Summer 2012

A Survey of Mobile Computing Security Issues and Possible Solutions

Glenn Kimpell
Governors State University

A Survey of Mobile Computing Security Issues

And Possible Solutions

By

Glenn Kimpell
A.A.S., Joliet Junior College, 2004
B.S., Governors State University, 2010

Submitted in partial fulfillment of the requirements
For the Degree of Master of Computer Science,

Governors State University
University Park, IL 60466
2012

Table of Contents:

Contents Pages:

Introduction:

Technology is ever so changing. The new latest craze over time turns out to be more or less a good laugh when looked into retrospect. These new devices have power that is unfathomable. Year after year it also increases. With that kind of power at to close at hand new problems arise.

I have always been a person intrigued by technology. I would read about these new items that are coming to market and every once and a while invest in that product. One of the items I did end up purchasing is this new $400 telephone which was unheard of called an “iPhone”.

This iPhone would solve all my troubles. So I thought. This item was an exquisite centerpiece of attention. At the time there were few people who could see the potential of the device. Mostly from people who were not tech savvy. These people saw this iPhone as a mere novelty. I saw this as the world at my fingertips.

Technology has also changed along with the people. The people who disgraced the so called novelty phone have now become what they have hated. They are owners of them. This is an incredible change in position from prior times. There are more and more people adapting to smart phones.

The market of cellular phone users has drastically changed in the last few years. More and more people have traded in playing snake on their Nokia phone for an Android or iOS device. These so called phones are actually portable miniature computers.

All phones run on operating systems but with the intense capabilities of the new smart phones the operating systems have become increasing larger [2]. There are people out there to capitalize on the data they can exploit from these phones. The best defense in security is knowledge. There is vast information on protecting your home personal computer but protecting a mobile device has not been in the forefront.

Mobile security but that can be quite vast. I have shifted the focus to areas that are beneficial to what is around us. Approximately 99% of the data communications around the world are done on networks that use either CDMA or GSM technology. There are also many different operating systems and even variations of the same operating system. Once again focus will be done on operating systems that represent 99% of the devices out on the market [1]. Most malware is created to infect the most users at a given time. With this being said there are other networks that can and will be compromised but the market isn't sufficient to make each and every one of them mentionable.

1.) Operating Systems:

The most popular mobile devices out today run operating systems such as iOS, Symbian, Windows Phone, Bada, Android, and BlackBerry OS [8]. It is vital it have knowledge of the current operating system because the malware exploits the vulnerabilities in the operating system.

iOS is an operating system that is created by the Apple Corporation. iOS is installed on hardware that is also created by them. The current products that run iOS are iPhone, Ipod Touch, iPad, and Apple TV. The current build is 5.1.1. iOS 6.0 is due the fall of 2012 [9]. The operating system is based off OSX and UNIX. Not only do they support the Apple series of process they are also ARM compatible. Apple employs security on their phones by using digitally signed code and running the code in a sandbox. The full year shipments for 2011 shows iOS having a 19.1% market share [8]. iOS devices do not support any version of Java including J2ME. Apple and BlackBerry make their own software for their own hardware. This pattern is showing a more secure device in general.

New features do present another security challenge. The Iphone 4S had the advanced feature know as “Siri”. With Siri the phone could run commands from voice. There was a security issue that with a phone which was locked was able to perform commands such as sending a text message. This was fixed by the way of the new firmware update [10].

Symbian is an operating system that is owned by Nokia [11]. This OS is now being abandoned for the Windows Mobile operating system. Symbian is a dying breed among because it is soon to be dropped. Although Symbian is being dropped for Windows Mobile it still was able to ship out a 16.4% market share [8]. This will drop in the near future while Windows Mobile will increase. Symbian systems can have the use of J2ME. J2ME is another potential source for malicious code. One of the Symbian vulnerabilities that were proprietary to the operating system was the Cabir Bluetooth worm. This worm would propagate though the Bluetooth network every time the device was powered on [5].

Windows Phone is an operating system created by Microsoft. This Os is installed on different platforms of multiple manufacturers. They have a basic minimum hardware requirement to run the operating system. The current build is Windows Phone 7.5. The operating system is based off of the Windows CE. This is also ARM compliant. The market share is at 1.4% for 2011 shipments [8]. Since Nokia is changing from Symbian OS to Windows Mobile this OS should increase in market share [11]. J2ME is not supported on Windows Phone.

Windows 7.5 had an issue when a malicious messages. A malicious message could be sent from SMS and even instant messenger applications such as Windows Live Messenger or Facebook Chat. The message would force a shutdown and a reboot. After the reboot it would complete a denial of service attack on the messaging hub [12].

Bada is an operating system that was created by Samsung. This OS is proprietary to Samsung. The current stable release is 2.0.5. They use their own proprietary kernel called Real-Time Operating System (RTOS) or a Linux kernel [13]. Bada has a 2.7% market share [8]. Phones that run Bada can use J2ME which has been known to have malicious code. This is another potential source for an attacker.

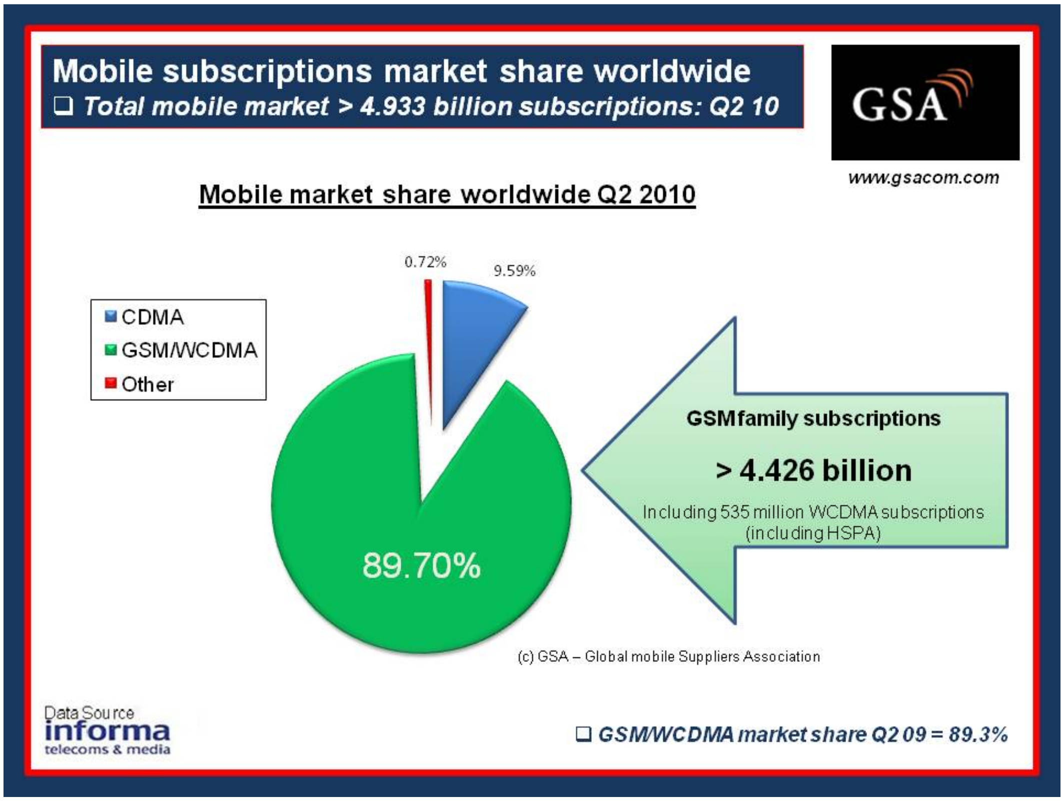
Android is an operating system that is created by Google. Android is installed on many different platforms of multiple manufacturers. This Os is installed on many devices from phones, tablets, watches, and even refrigerators. The current build is 4.0.4 Ice Cream Sandwich [14]. They are soon to release the next version of the Operating System which is called “Jelly Bean”. This operating system is based off of Linux. With Android 3.0 and later they have incorporated full encryption [15]. Along with being ARM compliant it can also run on MIPS and x86 systems. Android operating system runs applications in a sandbox mode [7]. This keeps the user in a safety mode from the kernel. Android notes that in order to break out of the sandbox the kernel itself must be compromised. Android has the most market share for 2011 shipments at 48.8% this is approximately twice as many shipments than its nearest competitor which is iOS [8]. This is primarily to Android having the adaptability to be used on different manufactures phones. Multiple vendors have them as an operating system instead of having their own proprietary operating system. J2ME is not supported directly by Android. There are other applications that can be installed to access the features of J2ME.

Android uses a different approach on security. Rather than regulate and enforces strict rules an application they let the user be in charge. Permissions are enforced at the local machine [15]. The user should monitor what the application is allowed to see and do. This creates an issue with novice users. Users may not be aware of what is happening on their device and assume that everything is good. The program will be setup to ask for permissions to access a specific item the request can give more permission to an item than is truly needed.

Blackberry OS is and operating system that is created by Research In Motion [17]. Their software is installed on proprietary phone that run its OS. BlackBerry 10 will be launching as the current build soon. This operating system is licensed for BlackBerry phones exclusively. BlackBerry OS has a 10.5% market share of shipments for 2011 [8]. BlackBerry also does not support J2ME. BlackBerry is quite secure in the same way Apple is. They build the software for the hardware that they are using. Blackberry had a recent security flaw with its web kit. This had to be done with a website that was created by an attacker. If the user were to visit that site it could result in a remote code execution [29]. This is with a Blackberry device that runs the Blackberry 6 operating system. When the system gets exploited the attacker can access the read and write area of the built in storage. Other areas such as contacts which are located on the internal files system are not affected. This issue at the time of this document is not even a year old. There is a fix for it and it involves updating the operating system [16]. Users need to be aware what version of software they are running.

2.) Network Types:

In the world there are two major types of cellular networks. Figure 1 shows GSM “Global System for Mobile Communication) and CDMA (Code Division Multiple Access) networks cover about 99% of the people in the world [1]. There is a larger divide among the two networks. GSM has a larger share at about 90% and CDMA has the remaining 9% [1]. Europe has a fonder liking of the GSM standard while the United States has a larger percentage of CDMA subscribers. GSM has been around much longer than CDMA .



Mobile subscriptions market share worldwide

❑ *Total mobile market > 4.933 billion subscriptions: Q2 10*

www.gsacom.com

❑ *GSM/WCDMA market share Q2 09 = 89.3%*

Figure 1: Market Share of GSM / CDMA.

GSM uses an encryption method called the A5/1. This encryption has been around for over 20 years. The enemy of any type of encryption is time. With time new ways and even faster ways of accomplishing the same task are eventually uncovered. This form of encryption is still widely used. In the near future something will have to be done to ensure the transmissions are not as easily decrypted. With GSM devices they incorporate the use of SIM cards (Subscriber Identity Modules).

The SIM ciphering key produces a 64 bit key. It has been shown that the bigger the key size it is exponentially safer from attack. a 64 bit encrypted key has 2^64 possible keys. There were known attacks that had to only process 25% of the keys for success. Since 2^64 is actually 18,446,744,073,709,551,616 they rounded them up to 18,500,000,000,000,000,000 which is 1.85* 10^19. 1.85* 10^19 divided by 4 is 4.625*10^18 this is the value they calculated to brute force. In the end it would take 36,700 years to crack the code. On the other hand it would take 1,440,000,000 years to do the same thing on 128 bit encryption. This all was done in relation to a 3.2 Ghz Pentium 4D machine in 2006. They also projected that if speed would quadruple every four years this would significantly reduce the time of the attack. A machine in 2006 which took 36,700 years to break the 64 bit code in 2028 could potentially process that same amount of data in about 4 days [6].

CDMA is the other form of network. This form of network evolved after the GSM standard. What is does is allows for multiple users to access the network by using the same frequency but at different patterns or codes. This allows the CDMA system to have a higher capacity than that of the GSM network. It has about five times the GSM network capacity [20]. CDMA can be more easily related to the ability to detect one's own language in a room full of people speaking other languages. The other languages will be rejected and be understood as noise. This network can be beneficial in highly populated areas. If we can get more users on a network than before this will also reduce cost in the higher capacity areas because not as much equipment or support will be needed. As stated before the global network is much smaller than GSM this is largely due to GSM was there first.

Similar to GSM there are algorithms that are used to ensure security. CDMA has flaws just like GSM. CDMA uses “CAVE” algorithm for authentication. It also uses CMEA and ORYX to protect the data. There are possible attacks that can be ran on those algorithms similar to the GSM attacks. A plain text attack has been used on GSM networks as well as CDMA networks [21]

Both GSM and CDMA networks that cover 99% of the people on the globe have common flaws [1]. CDMA has a benefit over the GSM technology. So far attackers have not successfully captured the CDMA digital packets. Without the packets there cannot be any type of cryptanalysis preformed. That in itself doesn’t guarantee that it cannot be compromised at a later date. This in itself is a great benefit over the GSM network. The United States has more CDMA compatible networks that are being used than other countries.

3.) Safe Practices:

Mobile security is also being aware of your device itself. Devices are compromised easier when they are in the hand of an attacker. Once in the hand of an attacker they have all the time they need to get what they want. Besides being conscience of the whereabouts of the device it is essential to know what features the device possesses. These devices have the ability of connecting to other devices on a network in other forms than the cellular connection. Tablets are more plentiful than ever and many do not have a self sustained connection. They provide the availability to connect to wifi and to Bluetooth.

A user using wifi on a mobile device needs to practice the same precautions because they are using someone else's connection. The router that they are connecting to hopefully will not be tracking your packets but there isn't a for sure way to know. The other users on the network can be also be capturing packets without anyone one knowing. If the mobile device is capable of using its own connection it is much safer to use [22]. The data that is being transferred is encrypted on another medium. It would take different equipment to acquire information.

Bluetooth is a type of short range wireless type. When connecting to a Bluetooth device it must be setup so it knows who to send what. Bluetooth uses a pin number to address the device. Most pins by default are 0000 [3]. Many people don't change the default pin. Users who do change them should also think about not using easily guessed pins such as "1234"[3]. This is a huge security breach since any user can address their device to that network and interpret the communication. The simple step of creating a new pin will help the security of the device.

4.) Jailbroken Devices:

Jailbroken devices are referred to iOS devices that have been programmed to circumvent the original operating system. This allows for code to be run in an elevated way [23]. There have been instances where malicious code has affected iOS devices that have been jailbroken.

Once the device is jailbroken it can run whatever code it is given without it being signed by Apple. A modified iOS device would prevent unauthorized code from event happening. Jailbroken devices have even been able to run Android OS.

Tools for Jailbreaking are blackra1n, PwnageTool, redsn0w, or Spirit. There are many tutorials on how to Jailbreak your iOS device. Once the device is Jailbroken there is an online app store called “Cydia” [23]. This is similar to other app stores on how it applications are downloaded and installed. Users can create their own applications and have to bypass digital signature protection to get their application to be functional. With Cydia anyone can host any program that they desire. There are definite security flaws that can cause problems if any program can be installed and ran. Applications can have similar names to confuse users and once installed and ran the damage can be unknown.

The monitoring of code in comparison to other app stores is relatively nonexistent. In regards to the security aspect the benefits of executing any code to having a more secured device do not make it worthwhile. Security expectations of these jailbroken devices should not be taking lightly. If fact they should not be used to connect to data on a network. There is huge risk involved that the operator most likely will not see or not know.

Software that is available on the Apple app store is significantly safer. Apple applies a digital signature to approved applications. Without the digital signature the code will not be processed on a non jailbroken Apple device [24].

5.) App Stores:

One of the major security issues of mobile devices surrounds app stores. Malicious code has been found on some apps. People are too trusting when they install them. Each of the major companies that have been explained before have an app store. There are variations of how they are run. The app store provider does make applications but allows for third party developers to create them. There are guidelines and some are vague in how they are described. There is a process for approval for these apps too. Some stores review code and digitally sign them as safe from malicious code. Some do not go to that lengthy process. The apps do have a "terms of use" on what they can access so it should be also read with care. Some applications ask for your current location. Users should ask themselves if the location service is really needed. There is no need for a calculator program to know your location.

Malicious software is on the rise. The main reason is the way the application gets approved. The Android store has an open applications store model. Unlike the iOS programs Android programs lack the code signing and an application review process that Apple enforces. Since the code isn't approved this now becomes a breeding ground for malicious code.

Kapersky Labs Figure 2: shows the differences between the main operating systems and the signatures it detected [4].

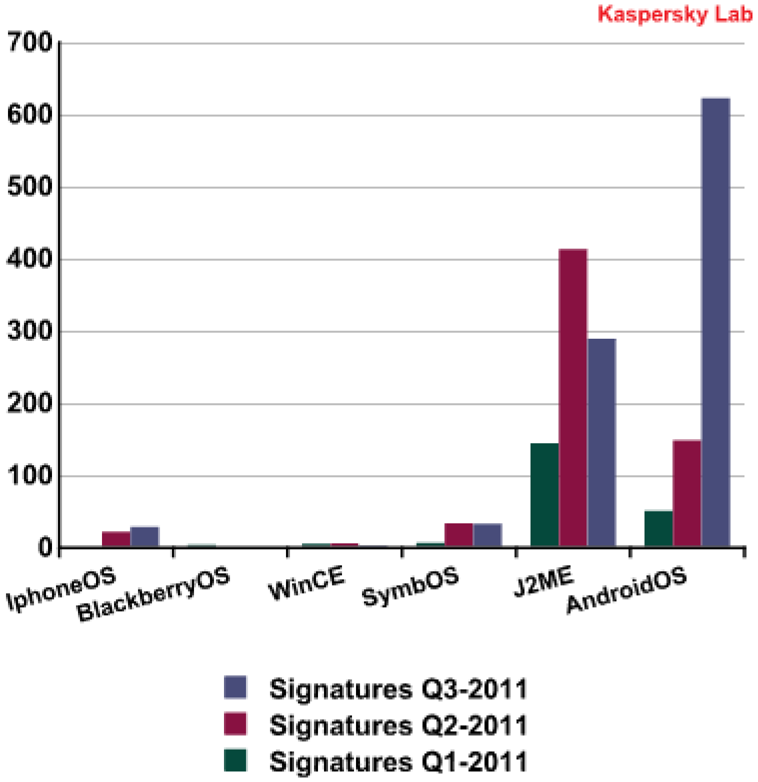


Figure 2: Signatures Based on Operating System.

It is obvious that Android has a much larger market of malicious activity brewing. A thing to note is the J2ME devices that are listed use a form of Java. J2ME is not supported on devices such as Black Berry 10, Windows 7 Mobile, Iphone, or even Android. It is used on so called lower end devices that use Symbian or Bada. Since Symbian is now being phased out the J2ME attacks will most likely diminish.

6.) Notable Issues:

Although mobile devices are quite powerful they have one huge disadvantage. The devices are designed to be portable size is a huge factor. The mobile devices are tiny and could easily be smaller but are limited by their battery. The battery makes up most of the size of the device. Too small of a battery and the device will not last till lunch. Too big and the device loses its portability. The battery is the ultimate resource of the mobile device. Many processes also diminish the battery life. With personal computers they are usually plugged in and the battery resource is not a vital. This eliminates the worry of excess battery consumption. Virus programs along with malware applications can monitor the computer at startup. Personal computers when they have a virus program it is usually signature based. These applications can run and scan the entire time the computer is running. If that was the same with a mobile device it would be much safer but, the use would be shortened significantly [25].

Another potential risk that needs to be understood is the risk in social engineering. Social engineering use social skills like talking or messaging [27]. This is more of a targeted attack. This attack is not random. Attackers can research a person and gather information about them based on what they said or by the people around them. There is more homework to be down with social engineering. Once the attacker infiltrates the victim they can have a bigger payday on the value of the data. Most accounts are linked to a single email address. When that email address gets compromised it is then much harder to reset those accounts because they are linked.

The use of legacy devices poses another potential threat. Devices are constantly being updated and improved but at some point support will end. Software does have a life cycle in which patches and updates are given. After that window the device is then not supported by the manufacturer. If the manufacturer is not monitoring the software there is no one else to. Exploits that have been uncovered are now not taken care of. These exploits are public and can gain attention of attackers [26]. It is hard to justify the upgrade when the device is physically functioning. The security of the device is now on a short fuse when support has been revoked.

7.) Possible Solutions:

Power will be an increasing priority of manufacturers. Devices need to have excess power to give to antivirus applications. If power was unlimited antivirus can be running and monitoring the device. At this time battery life is being jeopardized by using antivirus at all times. Not that antivirus is a fail proof solution it will significantly help in comparison to no antivirus.

Legacy devices are a forgotten potential problem. Similar to some of the issues stated with Apple and Blackberry devices the problem is fixed with an update. If they are not supported anymore the updates are not given. At some time the device even though it is still functional needs to be deactivated or taken out of service. In time cellular devices with eventually shift to a more client server adaptation. There have been some devices that are pioneers in this field such as the t-mobile sidekick which uses “cloud” technology. The devices can then be simplified while the server can process the information remotely. This will significantly help with battery life because the true processing is not done locally. This may save battery but there may be more security problems occurring from a cloud based system that are unknown. The device can then be virus scanned at the server too.

Eventually the networks will have to be upgraded. The United States has some providers who support the CDMA network over the GSM. Time is the worst enemy of encryption. The GSM networks have been around for some time and have had some security issues. Computers are only getting faster and that does not help the security when attacking encryption. The CDMA network is younger in time and does benefits over the GSM.

App stores will need to be monitored more efficiently. Apple and Blackberry have an edge at this moment. They make the hardware for the software they use. It’s a tighter circle to infiltrate. There is a lot of power for a user to create and distribute an application by themselves. The power is good to have but it can be abused.

Social engineering is only going to become an easier tool to use for attackers. Many people who are offering information online are not savvy enough to understand the privacy and security issues. People are too trusting and do not understand the settings on sites they use. After time this will have a plateau effect because more users are online and are becoming more aware of their surroundings. The attackers will have to find more ways to gain access instead of using the played out "Spanish prisoner" attack that has been used for quite some time [28].

With all this information and technology it wouldn't be anything without people. People will get better at what they are doing on their mobile devices. These devices are social so more and more people will eventually succumb to being a beloved owner of one of these devices.

8.) Survey:

A survey was created for the simple fact of getting to know the market. We have seen before that all the operating systems have had some security flaws. This particular survey had over approximately one hundred participants.

What is your age?

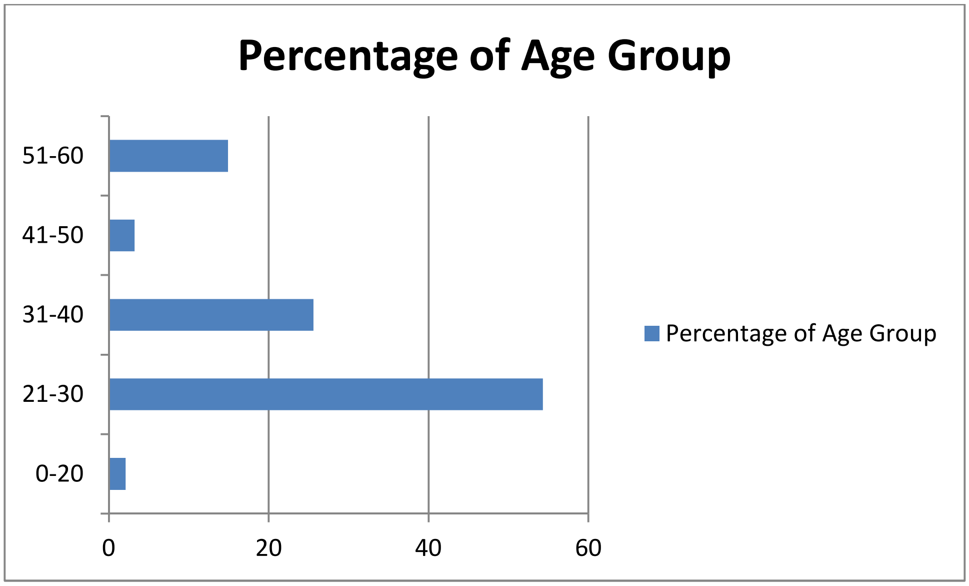


Figure 3: Percentage of Age Group.

Approximately 80% of the people surveyed are within the 21-40 age brackets per Figure 3. There is also a divide in that bracket itself. There are more than double in the 21-30 age bracket. This does show a little bit of a divide on who is more open up to get a smart phone. People in this age group grew up with more tech items. While the younger maybe too young to afford.

Male or female?

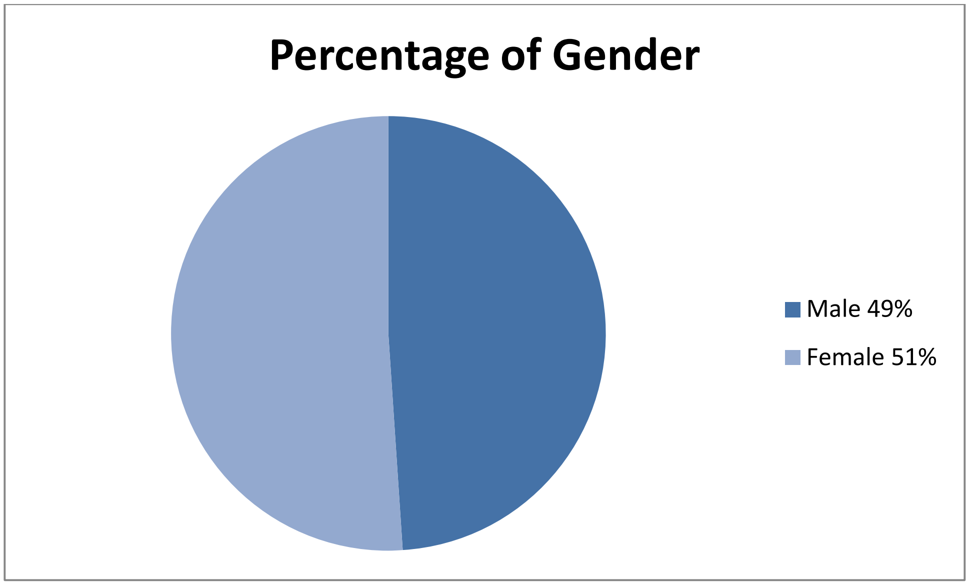


Figure 4: Percentage of Gender.

Figure 4: visually displays a small variation on gender across the survey. The difference in this figure is only a single percentage point. One could say that everyone can see the use in these devices regardless of sex.

Do you have a smart phone?

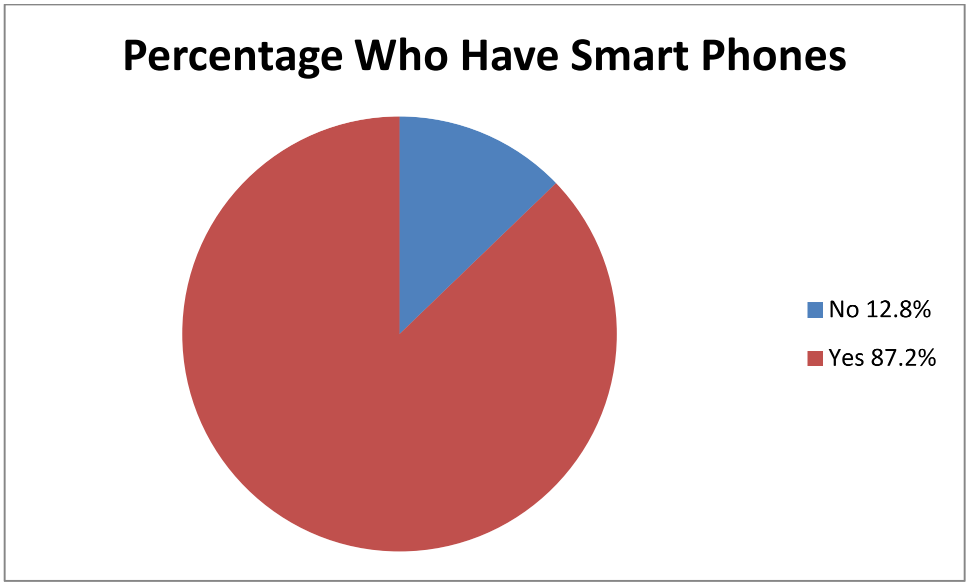


Figure 5: Percentage Who Have Smart Phones.

Of the people surveyed Figure 5: represents that a staggering amount of users that have smart phones. If this survey was given five years prior one could argue that the numbers would be reversed. This shows that the smart phone trend has been on the rise.

If you have a smart phone how long have you had it?

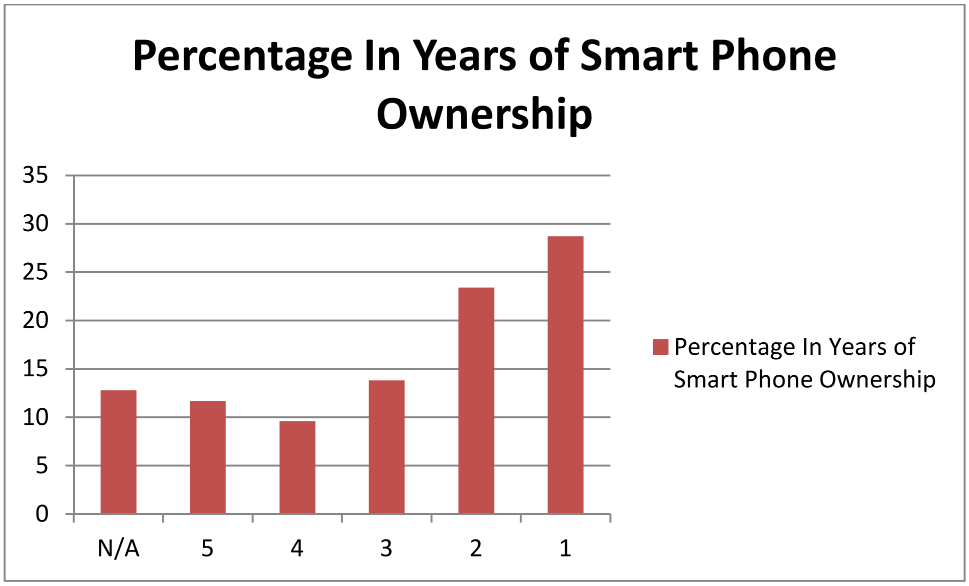


Figure 6: Percentage in Years of Smart Phone Ownership.

For the last for years of the people surveyed the percentage has increased as shown in Figure 6. Approximately thirty percent have bought a smart phone in the last year. This also shows that the people who do not have a smart phone are approximately thirteen percent. The trend cannot be expected to keep on adding more subscribers at the same rate as before.

If you have a smart phone would you go back to a basic phone ever?

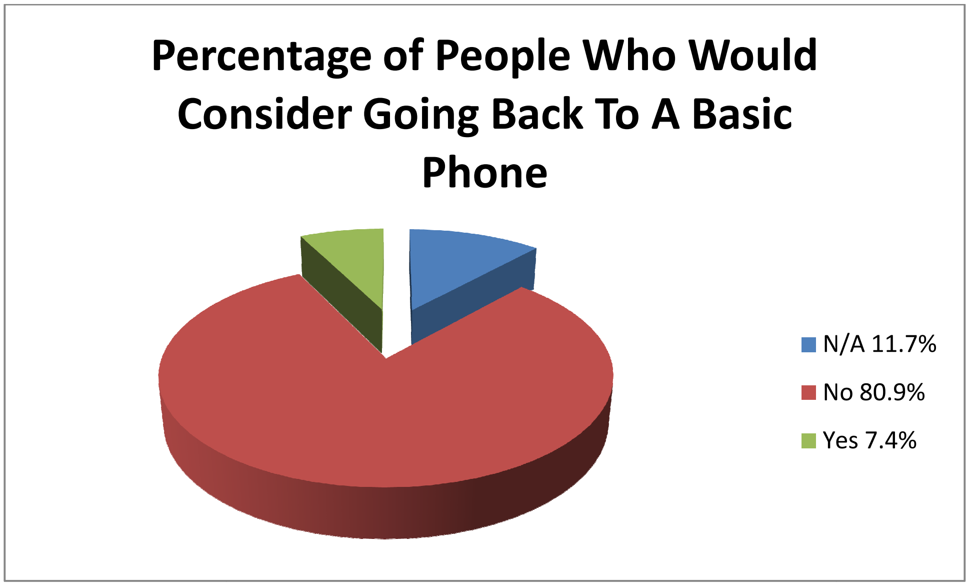


Figure 7: Percentage of People Who Would Consider Going Back to a Basic Phone.

Data from Figure 7 reveals that once you get a smart phone there is a slim chance of getting out. People who have a smart phone said that they are keeping it at a significant rate. There is a small margin that some people would go back to a basic phone though.

How safe do you feel your data is from attackers?

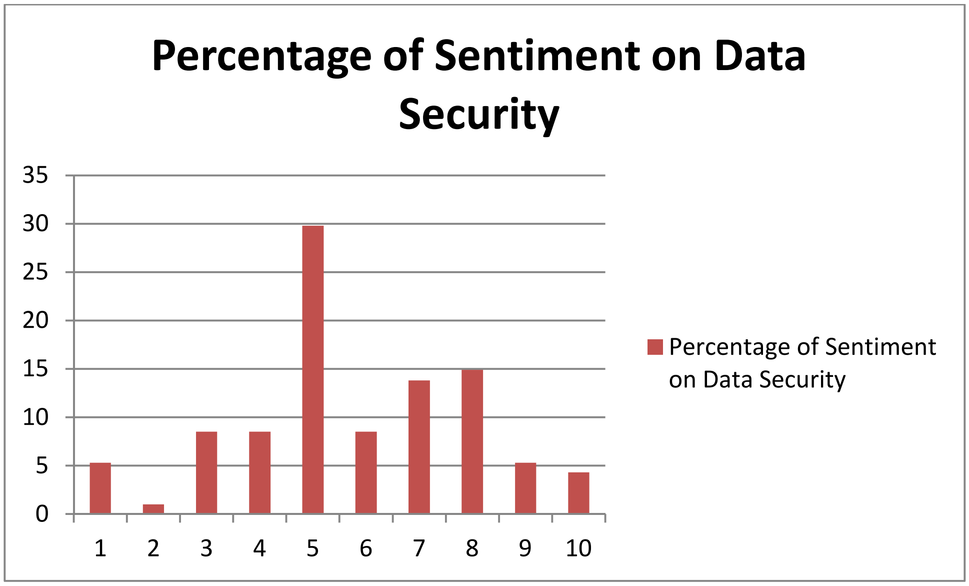


Figure 8: Percentage of Sentiment on Data Security.

In Figure 8: many of the people chose a “5” which is a safe answer. After the removal of the middle answers and add them up we find that there are twenty two percent below five and forty above six. Roughly twice the amount of people feel that their data is more safe on their phone than not.

How safe do you feel the data transmission from your phone is free from attackers?

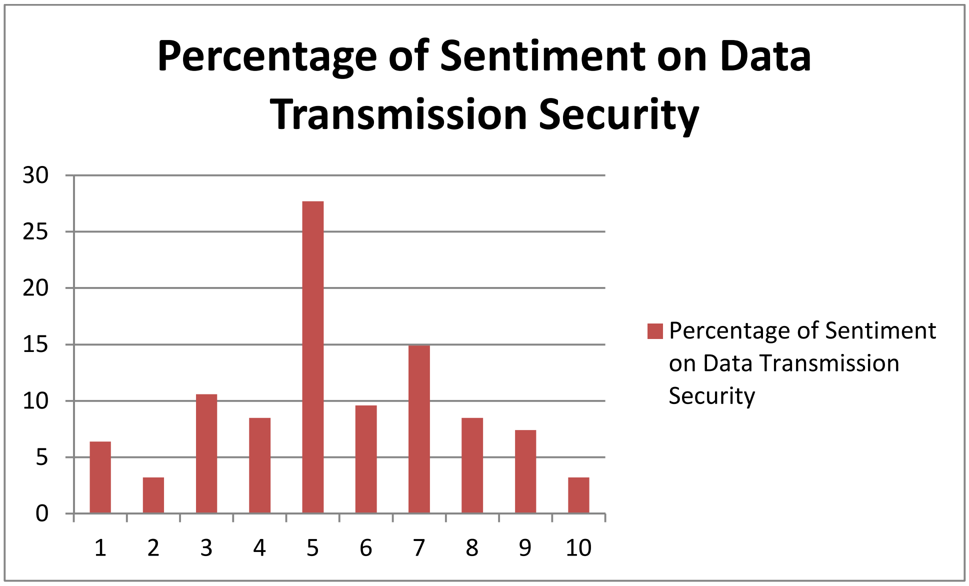


Figure 9: Percentage of Sentiment on Data Transmission Security.

When we take the same scenario as the previous question and remove the five and six answer we find that the result of Figure 9: is similar. The range is much closer.

9.) Closure

Times have moved fast in the computer world. The mobile computing has grown exponentially. The networks have not been updated at the same speed. The CDMA network was shown to be more secure than the GSM network. Many of the potential threats do revolve around the user though. Users need to be more conscious of their own devices. The updating of software and the use of passwords other than default ones are easy precautions to follow. The percentage of people who are smart phone users are huge. These people will be increasingly become more proficient at their devices. These devices have only been around prominently for five years. I am eagerly waiting on the next generation devices along with their potential problems. There is now a better understanding of what happens beyond making a simple call. With this knowledge one can help reduce threats.

Sources:

[1] http://www.gsacom.com//downloads/charts/GSM_market_share_global.php4
[2] http://en.wikipedia.org/wiki/Operating_system
[3] http://www.nsa.gov/ia/_files/factsheets/I732-016R-07.pdf
[4]http://www.kaspersky.com/about/news/virus/2011/IT_Threat_Evolution_n_Q3_2011_From_Malware_in_QR_Codes_to_Targeted_Attack_on_Corporations
[5] http://www.symantec.com/security_response/writeup.jsp?docid=2004-061419-4412-99
[6] http://tjscott.net/crypto/64bitcrack.htm
[7] http://source.android.com/tech/security/index.html#android-security-overview
[8] http://www.idc.com/getdoc.jsp?containerId=prUS23503312
[9] http://www.apple.com/ios/
[10] http://news.cnet.com/8301-27080_3-20122632-245/bad-siri-shell-let-anyone-use-a-locked-iphone-4s/
[11] http://www.developer.nokia.com/Community/Wiki/Category:Symbian
[12] http://news.cnet.com/8301-1009_3-57341918-83/sms-flaw-reportedly-found-in-windows-phone-7.5/
[13] http://www.bada.com/whatisbada/index.html
[14] http://www.android.com/about/
[15] http://source.android.com/tech/security/index.html#android-security-overview
[16]http://www.cio.com/article/692407/New_Security_Flaws_ID_d_in_BlackBerry_6_OS_Enterprise_IM_Apps
[17] http://us.blackberry.com/software/smartphones/blackberry-7-os.html
[18] http://www.techmagnifier.com/482/applications/gsm-vs-cdma.aspx
[19] http://www.sccs.swarthmore.edu/users/08/ajb/tmve/wiki100k/docs/Code_division_multiple_access.html
[20] http://www.pcmag.com/encyclopedia_term/0,1237,t=CDMA&i=39462,00.asp
[21] S. Gayal, S. Manickam. Comparative analysis Of GSM And CDMA technologies. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.11.3538 [22] http://www.esecurityplanet.com/trends/article.php/3929541/How-to-Securely-Manage-WiFi-on-Smart-Phones-and-Tablets.htm
[23] http://www.hackthatphone.com/3x/read_me_first.html
[24] N. Seriot. iphone privacy (2010) retrieved from http://seriot.ch/resources/talks_papers/iPhonePrivacy.pdf
[25] http://www.techrepublic.com/blog/smartphones/are-antivirus-applications-necessary-on-the-android-mobile-platform/2670
[26] http://www.mysecurecyberspace.com/secure/e-commerce/threats/data-theft.html
[27] http://www.us-cert.gov/cas/tips/ST04-014.html
[28] http://en.wikipedia.org/wiki/Spanish_Prisoner

[29]http://btsc.webapps.blackberry.com/btsc/viewdocument.do?noCount=true&externalId=KB26132&sliceId=2&cmd=displayKC&docType=kc&ViewedDocsListHelper=com.kanisa.apps.common.BaseViewedDocsListHelperImpl