Security and Privacy of app Permissions on Mobile eServices

Francis Xavier LOWU[1]
[1]*Bugema University, P.O. Box 6529 Kampala, Uganda*
Tel: +256 0752818997, Email: hodct@bugemauniv.com, flowu.x@gmail.com

Abstract: Eservice providers depend much on mobile app user's data to market their services, to gauge their business growth and compare notes with competitors among many other factors. This paper uses analytical approach to discusses issues that come with the installation and usage of mobile eservice apps on Android devices and how app permissions threaten the security and privacy of users through collecting data and information from the mobile app users. This paper is based on the following objectives; to identify security and privacy lapses on mobile eservices, to propose a framework for eservices based on app developers, app users and eservice provider's functional requirements, and to discuss and analyze the security and privacy of each app permission group based on the usage of the eservices. To achieve the objectives, using Google play store, different eservice apps were identified, such as mobile banking apps, ehealth apps among others, that have impact on group or individual privacy. A framework was designed to show how app developers and eservice providers can involve users during app development and adoption. App permissions were grouped in sets and analysis was made on each app permission set based on popularity given on Google play store for android eservice apps. The analysis showed that eservice users do not understand the use of app permission and they fear for their security and privacy due to lack of technical ability to analyse them.

Keywords: Mobile, Apps, Eservice, Permissions, Android, Security, Privacy

1. Introduction

Mobile eservices use anytime, anywhere service model in both government and private sector. Businesses have become so competitive that they need to find the equally very busy customers without inconveniencing their day-to-day work. Mobile devices that use android apps are many and users prefer them, however other mobile apps running on different mobile based operating systems like iOS are also used. Users of the mobile app eservices give to much private data and information which is captured by these mobile apps. The mobile apps also capture or use some information and data on the mobile devices without the consent of device owners.

While mobile eservices have shown a tremendous growth in the urban regions, it is still a challenge to be implemented in the rural and semi-urban areas. This is due to lack of technical knowledge by the citizens and or users and guarantee from the government on issues of privacy and security. The security concerns such as attacks by hackers, theft of data and information from eservices portals, makes users hesitant. Governments also seem to be hesitant to implement and roll out eservices, through e-Government portals due to fear of cyber attacks. Data Mining remains threatened by the security and privacy gaps in eservices, since mobile eservices need presence of confidentiality, integrity and availability.

Mobile services apps that have similar functionalities are likely to have more attacks, for example banking eservice apps which are accessed by unsuspecting users on daily basis. Lack of technical knowledge and ability to analyse the app permission requirements has also played a big role in increasing vulnerability to mobile eservice subscribers and users. For example most of the eservices have an attachment to financial transactions. This is due to the increased pay- as-you-go and self-help services, with

majority having android mobile apps developed for them. app developer need to rethink of the involvement of users requirements through service providers.

Hezal Lopes et al (2013) assert that, the rate at which mobile malware is growing is alarming. It still remains the biggest threat in the mobile device industry today. The dominance of android mobile device has put it in the path of the hackers who use malware to attach mobile devices. The largest market of mobile device users today is in Africa, and this makes it an opportunity and return in investment for malware professional to attack. Training, sensitization by mobile telecommunication company and sell of devices with malware protection software can reduce the risks of being attached. Android mobile platform normally warm users before they install mobile apps. This is to help them make decisions on whether to continue installing the app or not. However most of the users either ignore or do not understand the implication of the app permissions.

1. The Problem

Private and public sector services today have adopted the use of mobile eservice model to provide self-help spot-on services. Such services require the use of mobile device such as, android mobile devices and installation of the mobile eservice app upon submission of relevant information and data about the user and device. Data and information submitted via app permissions policy infringes on the security and privacy of users of mobile eservices. With increasing use of data analytics due to availability of too much data and information of unsuspecting mobile android devices, mobile app eservices users doubt the intention of app permissions submitted during installation for usage of the eservice apps. Politics and businesses have continuously used the collected data without the knowledge of the users for campaigns, business analytics and further for competitive advantage between business competitors. This has put privacy and security of mobile app eservice users in open to vulnerabilities without their knowledge.

2. Objectives

The use of eservices today can not be avoided, as most Banks, higher institution of learning, health organization among others have developed android apps that can directly be downloaded from Google play store.

This paper presents concerns on the security and privacy of app permissions on mobile eservices with the following objectives.

1. To identify the security and privacy lapses on mobile eservices and how they relate to app permission policy of android mobile devices,
2. To propose a framework for eservices based on apps permission and user involvement in their development
3. To discuss and analyze the security and privacy of each app permissions based on the use of mobile eservices.

The objectives are guided by the research questions below:

- What are the security and privacy lapse that is encountered during the installation and usage of Mobile eservice app?
- What should be done to make the users involved in the processing of developing the mobile eservice app?
- How do the app permissions make security and privacy of users vulnerable?

3. Literature Review

Hezal et al (2013) studied four subjects of security, security of operating systems on mobile devices, security of mobile devices, mobile database security and security of mobile network. They acknowledge that smart phone and other mobile devices do not have pre-installed security software, which gives opportunity to cyber attackers to access the mobile devices. There is no installed security softwares such as firewalls, antivirus on the mobile devices. Further that the operating system security model of android supports the android based application distribution model, such as permissions which cannot be changed after installation of the application. However their work did not concentrate on the effect the permissions can incur on the unsuspecting users. Most of the users have no ability to evaluate permissions requested by the apps.

Jing et al (2015) identified personal information privacy, monetary risks and device stability and availability risks. "The convenience of smartphones is undeniable. But, along with that convenience comes new risks in terms of security and privacy. Smartphones contain an unprecedented amount of personal and often sensitive data including contacts, call logs, browsing history, personal photos, financial information, and personal messages. Moreover, with advanced sensors such as Global Positioning Systems (GPSs),cameras, and microphones, smartphones are capable of fine grained tracking and monitoring of a person's movements,communications, and surroundings. Thus, although smartphone apps can enable rich new functionality, they also pose risks to the personal privacy and security of smartphone users. Effective risk communication mechanisms are critical for helping users make safe and informed decisions regarding the apps that they install on their mobile devices." Jing et al(2015).

Milda et al (2017) as technology evolves, users now face different challenges, mobile devices have evolved to become a powerful tool that is connected to the internet and also cheap enough to be available to a large population of users that may be unable to afford a laptop and broadband service.

According to AVast Internet security report 2017, reveals that there is an increase in attacks that target Android smartphones and tablets. This raised to 40% in the second quarter of 2017. To address the threat, Avast upgraded its Avast mobile security and Antivirus and AVG Antivirus mobile apps to combat the threat. The top three major threats that were listed are:

- **Rooters:** These Rooters request the root access of a smartphone or sometimes use exploits and obtain the root access. When they gain control of the device, spying on the user starts and it may result in stealing information from the user.
- **Fake apps:** There are many which are illegitimate apps that pose as real ones in order to attract downloads and expose users to advertisements, hence attacking them.
- **Downloaders:** Most devices have Downloaders or droppers which use social engineering tactics to trick victims into installing more malicious apps. The Droppers also typically show full-screen ads, even outside of the app itself. These ads are not just annoying, but are often linked to suspicious sites which steal data.

However the AVast Internet security report 2017 says that users can control the app online, activate a siren if the phone has been stolen, remotely adjust settings and set custom screen messages, using;

- **App Permissions:** This help and allows the user to understand which apps installed on their phone have which permissions and what information they can access.

however most of the users do not bother so long as the app has installed. They just delete the app in case it's not liked.

- **Wifi Speed Test:** Checks the download and upload speed of the Wi-Fi network users are connected to. This helps the attachers how much time they will use to attack successfully. Slow internet access is not good for attackers.
- **Call Blocker:** this gives the users options to block unknown callers or send them directly to voicemail. This feature has been optimized for users to not only block numbers stored in the address book but also all unknown, and hidden numbers.
- **Safe Clean:** This cleans residual data and caches to improve smartphone speed and performance.

According to Esmeralda (2017) security concern is key to mobile device management strategy today, where what the users find as convenient also becomes convenient to the attackers. The study focused on human factor as the weakest point in the security of mobile devices. The contribution of users to smartphone threats and reducing the risks brought about by the smartphones was the basis of the research.

Based on work by Adrienne et al (2011), Smartphone and browser operating systems provide development platform that support different markets to thrive on third part applications. Users get security risks from the third party applications, implying that some of the third party authors are malicious, due to their expertise in security vulnerabilities. To protect users from attack and threats due to third party codes and applications, app permission controls are used by modern app platforms to control access to relevant parts of security and privacy of a user.

4. Methodology

To achieve the objectives of this study, Google play store was used to identify the different android based mobile eservice apps. The data collection goal was to identify as many mobile eservices app permissions as possible. Each mobile eservices app identified was matched with its permissions and put in a relational table set. Different types of permissions were identified and grouped. there are permissions that have risk privacy of mobile users and there those that risk the security of users more.

4.1 Identification of Security and Privacy Lapse

A group of three mobile eservices areas were identified and each group had different mobile eservice apps under it. These included Banking apps, eHealth & Life Insurance apps and Bill payment apps. The mobile apps that were identified under mobile banking group were; Eazzy Banking for Equity Bank, Standard/Stanbic Bank app, EcoBank Banking app, all of them had same requests such as contacts, location and others app permission. Almost all big Banks and telecom mobile network apps in the region have at least an app to be accessed by the users. This makes the users vulnerable in all directions.

As shown, in *Table 1*, each app was matched with the permissions.There are permissions that are mandatory to each app, more so for the apps that give the same services, for example Banking apps. Digits 1 and 0 were used in *Table 1* to show that which permissions hold for a respective app or does not hold respectively.

MOBILE ESERVICES	MANDATORY APP PERMISSIONS										
	Contacts	Locations	Photo/Media/Files	Identity	Storage	Phone Calls	Device ID & Call Info	SMS	WiFi	Microphone	Camera

Banking Apps											
• Stanbic	1	1	1	0	1	0	1	0	0	0	1
• Eassy Pay	1	1	1	0	1	0	1	0	0	0	1
• Airtel M'ney	1	1	1	1	1	1	1	1	1	1	1
• MyMTN	1	1	1	1	1	1	1	1	1	1	1
• EcoBank	1	1	1	1	1	1	1	1	1	1	1
• KCB	1	1	1	1	1	1	1	1	1	1	1
• CenteMobile	1	1	1	1	1	1	1	1	1	1	1
• MPesa	1	1	1	1	1	1	1	1	1	1	1
• Bankclays	1	1	1	1	1	0	1	0	0	0	1
• Eazzy Equi	1	1	1	0	1	1	1	1	1	0	1
eHealth & Life Ins											
• Weight	1	1	1	1	1	1	1	1	1	1	1
• Nutrition	1	1	1	1	1	1	1	1	1	1	1
• FWD Insura	1	1	1	1	1	1	1	1	1	1	1
• NSSF GO	1	1	1	1	1	0	1	1	0	1	1
Bill Payments											
• Water	0	0	1	0	1	0	0	0	1	1	1
• TV	1	1	1	1	1	1	1	1	1	1	1
• Electricity/U meme	1	1	1	1	1	1	1	1	1	1	1
	1	1	1	1	1	1	1	1	1	1	1

Table 1: Mobile Eservices and Permission that infringe on Privacy and Security

Each group was put in a dataset to find out which mobile app permission was mostly valued by the app developers and service providers. Mobile eservice app users have less permissions and this makes them be used without objection.

Table 2: shows that most eservice providers require contacts, locations, access to photos, storage, device ID and Cameras, yet these are key to the privacy of individual users.

MOBILE ESERVICES GROUPS	**FREQUENCY PER APP PERMISSION**										
	Contacts	Locations	Photo/Media/Files	Identity	Storage	Phone Calls	Device ID & Call Info	SMS	WiFi	Microphone	Camera
Banking Apps	10	10	10	7	10	7	10	7	7	6	10
eHealth & Life Ins	4	4	4	4	4	3	4	4	3	4	4
Bill Payments	3	3	4	3	4	3	3	3	4	4	4

Table 2: Mobile Eservice Groups and Frequency

4.1.1 Cyber Attack Prune app Permissions

To identify cyber attack prune permissions, the researcher looked at permissions that are linked directly to Internet service providers to contact or access the user through phones calls. These and others expose the mobile service users greatly. The majors ones that had similarity in all apps included;

Permission Type	**Security Lapse due to Permission**
Receive data from Internet	This may involve malware and viruses
View network connections	Knowing the network connection of the user

	may also compromise information and connectivity to sensitive NODES
Disable your screen lock	this may come with Denial of services attacks were the owner of the mobile device may not access his/her information/contacts
Run at startup	It's always very difficult to detect malware that run at startup. They seem like app programmes
Prevent device from sleeping	This may let you starting clicking on everything that pops up. Which may be installed on your device.
Modify system settings	Most of the time users take long to modify settings from the default setting when a new device is acquired. Accepting modification by apps may be dangerous. They can restore to the known defaults once you had changed
View network connections	This will expose the use to know which network you are using. While some may be for data loading purposes, it may still be compromised.
Full network access	Okay,, but with high speed connectivity attack can occur very fast.Usually if the
Read Google service configuration	This will always target Google email contacts and Google drive content.
Access downloads manager	makes downloads faster to minimize detection. Which may be dangerous for users.
Download files without notification	Files downloaded without notification can be very dangerous. Apps are supposed to be installed for eservices. So any installation needs the knowledge of the user,.

Table 3: App Permission Security Lapses

All these permissions are dangerous as far as security of mobile e service users is concerned. The app developers and mobile service providers need to get a common understanding on how to develop the apps. Requirements of App developers was identified along side the user mobile eservice app security expectations. Six categories of functional and security requirements were identified to help in the design of the framework to meet objective two of the study. These included: *App Functional Requirements, User Functional Requirements, Service Provider Functional Requirements, App Security requirements, User Security Requirements and Service Provider Security requirements.*

4.2 Proposed Framework

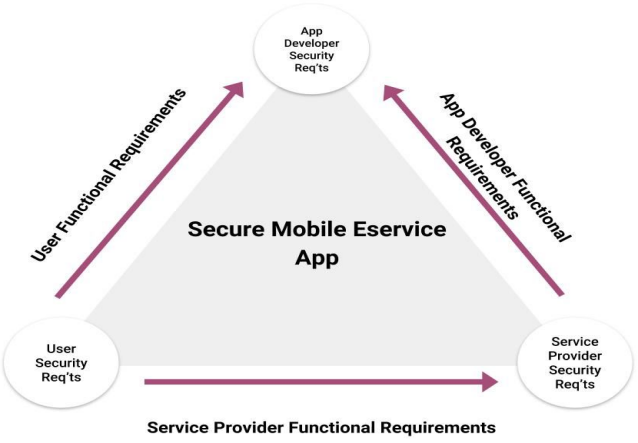

Figure 1: Secure Mobile Eservice App Development Framework

Figure 1 shows the proposed framework that involves all stakeholders, mobile users, eservice providers and the app developers in the process of developing eservice mobile apps. User consultation is required from service providers. This makes it easy to adopt the user functional requirements in the design processes. Service provider functional requirements are normally business oriented and they tend to have coincidence with the user security requirements. Since each entity understands their security requirements better

5. Results

The chart below show that mobile eservice app permissions by frequency. The three

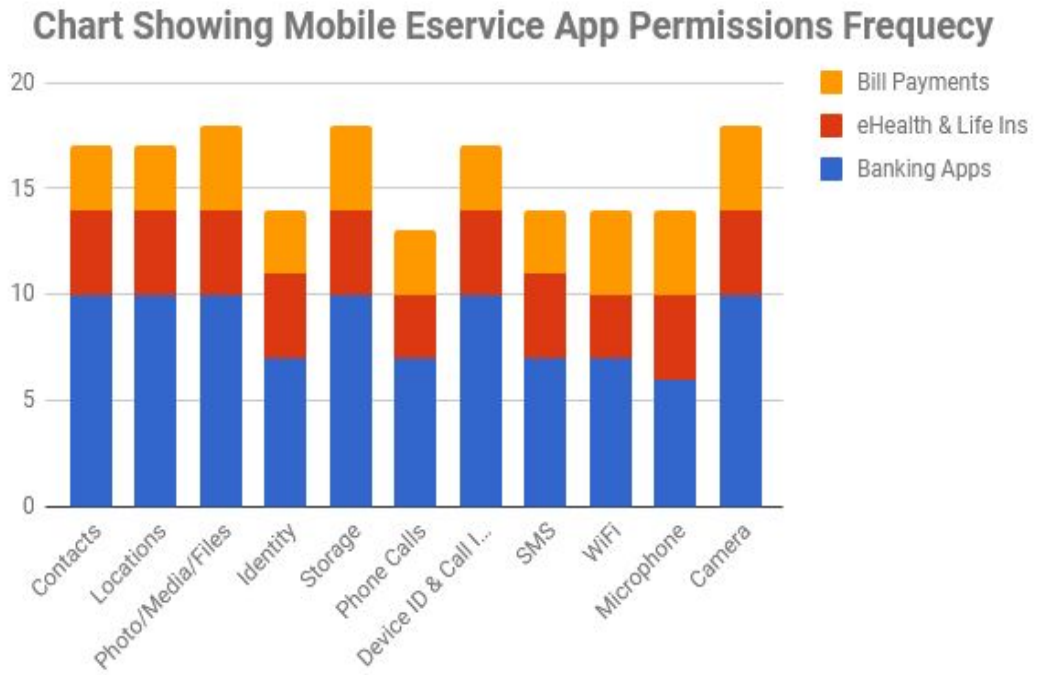

Chart 1: Frequency of Mobile Eservice Permissions

According to the graph here most of the apps require contacts from the user. This helps them to easily contact them in marketing. By using the contacts of the person without his/her concert is depriving them of the privacy. More messages will be sent frequently to the users.

Location also is required by most of the eservice apps. While this may be okay to some extent, by knowing the location of the target it becomes easy to attack the person. SO location is a security threat.

Photo and files of users contact information such as profiles of the person. This is both insecure and for privacy it becomes tricky for the person whose photo is taken by each app installed.

Storage space is normally got to scan through your device to find out if more apps can be installed. Mobile devices have limited space and therefore over usage of the space may make the device slow and this becomes problem to fast access or stop it in case of detection of malware tendencies.

Another permission that is liked by most eservice apps is the camera.However they are less security threat associated by it on a personal usage. However when someone takes your picture and puts it on a profile somewhere without your knowledge it becomes a privacy issue. The study as shown in the Chart above shows that most apps also identity, phone calls, SMS send and microphone which may equally be security and privacy breach for the service users.

6. Recommendations and Area for Further Study

In this study recommendation is such that; most of the users of mobile eservices show be able to take their time and read the permissions before installation of the app. Also the eservice app developers should involve the users to find out their function requirements alongside those of the eservice providers. By understanding the functional requirements of the users through the service providers makes it easy to develop an app that will be having security requirements of users and service providers.

6.1 Area for Future Study

In future the researcher will examine how cloud app permissions relate to mobile based app permissions. With interest on the security of Infrastructure as a service (IaaS), Software as a Service (SaaS) and platform as a service (PaaS).

7. Conclusion

This paper has evaluated the privacy and security of app permission on mobile eservice users. This study also analysed that the apps installed by the mobile eservices users requires installed based on similar permissions. The Researcher also found out that the permission that are required are those which infringe on the privacy of the users. In the study the eservices where grouped based on the service that are used most by the mobile eservice. Three groups were created, Banking apps, ehealth and life insurance apps, ebilling apps group. Most of these app groups had similarity in the app permissions requested.

A framework was developed to propose how users functional requirements can be included during development. In the frame developed its proposed that if all users have their functional requirements through the eservice provide and they also submit their functional requirements it becomes easy for the app developers to cater for the security requirements of the users.

References

Esmeralda, K. (2017). SMARTPHONE SECURITY THREATS. ÓBUDA UNIVERSITY, DONÁT BÁNKI FACULTY OF MECHANICAL AND SAFETY ENGINEERING, HUNGARY. *Management, Enterprise and Benchmarking in the 21st Century Budapest.*

Milda, P., Ali, D., Gregory, E. (2017). MOBILE PHONE FORENSICS: AN INVESTIGATIVE FRAMEWORK BASED ON USER IMPULSIVITY AND SECURE COLLABORATION ERRORS. Pg. 79-89, *Contemporary Digital Forensic Investigations Of Cloud And Mobile Applications. School of Computing, Science and Engineering, University of Salford-United Kingdom*

Jing, C., Christopher, S., Gates, Z. J., Ninghui, L., Proctor, Ting. (2015). DIMENSIONS OF RISK IN MOBILE APPLICATIONS: A USER STUDY.

Hezal, L., Rahul, L.(2013). COMPARATIVE ANALYSIS OF MOBILE SECURITY THREATS AND SOLUTION. *Department of Computer Engineering, Mumbai University, Universal College of Engineering. Int. Journal of Engineering Research and Application* 3(5) 499-502.

Adrienne, P., Felt, K, G., David, W. (2011). THE EFFECTIVENESS OF APPLICATION PERMISSIONS. *University of California, Berkeley. Proc. of the USENIX Conference on Web Application Development*.

Ondrej, V. (2017). Avast cyber security predictions for 2017.Redwood City, California, September 11, 2017 https://press.avast.com/avast-reports-40-increase-in-mobile-cyberattacks.

Muhammad, I., Narseo, V., Suranga, S., Mohamed, K., Vern, P.(2016). AN ANALYSIS OF THE PRIVACY AND SECURITY RISKS OF ANDROID VPN PERMISSION-ENABLED APPS. *IMC 2016, November 14-16, 2016, Santa Monica, CA, USA, ACM. ISBN 978-1-4503-4526-*

Primal, W., Arjun, B., Ashkan, H., Serge, E., David, W., and Konstantin, B. *(2013).* ANDROID PERMISSIONS REMYSTIFIED: A FIELD STUDY ON CONTEXTUAL INTEGRITY. *University Of British Columbia,Vancouver, Canada*