

**GEK 1531 Introduction to Cybercrime**

**Project Report**

**Semester II AY10/11**

**Issues Related to Mobile Phone Security**

**Done By:**

**Chen Zhenjin Mark U087067B**

**Neo Qi Yang U080305L**

Table of Contents

[Introduction 3](#_Toc290316535)

[1. The Growing Smartphone Market and its Implications 4](#_Toc290316536)

[Expanding Smartphone Market 4](#_Toc290316537)

[Malicious Mobile Applications 4](#_Toc290316538)

[2. What are mobile malware and why mobile malware 5](#_Toc290316539)

[3. Risks and effects of mobile malware 6](#_Toc290316540)

[Personal Risks 6](#_Toc290316541)

[Trouble for others 6](#_Toc290316542)

[4. Actions Taken by Software Developers 7](#_Toc290316543)

[Software Security Companies 7](#_Toc290316544)

[Operating System Developers 8](#_Toc290316545)

[5. Preventive Measures 8](#_Toc290316546)

[Update Firmware Regularly 8](#_Toc290316547)

[Anti-virus Software 8](#_Toc290316548)

[Use Only Trusted Applications 9](#_Toc290316549)

[Conclusion 10](#_Toc290316550)

[Bibliography 11](#_Toc290316551)

# Introduction

Awareness of risks that smartphones possess has been low and the general public is still unaware of the dangers of smartphones. In this report, we are analyzing the risks encountered when using smartphones as well as how individuals and companies can protect themselves from such risks.

Mobile phones have been around for over 30 years; they have played an integral part on how people communicate with one another. Initially, mobile phones were only used to make phone calls and communication was limited to voice-calls.

As technology improved, so did mobile phones. In 2001, the first commercial mobile 3G Network was released in Japan. Ever since then, mobile phones have become more than just mere telephones – they have become mini portable computers able to surf the Internet, check e-mails, and even run simple computer programs and games.

These new smartphones have revolutionized how people connect with the outside world. It has also created a new outlet for cyber criminals to phish for information. Security systems have become more open because of the portability of smartphones.

# 1. The Growing Smartphone Market and its Implications

## Expanding Smartphone Market

The Asia-Pacific smartphone market is expected to double to 200 million by 2016. These smart phones that allow users to surf the Internet and access their email on the go will account for one-third of all the mobile phones in the region.

Smartphones are also becoming more and more appealing to cybercriminals as they contain large amounts of personal data that they can mine on. A team of researchers from University of Hong Kong and Indiana University in Bloomington developed a Trojan, named “Soundminer”. “Soundminer” is able to obtain credit card numbers that are spoken during a conversation or those entered into the smart phone. (Moscaritolo, 2011) “Soundminer”, which targets mobile phone running on Android platforms, show that the threat of mobile malware is real and imminent.

However, most users are not aware of the risks involved with smartphones, while many others argue that mobile malware does not pose any significant threat now.

## Malicious Mobile Applications

The first mobile virus was discovered in June 2004. The virus comes with a mobile phone game named “Mosquito” which sends SMS messages to the game company without users knowing. Since then more and more mobile viruses have made their appearance and with the sharp increase in the number of smartphone users in the recent years, users cannot disregard the threat of mobile viruses any more.

Mobile web browsers and operating systems, like their PC counterparts, contain vulnerabilities that can be exploited for malicious purposes. Researches also suggest that mobile applications are one of the greatest threat vectors for smartphones.

In 1st March 2011, Google removed more than 50 apps from its app market after these apps were found to be carrying a malicious malware called “DroidDream”. But just 4 days later, cybercriminal have hacked and retooled Google’s security update to keep “DroidDream” going.

With cybercrime on the rise, what are the risks owners of smart phone are facing, what are enterprise and developers doing to reduce the risk of users’ devices getting infected and what preventive measure can users practice to reduce the chance of their smart phone getting infected?

# 2. What are mobile malware and why mobile malware

Malwares are now airborne, infecting smartphones in every part of the world.

Mobile malware are electronic virus that targets and infect mobile phone through the internet or installing of infected applications.

Cybercriminals are actively releasing these mobile malware, tapping at the vulnerability of the smartphones as compared to personal computers. Once the smartphone is infected, the mobile malwares can access personal information and even control the smartphone remotely, all without the user’s knowledge.

The combination of vulnerability of mobile firmware, ignorance of the general public on mobile security and the vast data and opportunities the cybercriminals can obtain has led to a significant increase in the number of mobile malware in the recent years. With mobile malware the cybercriminals are able to cause the biggest impact, or reap the greatest rewards with the smallest effort.

# 3. Risks and effects of mobile malware

## Personal Risks

A user of smartphone that has been infected by malware faces the possibility of losing his or her privacy and personal information. According to a mobile security company Lookout, 14% of free apps from iPhone and 8% of free apps from Andriod are able to access users’ contacts. While 33% of free iPhone apps and 29% of free Andriod apps are able to track users’ location.

Those who have their credit card numbers stored in their smart phone, or practices online transaction using their smart phone, face the risk of having their credit card number stolen. If their smart phones are infected with malware, cybercriminal can obtain their credit card and account information with ease. Having obtained these numbers, cybercriminals can then use them to do illegal transactions or sell the numbers to other criminals.

## Trouble for others

Users whose smartphones have been infected may not be aware that they have become a host for the spam and malware. The infected smart phones may send out spam SMS or emails containing malware without the users’ acknowledgement to friends, family and random people. These Users may also experience slow down in their smartphone’s daily operations.

There is also the ongoing threat that mobile devices could be used to smuggle PC-based malware onto corporate networks. When an employee connects his smartphone to the company’s network or to the company’s PC via the USB port, PC-based malware hidden in the smartphone can find in way into the company’s network. This can result in the lost of valuable secret files and documents.

# 4. Actions Taken by Software Developers

Fortunately, software developers have not turned a blind eye towards the multiple risks smartphone users face. They have been actively investing in the area of mobile security for the masses as well as business corporations.

## Software Security Companies

Capitalizing on the growing number of smart phone users and applications, traditional software security companies have also ventured into the field of mobile phone security.

Anti-virus companies such as McAfee have released mobile security software that protects users from viruses, Trojans and even battery-sapping malware. To combat the fact that mobile phones are easily stolen or lost, Kaspersky, another anti-virus company, has released security software that will disable a person’s mobile phone should he or she lose it.

Companies that specialize in mobile phone security have also emerged. Lookout Mobile Security, a San Francisco-based startup company, provides its users with spyware scanners, remote backup functionalities and stolen phone locators.

Investment in smartphone security is increasing as well. In 2010, Lookout Mobile Security received US$19.5M in funding for further development of their smartphone security technology. (McCullagh, 2010)

With the increasing interest in the area of smartphone security, smartphone users can look forward to better mobile security options in the future.

## Operating System Developers

Phone Operating System (OS) developers have also been vigilant in ensuring that users are secure while using mobile phones and related applications. Recently, Android OS developer Google removed several malicious applications from its online application store, “Android Market”. It also released a security update to help affected users repair the damage done by these malicious applications.

However, despite Google’s vigilance, the malicious applications were still downloaded by about 260, 000 devices before Google removed them from its Android Market. It is still up to the user to be cautious when downloading applications online.

# 5. Preventive Measures

As with other areas in cybercrime, most security risks related to using smartphones can be mitigated by understanding the situation and being cautious.

## Update Firmware Regularly

Similar to computer operating systems like Windows and Mac OSX, there are always constant patches to the system to fix any security vulnerabilities. Smartphone operating systems or firmware also has such security updates. Smartphone users should always ensure that the firmware of their phone is the most recent one to prevent any security loopholes that were present in older firmware versions.

## Anti-virus Software

Similar to personal computers and laptops, people must learn to protect their smartphone devices from malware, Trojans and viruses. The most basic level of protection would be to have some form of anti-virus software installed on your smartphone.

Leading software security companies have developed anti-virus software specifically catered to mobile phones and users, especially corporate users, should install these basic forms of protection onto their smartphones.

Having anti-virus software that is not updated is not sufficient to defend users against risks. New viruses and malicious programs are being created every single day and anti-virus software that is not up-to-date would not be able to protect the users from such dangers. Thus, users must get into the habit of regularly updating their anti-virus software to guard against newer types of malware and viruses.

## Use Only Trusted Applications

Even though having the most updated anti-virus software may protect users from most malware and viruses, it is not enough if users themselves carelessly download and run mobile applications.

As mentioned in previous sections, smartphone users have access to hundreds of mobile phone applications. Due to the relative ease to download and install these applications, many smartphone users carelessly download multiple applications a day just to play around with them. However, some of these applications may contain malware or Trojans that infect the smartphone when the application is installed. By the time the anti-virus software detects such malicious software, it may already be too late and users’ security could already be compromised.

The best way to prevent such a situation from occurring is to only download and install trusted applications. Pirated versions of original software should also be avoided as these versions are not checked or verified by the phone software companies like Apple or Google.

# Conclusion

In conclusion, mobile phones have evolved into smart, mini computers that people use not only for communication but also for entertainment purposes. The smartphone market is also growing rapidly.

The general public understands the importance of desktop security and how to protect their computers and laptops, but most people are still unaware of the security issues when using smartphones and how to protect themselves.

Mobile security issues are steadily gaining the attention of prominent software security companies as well as phone operating system developers and the amount of protective measures available to the public is growing steadily.

Ultimately, it is up to the user to make sure that their smartphones do not become another source for hackers to phish for their information or to obtain any sensitive information about their lives.

# Bibliography

AFP. (2011, March 24). *Asia-Pacific smartphone use seen doubling by 2016*. Retrieved from http://www.channelnewsasia.com/stories/technologynews/view/1118562/1/.html.

Hypponen, M. (2006, November). *Malware Goes Mobile*. Retrieved from http://www.cs.virginia.edu/~robins/Malware\_Goes\_Mobile.pdf.

Joris Evers. (2011, February 08). *McAfee Q4 Threat Report Identifies New Attacks on Mobile Devices; Malware Growth at All-Time High*. Retrieved from http://investor.mcafee.com/releasedetail.cfm?ReleaseID=548284.

Kaspersky. (n.d.). *Kaspersky Mobile Security 9*. Retrieved from http://usa.kaspersky.com/products-services/home-computer-security/mobile-security.

Liebowitz, M. (2011, March 10). *Hackers Hijack Android Security Update*. Retrieved from http://www.securitynewsdaily.com/hackers-hijack-android-security-update-0598/.

McAfee. (n.d.). *Wireless device protection against viruses and other cyber threats*. Retrieved from http://us.mcafee.com/root/product.asp?productid=mobile\_info.

McCullagh, D. (2010, December 23). *Lookout raises US$19.5M for smartphone security*. Retrieved from http://www.zdnetasia.com/lookout-raises-us-19-5m-for-smartphone-security-62205331.htm.

Moscaritolo, A. (2011, February 17). *RSA Conference 2011: Smartphone threats imminent, security lacking*. Retrieved from http://www.scmagazineus.com/rsa-conference-2011-smartphone-threats-imminent-security-lacking/article/196563/.

Moscaritolo, A. (2010, September 01). *The mobile app risk*. Retrieved from http://www.scmagazineus.com/the-mobile-app-risk/article/177100/.

Musil, S. (2011, March 7). *Google activates kill switch to remove malicious apps from Android Market*. Retrieved from Cnet Asia Website: http://asia.cnet.com/crave/google-activates-kill-switch-to-remove-malicious-apps-from-android-market-62207472.htm