and communication age mobile application is one of the most concerned and rapidly developing areas.

This paper demonstrates that how individual mobile user facilitate using mobile application and the popularity of the mobile application. Here we are presenting the consequence of mobile application in business sector. This paper also presents some effect of mobile application on society from the ethical perspective. The whole society can be facilitate using mobile application.

Some issues of social effect describe bellow.

### Quick communication:

Some mobile application like Facebook, Twitter, Messenger, Skype, Google Talk are helps the society people for communication to each other. They can stay in touch where the geographical distance is not a factor. So the social relation improves and make strong. And this is good for family, friend and society.

### Save time and increase productivity:

In society or in developed country people can do their daily work like check email, contact with business partner from any time in bus, train, car or walk. So, no need to wait in room or office. In this way save the time and people can get more time to work. The manpower’s productivity of society or country is increasing gradually.

### Improve IT infrastructure in developing country:

In developing country the uses of mobile application improve the knowledge of people. Because, they are accessing Internet from everywhere. As a result the IT infrastructure improves in any developing country.

### Increase Job vacancy:

The mobile application development and mobile application business make more job vacancy in society. So many people can get job in this field. This is also good for society/country.

### Less computer use less power consumption:

When most of the people will use mobile application for their daily simple work and getting facility from mobile application, the computer uses will be less as well as the power consumption will be less.

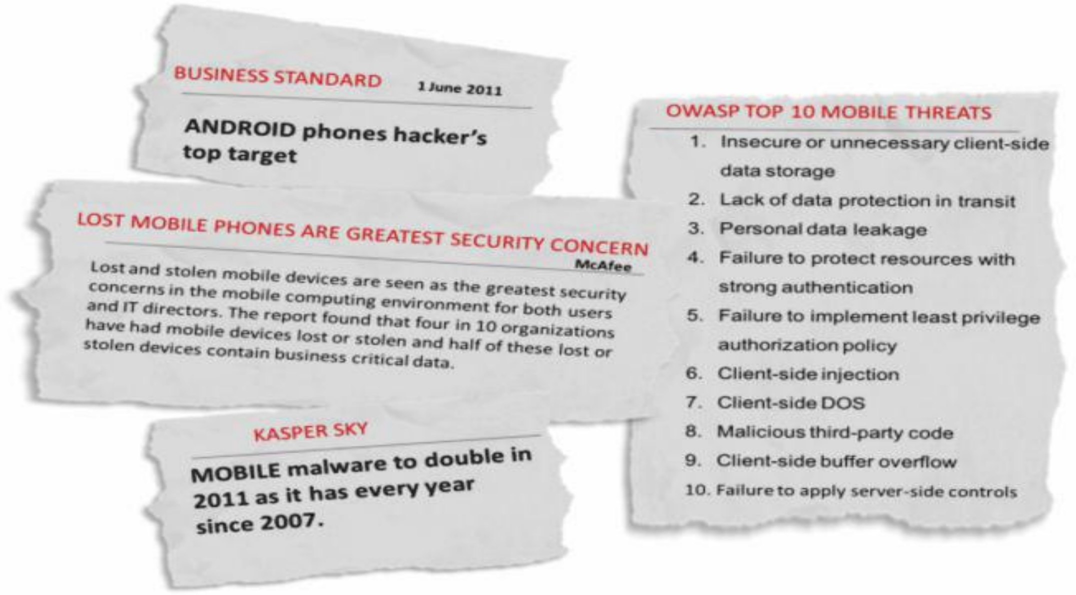
### Considerable Cost Saving:

Mobile VoIP application can help people to making international call from his mobile. As a result the monthly expenditure reduced.

### Entertainment:

Using mobile application people in society can entertained themselves. There are so many other social effect issues which all are ethically good for the society. On the other hand there are some bad effects of mobile application which are not ethically good for the society.

DOI 10.17148/IJARCCE.2016.52128



BUSINESS STANDARD 1 June 2011

ANDROID phones hacker's top target

LOST MOBILE PHONES ARE GREATEST SECURITY CONCERN
McAfee

Lost and stolen mobile devices are seen as the greatest security concerns in the mobile computing environment for both users and IT directors. The report found that four in 10 organizations have had mobile devices lost or stolen and half of these lost or stolen devices contain business critical data.

KASPER SKY

MOBILE malware to double in 2011 as it has every year since 2007.

OWASP TOP 10 MOBILE THREATS

1. Insecure or unnecessary client-side data storage
2. Lack of data protection in transit
3. Personal data leakage
4. Failure to protect resources with strong authentication
5. Failure to implement least privilege authorization policy
6. Client-side injection
7. Client-side DOS
8. Malicious third-party code
9. Client-side buffer overflow
10. Failure to apply server-side controls

Fig.2.Securiti Issues [2]

Those issues as follows:

1. When the so many Internet based mobile application is available to the teenager, they are wasting time by using Facebook, skype, YouTube etc. The young generations are in risk when they are using internet game or other bad application.
2. Beside the uses of mobile application most of the people use mobile in every place like bus, train, office, college, university. Some body feels disturb for them.
3. Frequently use of mobile is bad for health.

## 5. MOBILE APPLICATION USES LIMITATION

One of the big challenges of mobile application is its platform capability and limitation. Beside the interesting usability of mobile application they have some more interesting platform problems and limitation. We are trying to discuss the limitation in below.

1. **Small Screen Size:** In mobile platform it is difficult or impossible to view text and graphics like a desktop computer screen.
2. **Lack of windows:** In desktop we can see many windows at a time. But in mobile platform it is difficult.
3. **Navigation:** Most mobile devices do not have mouse like pointer, so it has limited flexibility in navigation.
4. **Types of pages accessible:** The mobile platform do not support all type of file format.
6. **Size of messages or email:** Many device support limited number of characters in message or email.

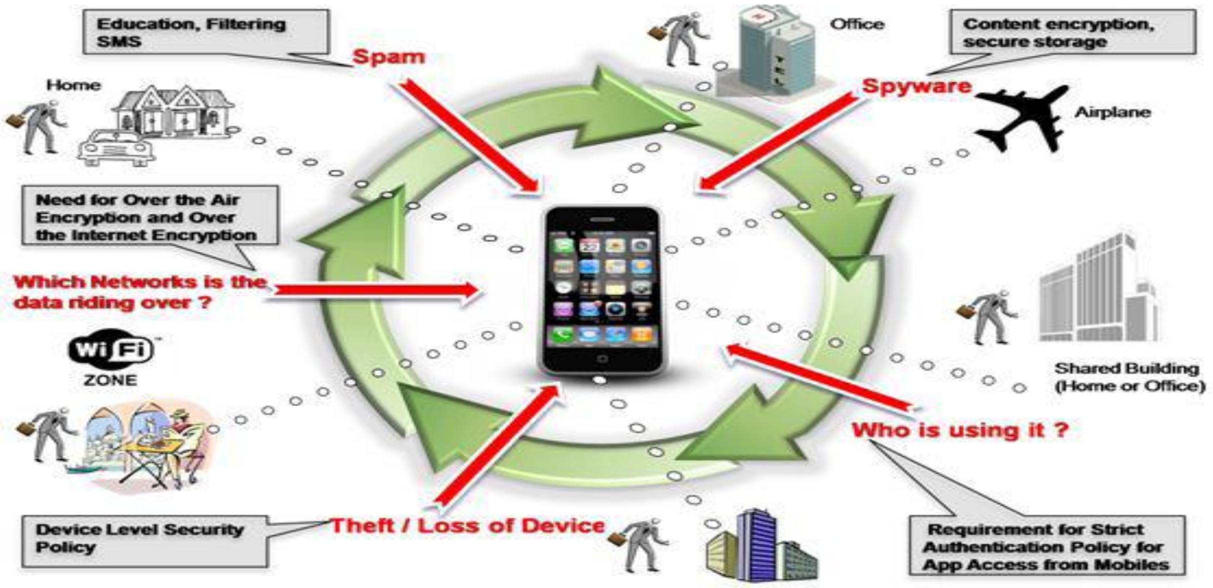

Education, Filtering SMS
Spam
Office
Content encryption, secure storage
Spyware
Home
Airplane
Need for Over the Air Encryption and Over the Internet Encryption
Which Networks is the data riding over ?
WiFi ZONE
Shared Building (Home or Office)
Who is using it ?
Device Level Security Policy
Theft / Loss of Device
Requirement for Strict Authentication Policy for App Access from Mobiles

Fig.3. Challenges[3]

## 6. CONCLUSION

Even though the solutions we got for the mobile applications still it is an open issue. While implementation of applications with integrity is working well. After all the limitation of mobile environment and mobile application, the uses and popularity of mobile application are increasing day by day. Most of the people are trying to use mobile device and mobile application instead of desktop for easy task. Gradually the uses of mobile applications are increasing corresponding to the use of desktop applications. All of the mobile manufactured companies and mobile application Developer companies are increasing the capacity, quality and functionality. So the modern mobile applications are more capable and more usable for the user. And the global impacts of mobile applications are going high.

## REFERENCES

[1]. Mobile Applications Security Safeguarding Data in a Mobile Device World, Sean C. Mitchem, Southwest Research Institute Sandra G. Dykes, Ph.D., Southwest Research Institute Stephen W. Cook, Southwest Research Institute John G. Whipple, Southwest Research Institute.

[2]. Security Challenges in Mobile Enabled Enterprises, Colonel Rajmohan, CISSP, Ruchi Choudhary, Somen Das

[3] Mobile Marketing Association, 2008, USA 1670 Broadway, Suite 850, Denver, CO 80202.

[4] Bin Yang, Yang-Yang Hao, Jie Wang, Zhi-Hua Hu "Flexible service architecture for maritime business promotion based on mobile technology " 978-0-7695-4011-5/10 $26.00 © 2010 IEEE DOI 10.1109/NSWCTC.2010.269.

[5] E.W.T. Ngai, A. Gunasekaran, A review for mobile commerce research and applications. Decision Support Systems, 2007. 43(1): 3-15.

[6] Mobile Applications – Past, Present and Future, Posted by Diogo Caldeira Pires, July 2, 2009, http://mobilemondayportugal.com/?p=180.

[7] International Telecommunications Union, "THE WORLD IN 2009: ICT FACTS AND FIGURES", Oct 2009.

[8] Mobile web, Wikipedia, URL: http://en.wikipedia.org/wiki/Mobile_Web.

[9] The Nielsen Company, "The State Of Mobile Apps", released in September 2010

[10] Adriana N., "Uses Of Mobile Applications For Smart Phones"http://ezinearticles.com/?Uses-Of-Mobile-Applications-For-Smart-Phones&id=5161301, Visited 24-10-10

[11] Eric Slivka, "Flurry: 22% of Recent Mobile Applications Starts Targeting iPad", Friday April-02, 2010 11:16 AM EST, http://www.macrumors.com/2010/04/02/flurry-22-of-recent-mobile-applications-starts-targeting-ipad/.

[12] IBM Survey: IT Professionals Predict Mobile and Cloud Technologies Will Dominate Enterprise Computing By 2015, Posted October 17, 2010, URL:http://www.fiercemobilecontent.com/press-releases/ibm-survey-it-professionals-predict-mobile-and-cloud-technologies-will-dominate-enter.

## BIOGRAPHIES

**Ms. Y Sowjanya** received Master Degree in Computer Science and Engineering form Jawaharlal Nehru Technological University, Hyderabad (JNTUH). Published 3 Paper in various International Journals on Data Mining & Network Security. Her research interest includes Information and Communication Technologies. Presently she is working as an Asst.Prof in IT Department, Guru Nanak Institutions Technical Campus. Hyderabad, India.

**Ms. M Nishantaha** received Master Degree in Information Technology form Jawaharlal Nehru Technological University, Hyderabad (JNTUH). Published 4 Paper in various International Journals.. Her research interest includes Networks and Software Technologies. Presently she is working as an Asst.Prof in IT Department, Guru Nanak Institutions Technical Campus. Hyderabad, India.

DOI 10.17148/IJARCCE.2016.52128