**Australian Journal of Basic and Applied Sciences,** 10(12) July 2016, Pages: 205-212

AUSTRALIAN JOURNAL OF BASIC AND APPLIED SCIENCES

ISSN:1991-8178 EISSN: 2309-8414
Journal home page: www.ajbasweb.com

# A Study on the Existing Banking Trojan to Mobile Applications

[1]S. Geetha, [2]Indumathi. R, [3]Mary Sheeba Theodore. R, [4]Agalya. S, [5]J. Madhusudanan, [6]V. PrasannaVenkatesan

*[1]Research Scholar, Department of BT, Pondicherry University. Puducherry*
*[2]UG Student, SMVEC, SMVEC, Madgadipet, Puducherry*
*[3]UG Student, SMVEC, Madgadipet, Puducherry*
*[4]UG Student, SMVEC, Madagadipet, Puducherry.*
*[5]Associate Professor SMVEC, Madagadipet, Puducherry.*
*[6]Associate Professor Department of Banking Technology, Pondicherry University, Puducherry.*

**Address For Correspondence:**
S.Geetha, Research Scholar, Department of BT, Pondicherry University. Puducherry
E-mail: Geethaa_ss@yahoo.co.in

**ARTICLE INFO**

***Article history:***
*Received 26 April 2016*
*Accepted 21 July 2016*
*Published 30 July 2016*

***Keywords:***
*Mobile Banking, Security, Threats to Mobile Banking, Trojans in Banking services, Banking Applications, Keyloggers.*

**ABSTRACT**

Today people can do anything and everything that they want at any time through their Smart phone. This technology development has also taken us into the world of Smart applications. These applications play a key role in the day-to-day activities of the people. Every activity that the user performs is driven by the apps available in the Smart phone. These apps have made the world in such a way that without their presence nothing can be done in the current world. This technology development has also been brought more changes into the banking sectors. Thus banks have introduced the banking services through their mobile banking applications. The use of mobile banking have increased more due to their faster and easier use in doing the transactions from where ever the customers wants to do it. But more customers don't use the mobile banking application due their lack of confidence in the security of the application. Security is one of the major challenges for banks to make their customers to adopt them for mobile banking services. More and more threats are been introduced into the mobile banking applications. This paper describes a brief study about the various types of threats that are available in the mobile banking services.

## INTRODUCTION

The recent developments in the technology have brought more changes in the banking industry also. The banking sectors have introduced smart features into their banking applications that are done through internet and mobile devices. These technology developments in banks have increased their customers because of its faster transactions carried out from a remote location and whenever they are in need to do it. The convenience that is been achieved by the mobile banking applications has grabbed more users attention to use these services through their Smart phone. The recent surveys on mobile banking says that the number of customers using mobile banking applications is been increased. But most of the users are not using this service due to their lack of confidence in the security of the mobile banking applications. The emergence of more threats into the banking applications has created a large number of challenges in this area. Though researches are carried out in the security of the mobile banking applications still the proof for its security level proved is not provided to the customers. If this customer awareness about the security provided is achieved the mobile banking applications success will be at its top.

This paper gives a study on the various threats that is existing for mobile banking applications and the discussion on the prevention measures that can be used to increase the confidence level of the customers in mobile banking usage is been carried out. The section 2 of the paper is the literature review about mobile

**To Cite This Article:** S. Geetha, Indumathi. R, Mary Sheeba Theodore. R, Agalya. S, J. Madhusudanan, V. PrasannaVenkatesan., A Study on the Existing Banking Trojan to Mobile Applications. ***Aust. J. Basic & Appl. Sci.,*** *10(12): 205-212, 2016*

banking threats. Section 3 describes briefly about the threats to Mobile banking. Section 4 shows a proposed method for Keyloggers implementation for mobile applications. The section 5 is the discussion about the prevention measures to overcome the attacks in mobile banking applications. Section 6 is the Conclusion.

***Literature Review:***

Md. Shoriful Islam (2014) has done a literature review on the various challenges to Banking Systems. He has given a clear description about the various threats and the challenges that the mobile banking systems are facing. The paper shows the various levels by which threats enter into the mobile devices and how it affects the user's confidence in using the mobile banking applications. They have suggested improving the user's knowledge level about the threats and their smartness needed to overcome these issues. Panida Subsorn *et al* have done an analysis about the security of the mobile and internet banking. They have given a conclusion that the banks should upgrade their security encryption technique from 128-bit to 256-bit encryption with extended validation. Mr. Shakir Shaik *et al*, (2014) have stated that "Availability of confidential information which is secured by user name and password is vulnerable to attacks". The paper concludes that the success of the mobile and internet banking can be achieved if the customer satisfaction is more. To achieve more customer satisfaction the banks should provide a better security in their banking applications.

According to the January 2016 report of Bank info Security (Working of Keyloggers available at http) most of the Android phone malwares is been developed to get the OTP sent to the customers to complete the transaction process. They are also designed to trick the users to get diverted into their websites by the links and pop-ups that is been displayed on the screen to make all kind of phishing attacks in the device.

***Threats to Mobile Banking Applications:***

The attackers have introduced various means to enter their threats into the mobile banking applications. The threats are attached to the victim's smart phone through different means, they are done by

- Unauthorized access to the smart phone
- Malicious hacking of the data
- Malware and Mobile Viruses
- Downloads from play store
- E-mail links or SMS

There are trojans whose main objective is to attack the mobile devices. In the recent days number of trojans has been introduced in the smart phone to get the valuable information of the users. The below table shows the various trojans that are existing in the smart phone and their actions in the device once it is installed.

**Table 1:** Threats to Mobile Banking

| S. No | THREAT | METHOD OF INJECTION | ACTIONS PERFORMED |
|---|---|---|---|
| 1. | Carberp | Through SQL Injection in the Web Browser | Intercepts all the Communication done through the mobile. |
| 2. | Freak | While Opening an infected website. | Steals the passwords and transaction information sent or received from the device. |
| 3. | Keyloggers | Through various means either as a attachment or through links from emails. | Places a third party keyboards into the smart phone and records all the keystrokes in a log file and sends it to an attacker. |
| 4. | Zeus | Through links from social networks. | Saves the user input data in the mobile interface and then later transfers it to the attackers system. Also capable of by-passing two-factor authentication. |
| 5. | Bankum | Through web browser injection. | Acts as a legitimate banking app and replaces the original version with the fake app. |
| 6. | Hesperbot | Injected through SMS sent to the Smart phone. | It takes the full control of the device and hijacks all the information stored and shared through the device. |
| 7. | SpyEye | Through Social networks as link to install an app or website. | One of the successful banking trojan. Performs the spying action through a webcam installed into the device. It is capable of even altering the account balances in the users screen. |
| 8. | Lurk | Through web browser downloads. | This is a Token Bypass of the local transaction process. Create a remote access to the process and allow the malicious system to hack the details. |

These are the various threats that is been inserted into the smart phones to hack the information about the mobile banking transaction information to perform malicious activities using the details gathered.

***Keyloggers:***

The existing threats/trojans to mobile banking applications have created more number of security risks in the banking industry. To know about their working and effects one of the trojans Keyloggers is studied and it is been implemented to find out how it is been attached to the smart phone.

Keyloggers are used for both good and bad activities. Keyloggers are also used to monitor the activities of the employees of the organization. It is utilized in the home to monitor the activities of the children.

The main aim behind Keyloggers is to take the information between any of the two links i.e., when a key is pressed and when information about that keystroke is shown on the screen. This is achieved by using spyware in the mobile or introducing an application which logs the activities of the user without the knowledge of the user.

These applications are downloaded and installed in the user's mobile. It enables automatically and transfers the information when the mobile is been connected to an internet. These apps are also downloaded when they visit a website that is not an authenticated one or through a fake link which downloads these apps and runs in the background.

Keyloggers are inserted into the device through various means, they are

a) As a file attached within an email or as messages in the Smartphone
b) Files accessed from an open-access directory on a P2P network
c) When a user visits an infected site in the internet
d) Through a malicious program which is been installed in the device
e) When downloading an app from the play store of the mobile they get attached

***Implementation:***

A Keyloggers application is been developed to check how it works and how does it gathers information from the user. A soft keyboard is been developed as an apk file. Whatever the user types using this specific keyboard, the keystrokes will be stored in the file known as keylogger.txt.

The apk file is sent to other devices through Cloud Send. The file is uploaded to the Cloud Send and a request to open the link in the victim's mobile is sent through the social networking sites lie face book, twitter, whatsapp, etc., The file is stored into the Drop box and if the victim opens the link the apk file will be downloaded into its device.

***Sample Code:***

***Displays the IME preferences inside the input method setting:***

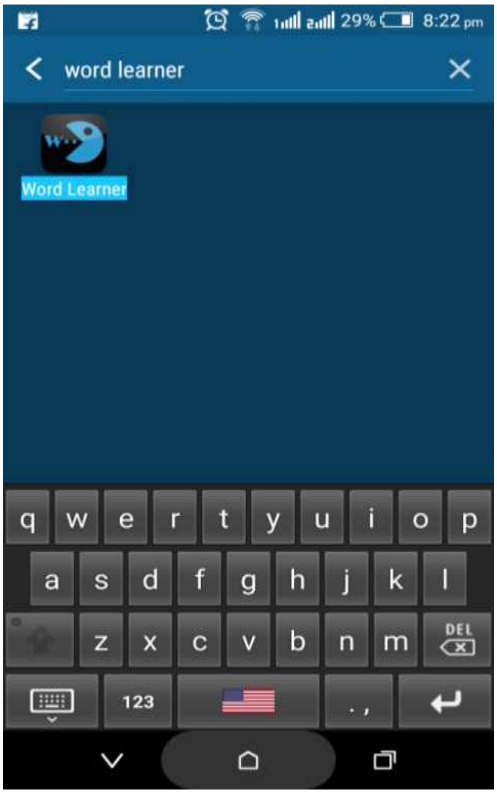
```
public class ImePreferences extends PreferenceActivity {
@Override
public Intent getIntent()
{
final Intent modIntent = new Intent(super.getIntent());
modIntent.putExtra(EXTRA_SHOW_FRAGMENT, Settings.class.getName());
modIntent.putExtra(EXTRA_NO_HEADERS, true);
return modIntent;
}
@Override
protected void onCreate(Bundle savedInstanceState)
{
super.onCreate(savedInstanceState);
// We overwrite the title of the activity, as the default one is "Voice Search".
setTitle(R.string.settings_name);
}
public static class Settings extends InputMethodSettingsFragment
{
@Override
public void onCreate(Bundle savedInstanceState) {
super.onCreate(savedInstanceState);
setInputMethodSettingsCategoryTitle(R.string.language_selection_title);
setSubtypeEnablerTitle(R.string.select_language);
// Load the preferences from an XML resource        addPreferencesFromResource(R.xml.ime_preferences);
}
}
}
```

***Code for latinkeyboardview:***

```
public class LatinKeyboardView extends KeyboardView
{
static final int KEYCODE_OPTIONS = -100;
public LatinKeyboardView(Context context, AttributeSet attrs)
```

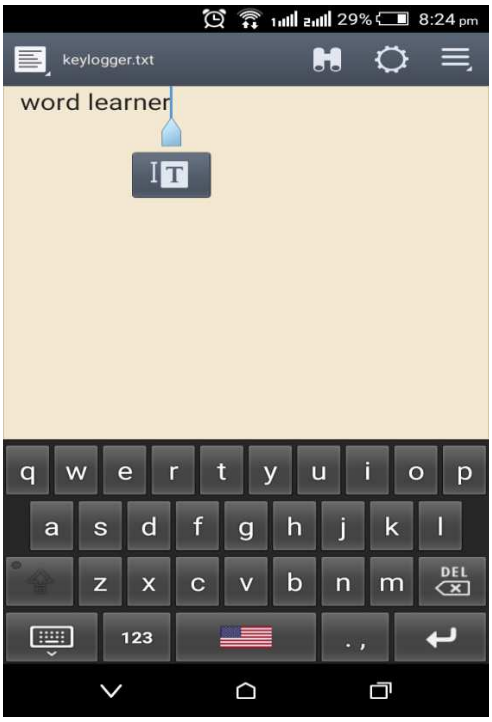
```
    {
    super(context, attrs);
    }
    public LatinKeyboardView(Context context, AttributeSet attrs, int defStyle)
    {
    super(context, attrs, defStyle);
    }
    @Override
    protected boolean onLongPress(Key key)
    {
    if(key.codes[0]==Keyboard.KEYCODE_CANCEL){
getOnKeyboardActionListener().onKey(KEYCODE_OPTIONS, null);
    return true;
    } else {
    return super.onLongPress(key);
    }
    }
    Void setSubtypeOnSpaceKey(final InputMethodSubtype subtype)
    {
    FinalLatinKeyboardkeyboard=(LatinKeyboard)getKeyboard();
keyboard.setSpaceIcon(getResources().getDrawable(subtype.getIconResId()));
    invalidateAllKeys();
    }
    }
```

***Screen Shots:***



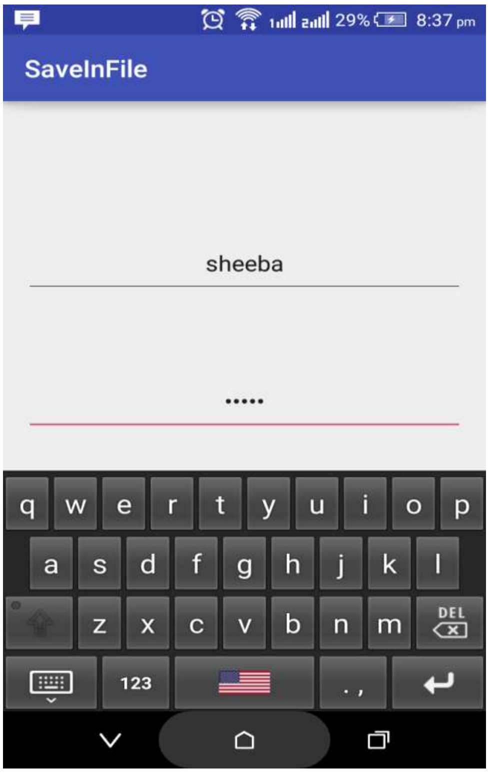
word learner

**Fig. 1:** Typical Keyboard



word learner

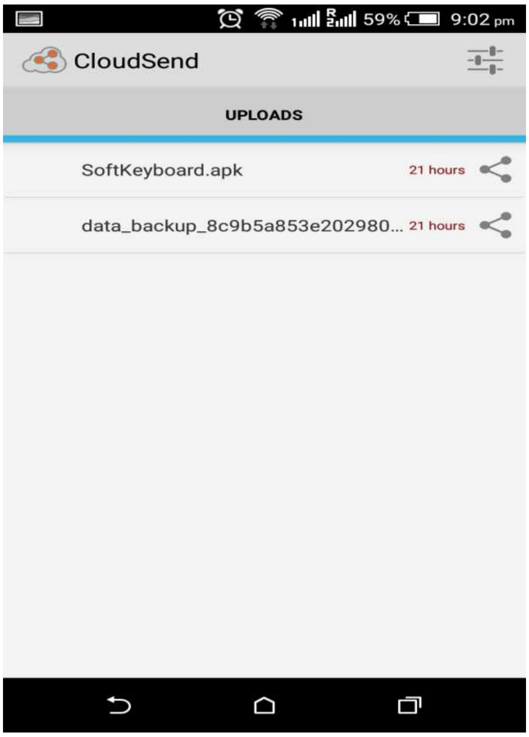
**Fig. 2:** Keyloggers Keyboard



sheeba

•••••

**Fig. 3:** File to Store The Keystrokes



SoftKeyboard.apk 21 hours

data_backup_8c9b5a853e202980... 21 hours

**Fig. 4:** Sending the Keyboard through Cloud Send

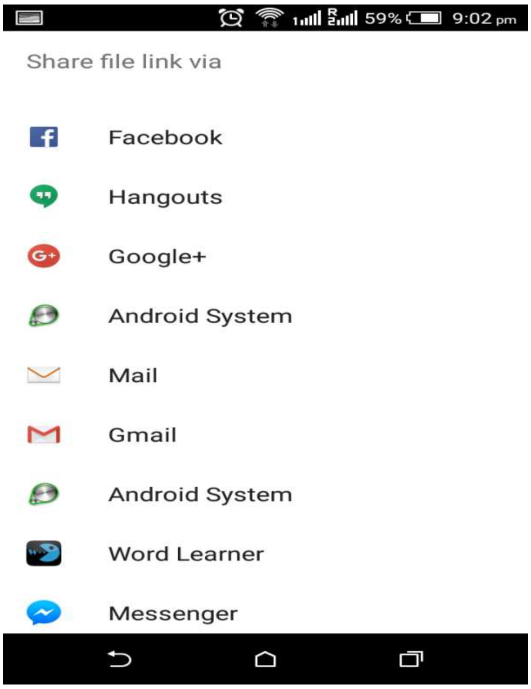


**Fig. 5:** Sharing the link of Keyboard

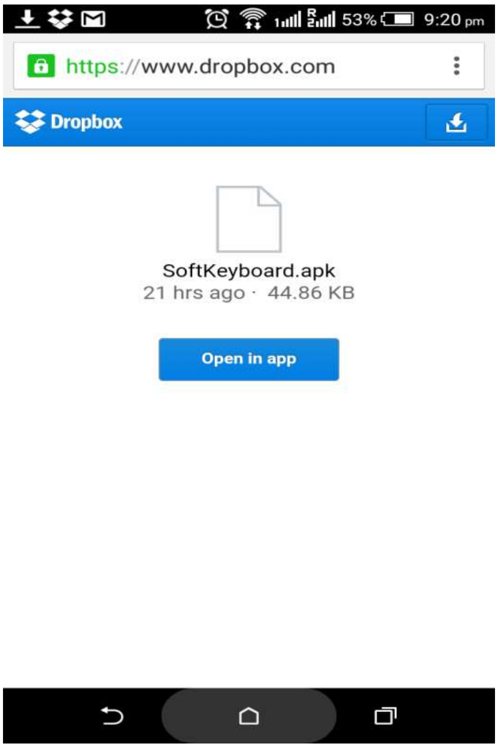


**Fig. 7:** Saving it in the Drop box

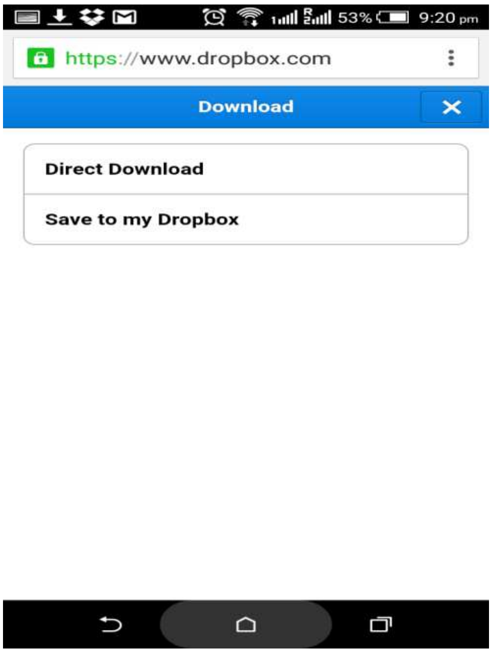


**Fig. 8:** Downloading it to the Device

***Discussion:***

The emergence of more and more threats into the Android application has become a great challenge for the Mobile Banking Applications. Banking Industry is taking various measures to overcome these issues for increasing their customer's confidence in the security provided to them. But on the other end, attackers are very smart and they are introducing new and newer trojans into the field to get the confidential details of the users. To find a better solution to this the developers also should think smartly to tackle the attackers. The users should be given awareness about the threats that is been attached to their devices. They should be trained to identify the misbehaviour or changes that are happening in their screens while doing a transaction. A watchdog type of mechanism can be introduced into the android or smart phone by which a monitoring of the activities can be done. But still monitoring is not enough for the existing threats in smart phone. The vulnerabilities or a Trojan that is entering the smart phone has to be sensed before they are been inserted into the device. Thus a better sensing technique like bio-inspired techniques can be applied to get a better solution from the various threats of the mobile applications.

### *Conclusion:*

This paper shows a detail study about the various threats that is employed in the Mobile banking applications. An implementation on Keyloggers is done to show how it is been installed in to the devices and how it saves the keystrokes in the log file. The methods of sending the infected file to other devices is also been shown. This clearly describes about the effects of the trojan inside our device and what activities it is performing in the smart phone. A discussion on the solutions that can be provided for the mobile threats is done. Thus a better understanding about the existing mobile banking trojans and their working can be achieved through the study carried out.

## REFERENCES

Bank Info Security Report, 2016. http://www.Bankinfosecurity.com/

Jesudoss. A. *et al*, “A survey on authentication attacks and countermeasures in a distributed environment”, Indian Journal of Computer Science and Engineering (IJCSE).

Malware Definition Available at <http://www.wisegeek.com/what-is-malwa re.htm>.

Malware Definition Available at http://en.wikipedia.org/wiki/Malware.

Md. Shoriful Islam, 2014. “Systematic Literature Review: Security Challenges of Mobile Banking and Payments System”, International Journal of u- and e- Service, Science and Technology, 7(6): 107-116. http://dx.doi.org/10.14257/ijunesst.2014.7.6.10

Mr. Shakir Shaik *et al*, 2014. “ Security Issues in E-Banking Services in Indian Scenario”, Asian Journal of Management Sciences 02 (03 (Special Issue)); pp: 28-30.

Panida Subsorn *et al*, “A comparative analysis of the security of Internet banking in Australia: a customer perspective”, Proceedings of the 2nd International Cyber Resilience Conference.

Sebastián Sznur *et al*, 2013. “ Advances in Keystroke Dynamics Techniques to Group User Sessions” , International journal of Information Security Science, 4: 2.

Thefts in Remote Banking Systems: Incident Investigations Secure list, by Mikhail Prokhorenko on September 11, 2014.

Types of Malwares Available at http://arstechnica.com/security/2004/111rnalware/.

Working of Keyloggers available at http://securelist.com/analysis/publications/36138/keyloggers-how-theywork-and-how-to-detect-them-part-1/.