ISSN 1991- 8690 الترقيم الدولي 8690 - 1991

Threats and Solutions to Mobile Devices

Ali Ghalib Mohammed Khidhir
Department Of Physics. Science College. Thi-Qar University
E-mail: ali.khidhir@gmail.com
Tel: 07811838982

Abstract

Mobile devices have now surpassed personal computers (PC) in terms of popularity. Smartphones now come with powerful multi-core processors, loaded with considerable amounts of memory and are capable of carrying out complex operations with relative ease. However, this increase in technology has meant that it has now become susceptible to some of the same problems that PC's face. In this paper, I will talk about the malware, virus and other security problems facing mobile devices and their possible solutions.

Keywords: Threats facing Mobile Devices, Apple iOS, Google Android, mobile vulnerability, smartphone malware.

الخلاصة

تجاوزت الاجهزة النقاله (الهاتف المحمول والآي باد ومثيلاتها) اجهزة الكومبيوتر في شعبيتها وشيوعها. فأجهزة الهاتف الجديده لها انواع متطوره من حيث المعالج (CPU) والحجم الكبير لذواكرها مما يمكنها من انجاز عمليات واوامر معقده وبشكل سهل. بيد ان هذا التطور صاحبه مشكلات مماثله لما تعرضت لها الكومبيوترات قبلها. في هذا البحث سناتي على ذكر بعض من هذه المشكلات وخصوصا فيما يتعلق بالبرمجيات المؤذيه (malware) والفايروسات ومشاكل الاختراقات غير المسموحه لهذه الاجهزه والطرق الممكنه لمعالجة هذه المشكلات.

الكلمات المفتاحية :التهديدات التي تواجه الاجهزة النقاله, نظام تشغيل ابل iOS , كوكل اندرويد, نقاط ضعف الاجهزة النقاله ,الهواتف الذكيه والفايروسات

1.Introduction

The appearance of smartphones and other forms of mobile technology has ushered in a whole new period of the Information Era. Operations that were once limited to workstations and laptops have now become possible on handheld devices that are both lightweight and portable. In very little time, these mobile devices have become more popular than personal computers (PC). The reason for this is understandable.[8] Smartphones now come loaded with considerable amounts of memory and are capable of carrying out complex operations with relatively acceptable speed. Additionally, these devices are lightweight and possess none of the bulk that PCs and laptops do. Moreover, the appearances of specialized applications – or "apps" – now enable users to employ smartphones for literally thousands of specialized tasks.9 Some common examples include watching movies, reading books, accessing the World Wide Web (WWW), taking and storing photographs, learning foreign languages, conducting online banking functions, paying credit card and utility bills and more. Unfortunately, this new mobile technology comes with a great deal of risk as well. Yet many consumers remain unaware of the variety of ways in which their wireless devices can be compromised. Although portable (tablets / phablets) and mobile devices use many of the same operating systems that PCs and laptops utilize, media coverage and awareness of mobile vulnerability is far from comprehensive.2 However, it is this very reliance upon computer-based operating systems that renders mobile technology susceptible to the same kinds of intrusions that PCs commonly suffer, including data theft and viral exploitation. Moreover, consumers' constant use of mobile devices means that these units generally contain a great deal of personal and exploitable information, including bank account data, credit card numbers, website log-in credentials, and even intimate photographs.5 Hackers and data thieves have numerous ways to steal all of this personal information. Yet as the problem escalates, so do the means of combatting it and preserving the integrity of mobile technology.

2.Threats Facing Mobile Devices

The data contained in mobile devices is more easily stolen than one might believe. The simplest way to lose data is to simply misplace one's smartphone. The party that finds the device is then able to access the information it contains, provided adequate passwords have not be employed. The inclination to steal data is more widespread than many people understand. One study carried out by Symantec, a well-known manufacturer of information technology security software, revealed that a majority of people who come across misplaced smartphones attempt to obtain personal information or exploit these devices in other ways.[23] Symantec's study involved the purposeful misplacement of mobile devices in such a way that strangers could easily find them. A total of fifty smartphones were tagged with specialized tracking software and left sitting in various public places across the U.S.[23] These smartphones also contained a hidden software program that reported back to the company on how the device was being used. More than forty percent of those who came across a smartphone attempted to access the "owner's" online banking information by clicking on a special app.[23] Even worse, roughly ninety percent of these finders went snooping through the phones in an attempt to discover private data or view personal photographs. Finally, even though these devices contained prominently displayed instructions on how to return them to their owners, only half of the finders attempted to do so.[23] The other half simply discarded them. The temptation to access the data found on smartphones is nearly irresistible. However, some of the risk can be mitigated by putting a security access code on your device. In a report by Lookout, it showed that 70% of people protected their smartphones with a passcode or with the latest Apple iPhone 5S or Samsung's Galaxy 5 Android devices fingerprint identification system.[19] There is also talk of the front facing cameras being used to incorporate them as retinal scanners in the not too distant future.However, the bulk of the threat does not arise through lost devices. The bulk of the threat is actually manufactured by hackers and developers seeking to exploit smartphone capabilities through data theft or other disruptive means. These include direct hacking, such as by determining an owner's password, as well as the use of specialized malware that can steal data and relay it back to the software's creator without the user's knowledge. Indeed, hackers have even developed fake applications that function in the same manner as Trojan Horse. Users download these apps only to have the contents of their smartphones relayed elsewhere. The number of smartphone malware programs in existence, though difficult to estimate, is certainly significant. In one study alone, for instance, in 2012 a study found more than 700 malicious apps were identified in the more than 118,000 that were available on the Android market. 12 Such numbers as these represent a significant global security issue, given that more than a billion smartphones and other portable devices are now in use worldwide. The consequences arising from this exploitation can certainly be disastrous. Not only can credit card and other kinds of financial data be stolen, but various other forms of abuse often take place as well. In 2011, for instance, a longstanding British tabloid called News of the World ceased operations after its reporters were caught recording smartphone conversations and even the voicemails of high profile celebrities.4 In another well-known example, Florida resident Christopher Chaney was charged with multiple counts of hacking into celebrities' mobile devices. Indeed, Chaney's hacking activities were so prolific that he eventually came to the attention of the FBI, after posting explicit pictures of film actress Scarlet Johansson on the Internet.33 Celebrities are not the only ones who fall victim to smartphone hacking, however. It is also possible for hackers to intercept text messages and exploit the information they contain as well. This is how people who transmit explicit pictures of themselves to a loved one for example, can end up being victims of blackmail. Commonly known as "sextortion," the practice involves forcing people to send explicit pictures of themselves to a predator in order to keep other private images of themselves from being posted online.32 Indeed, several smartphones application have appeared that enable hackers to secretly sift through photographs and texts (MMS messages) on targeted devices and save any images they so desired.[8] Sextortion is, of course, against the law, but the anonymous nature through which it is carried out often makes it difficult to investigate and prosecute. A smartphone version of electronic phishing malware has also been developed. Phishing involves the creation of fake emails pretending to be from a trusted source, such as a bank or credit card company, thereby inducing users to give away sensitive personal and financial information. When private data is collected through fake text messages, the technique is called "SMishing."[37] In other instances, data thieves may resort to "vishing," the use of fake voicemails

pretending to be from the smartphone owner's network provider, bank or other institution.[37] With vishing, users receive an urgent voice mail falsely informing them that their account has seen unusual or suspicious activity, and that they need to call a specific number in order to clear the matter and have their privileges restored. Calling the number, however, merely puts them in touch with a fake customer service representative, who steals their information by pretending to be a trusted entity.[37] Such bait and switch tactics as these have also proven difficult – if not impossible – for investigators to root out and abolish. Another potential risk for smartphone users exists in the form of global positioning system (GPS) software. In 2005, the Federal Communications Commission (FCC) mandated that mobile companies make "at least 95 percent" of all mobile devices traceable through GPS. The rule was enacted for safety purposes, so that rescue workers could quickly find someone calling for help from an unfamiliar location. [28] However, the ability to track a phone's geographic location sometimes enables others to exploit that information. GPS tracking, for instance, has enabled abusive spouses to track down victims who were fleeing domestic abuse.[28] Moreover, GPS is often impossible to disable. In 2011, for instance, the *Wall Street Journal* discovered that even when tracking functions have been turned off, most smartphones continue to record location coordinates for later referral. [31]Malware can have detrimental consequences for more than simply the individual device owner; however, indeed, the recent introduction of bot technology means that mobile malware can create large scale security risks as well. In 2009, for instance, the Zeus bot first appeared. Its purpose was to steal and transmit users' banking data. [26] Since then, new bots have been created that carry out this and similar other kinds of tasks. For example, some bots can take over the device's communication and Internet functions without the device owner's awareness of it. Thiscapabilityrepresents a serious problem, indeed. With enough infected smartphones under its control, a terrorist organization could feasibly orchestrate the phones to carry out distributed denial of service (DoS) attacks on significant targets. 10 Denials of service occur whenever traffic overload renders a specific website inoperable. All the bot owner need do is direct the devices to flood the target's website with too much traffic. The site in question might be an essential governmental website or that of a utility company, for instance. Indeed, if the website proves vulnerable, it may even be possible for the bot owner to use a smartphone to carry out an intrusion or upload malware to the site itself. It is by no means far-fetched to imagine that a networked of hijacked devices - commonly called zombie phones - could be used to bring about a utility failure or some other major disruption.10 Yet the use of smartphones to carry out an attack is such an effective cloaking technique that bot creators have also proven themselves to be difficult to trace and identify.The potential consequences of malware attacks become ever more severe as society increases its dependence upon what is known as the Internet of Things. The Internet of Things is a gradually developing configuration of devices interacting with one another through various domains, protocols and applications.2 Programmers and developers anticipate that this growing array of machine-to-machine (M2M) connectivity will bring automation to a variety of domains that are currently under human control.2 For instance, the Internet of Things may one day bring complete automation to air transportation as devices on jet airliners communicate with devices on the ground, transmitting and receiving flight plans, travel instructions and so on. In its complete state, the Internet of Things may constitute a complete infrastructure of automation and may likely regulate a wide array of disparate functions, such as meteorological measurement, air traffic control, record storage, television and Internet broadcasting, utilities delivery, and much more. The social impact that mobile malware could bring about under such a configuration would be of no small consequence. Through viral uploads and orchestrated DoS attacks, a hostile entity could potentially trigger massive shutdowns and even life-threatening scenarios. Malware could theoretically be used to ground airplanes, slow highway traffic, halt commerce, and even detonate devices from a remote position.[2] Moreover, because all of these various functions would be interconnected by various M2M configurations, an attack on one sector could feasibly lead to fallout in other domains as malware jumped from network to network and from system to system.[2] The same virus used to halt street traffic, for instance, might also be deployed to disrupt banking operations or destroy electronic health records. Thus, while the problem of malware is certainly significant in the present day, it will likely be considerably more critical in the very near future.

3.Other Challenges

Although the effort to develop better mobile safeguards is well underway, there are nonetheless a variety of challenges that further impede progress. Many smartphone users simply do not understand that malware poses a serious threat to mobile devices. In short, they "treat mobile handset malware as a problem which has not happened yet, or believe that it's not an issue which really concerns them."[8] Such attitudes create unnecessary risk by dissuading smartphone users from taking even the most basic precautions. Yet for the want of a few preventive measures, a vast network of mobile devices worldwide remains highly susceptible to data theft and other forms of malware-based electronic exploitation. Another major challenge lies in the fact that many mobile devices have limited computing capabilities. Although a high-end smartphone may contain a great deal of memory, it hardly matches that of a newer PC model.[35] Smartphones also run on limited amounts of power and must be recharged on a recurring basis.[35] These design issues present certain challenges that security professionals must find ways of overcoming. Any protective measures that are developed must be capable of running on low capacity processors while also consuming very small quantities of electricity. Otherwise, the safeguards that are installed will undermine the device's other capabilities, making them considerably less effective and potentially undermining their market value. It is also the case that smartphone malware does not operate in the same manner as PC-directed worms and viruses. Whereas workstation malware targets a single operating system, such as Microsoft Windows, hackers have chosen a hybridization approach for targeting mobile devices.[8] On the one hand, the malware is capable of infecting different devices from different manufacturers. On the other, it is also capable of executing multiple forms of sabotage.[8] The same smartphone virus, for instance, may be written to steal financial information, retrieve and transmit personal photographs, and take control of a device's Internet activity.[8] As a result of this hybridized approach, an increasing number of mobile devices are becoming vulnerable to numerous forms of electronic exploitation.The manner in which smartphones connect to the Internet and to other devices is also a challenge that security designers have to navigate. Whereas PCs access the Internet via discrete networks, smartphones also connect to the web using text message and mixed message (SMS/MMS) protocols. [16] They are also able to communicate and relay information to other devices through WIFI, Bluetooth and Near Field Communication (NFC) technology. In recent years, however, virus authors have learned how to infect smartphones using mobile and Bluetooth delivery systems.[16] This approach makes mobile malware considerably more difficult to contain. These extra connectivity methods mean that even when a device is disconnected from the web, it can still be hacked and infected. This is because mobile devices are always turned on and receiving data through SMS, WIFI, Bluetooth and NFC reception.8 Additionally, the fact that smartphones are always on makes malware difficult to contain geographically, primarily because mobile devices almost always travel with their owners. Yet as infected smartphone owners move about from place to place, they may be unknowingly infecting other devices they brush up against. [8] Finally, there is the problem of polymorphic coding. Polymorphism is an approach by which virus manufacturers mask the malware's true functions beneath coding designed to meet other purposes.[1] For instance, a downloadable video game may contain a hidden subroutine that instructs it to gather data and transmit it to a specific email or smartphone address. Because of these multiple functioning protocols, polymorphic malware can be difficult to recognize even through inspection. This is the case because the program is also executing legitimate functions while concealing stolen information within its own coding.[1] It is precisely because the software is seemingly harmless that it is able to cloak its true directives and continue to secretly gather information from unknowing smartphone owners for weeks, months, or potentially even years at a time.

4.Mobile Operating System Vulnerabilities

When looking at the three main mobile operating systems—Apple's iOS, Google's Android and Microsoft's Windows Mobile — there are clear trends in how devices are affected by malicious software. '97 percent of mobile malware is on Android devices. Windows Mobile and Apple's iOS boasted less than one percent combined'.[18] While the statistics are revealing, it is important to note that infiltration can and does occur on all three operating systems.

4.1 Apple iOS

Apple is careful about what is offered to iPhone users, ensuring apps are as safe as possible. This careful quality control contributes to the protection of iOS devices against malicious software. " Apple doesn't need an anti-virus program for iOS because it doesn't

leave room for a virus (or trojan or other malware etc.) to get into the system in the first place."[34] When iPhone owners use their phones as intended and purchase apps through Apple's app store, there is no need for additional protection. Apple checks apps rigorously before approving apps for sale, ensuring there is no malicious elements that can infiltrate iPhones once the user downloads the apps. Despite Apple's careful monitoring of apps released to users, developers who create viruses and malware are inventing ways around the process, leading to viruses and malware that can be leaked to users, as was evidenced by a Russian-based virus in 2012 and the research into "Jekyll apps" in 2013.In July 2012, iOS was faced with its first virus, which caused newly updated apps to crash when opened.[7] "A Russian-language app called Find and Call, which was available in both the Apple App Store and Google Play, has been discovered to be the cause of the bug, Wired reported." 7 The Trojan, once downloaded, stole and uploaded the user's address book to a remote server, then spammed email addresses and phone numbers in the address book.Once the Trojan was discovered by Kasperksy antivirus experts, and the app was immediately removed from both Google Play and the Apple App Store and an investigation into the malware was conducted, with the goal of tightening development regulations to combat malware. In 2013, researchers at the Georgia Institute of Technology revealed a method allowing them to slip malware through Apple's approval process for iOS apps. "Their 'Jekyll' app was created with remotely-exploitable vulnerabilities built in, masked by legitimate features to evade detection during the App Store approval process, but ready to be triggered once the app was installed on an iOS device."[6] This research highlighted vulnerabilities in Apple's processes, showing researchers, developers, and users that it is not perfect. As developers learn vulnerabilities like these, Apple will likely have to rethink its position that antivirus software is not needed on iOS products, even if malware is rare due to the stringent approval process.

4.2 Google Android

One of the draws of Android devices is the openness of Android to allow developers to create apps and make them available to users. Unfortunately, the open-source operating system also leaves users open to malicious software.One of the most famous infiltrations into Android was Heartbleed, which occurred earlier this year. Eadicic.[27] Much of the publicity surrounding Heartbleed was its impact on computers because it was an Internet bug, but it did affect Android mobile devices running older versions of software, as well. "Millions of devices globally using Android version 4.1.1 (codenamed Jelly Bean), which was released in 2012, carry the Heartbleed flaw. And while Google has 'applied patches to key Google services,' according to the company, individual wireless carriers and handset makers still need to push out the fix".[27] Android has adapted to the possibility of malware by installing security measures that allow users to verify apps. "Devices running Android 2.2 or higher, which essentially means nearly all Android devices in circulation today, have access to Google's malware scanner. Prior to installing an application you downloaded outside of the Play store, Google will scan the app and warn you of any potential threats".[13] This helps protect users from malicious code on their phones. Unfortunately, since one of the major draw to Android by users is the open-source operating system, malicious software will continue to be a very real possibility.

4.3 Microsoft Windows Mobile

Specific apps that offer virus protection for Windows phones is not as widely available. This is because, like Apple, Windows phones offer protection through their app store called Windows Marketplace, which provides security before the apps are approved to become available to users.This is not to say that there are no threats to security for Windows Mobile users. However, instead of viruses and worms, personal information is gathered from users through fake scams and alerts that trick users into thinking their phones are infected. This leads users to then give credit card and other personal information to try and get anti-virus protection that likely does not exist.[20] In addition, in 2010, malware was discovered hidden in Windows Mobile apps that made expensive calls across the globe, at cost to the users.[21] "Someone has copied the programs and repackaged them with the malware inside, John Hering said. Once the app is installed the virus wakes up and starts dialing premium-rate numbers."21 In most cases, the victims did not know about the infiltration until receiving their phone bill with the added charges.In the case of this malware, Microsoft claimed that the problem was not vulnerability in Microsoft software, so it could not simply be patched. Instead, the company placed the responsibility on the users, urging them to be aware of what they download, and from where. .[21]

5.Threat Prevention Techniques

Given the various threats that malware and viruses pose to mobile operating systems, security professionals have been actively working to enhance safeguards against them that are capable of infecting mobile devices. Yet the existence of so many special challenges makes the development of new preventive techniques especially difficult from a coding and engineering perspective.

5.1 Firewall

One major line of defense against mobile malware exists in the form of the personal firewall. .[11] By installing a personal firewall such as NoRoot for Android and Firewall iP for iOS, a smartphone owner can block uninvited traffic and restrict devices from accessing inappropriate Internet protocols.[24, 25] Hackers who come up against firewalls are unable to probe a network or device for exploitable weaknesses. A personal firewall can even protect systems that are already infected. Once the firewall goes up, the malware can no longer send out stolen data or communicate with an offsite server.[11] In short, the zombie functions of a hijacked device are considerably reduced. Moreover, a firewall can limit Bluetooth and wireless accessibility to a smartphone, making it difficult for hackers to target devices in public settings, such as libraries, airports, coffee shops and Internet cafes.Firewalls are only of limited effectiveness, however, because they cannot prevent traffic from entering a device through ports that are already being utilized. As Friedman and Hoffman have written, firewalls "are like security guards who can shut unneeded doors and windows in a building, but cannot identify intruders who enter by the front door."[11] This is the reason why other security measures are also necessary for smartphone owners.

5.2 Anti-Spyware & Anti-Virus

These include anti-spyware and anti-virus packages such as AVG Family Safety which is available for Android, iOS & Windows Mobile devices and are capable of scanning incoming traffic over a given network.[3] Programmed to recognize the signature coding of malware, this software can isolate viruses and worms, thereby preventing them from infecting smartphones and other devices.[8] Unfortunately, though protective packages for handheld units are currently in existence, they are not yet widely available on the market. However, many security experts believe such software will see wider usage as the problem of malware continues to proliferate across platforms and devices.11 Yet anti-viral ware has its limitations as well. As security measures grow more sophisticated, virus writers devise new methods of attacking both handheld and PC units. Designer malware, for instance, can be especially difficult to identify and filter, which partially explains why malware detection rates are only at 70 percent or so.[11] Additionally, anti-virus software is typically written in response to new viruses that appear. Consequently, malware typically has a two to three month head start on anti-virus programmers, which means that the newest variants of worms and viruses are usually capable of getting past software-based detection systems.11 In short, then, there is never a period in which mobile devices are completely secure from malware attacks.The inability of anti-viral software to keep pace with malware means that other security measures are also necessary. One method of intrusion detection involves behavioral analysis. When signature scanning techniques fail to identify malware, it still remains possible to safeguard a system by isolating incoming packets that behave in an unusual manner, the way malware is inclined to do.[8]

5.3 Intrusion Prevention System

For instance, specially designed intrusion prevention systems (IPS's) can detect traffic attempting to enter a system through an inappropriate port or one that is attempting to carry too many header packets.[22] Such behaviors are contrary to standard Internet traffic protocols and, hence, are usually indicative of an attempted malware attack. The value of an IPS is that it is also able to sniff out newer versions of malware, based on their unusual behavior patterns, and then set them aside for later inspection by anti-virus programmers.[22] Thus, not only do they help keep present systems secure, but they also play a role in the constant effort to upgrade against new malware. The IPS approach is also better suited for smartphones than the traditional anti-virus software. Anti-virus software operates through signature recognition, which requires a great deal of storage capacity and processing power, ultimately slowing down the phones usual speed and response times to actions and processes. An IPS program, however, instructs a device to trust or distrust incoming traffic based on the manner in which it is behaving. It is essentially a limited checklist that the device is programmed to follow.[8] Therefore the memory requirements are considerably lower. For instance, an IPS may instruct a system to only acknowledge and install applications that come with an acceptabledigitalsignature,trusted

developers/manufacturers. The system itself then follows these instructions, thereby preventing the need for a large database of malware signatures that consumes both memory and processing power.The IPS behavioral analysis approach is far from foolproof, however. For one thing, there is considerable disagreement over the degree of flexibility that should be built into an IPS package.8 It almost goes without saying that at least some degree of built-in flexibility is necessary. Otherwise, virtually no traffic would get through at all, since there is no singular behavioral pattern that all valid traffic follows. For example, the RacingPost (most popular horse racing publication in the UK) has applications for iOS and Android which are not available through normal mobile application stores due to gambling restrictions and uses multiple ports to send and receive live data needed for the application to work and is a perfectly legitimate, may otherwise be deemed inappropriate by the IPS if the restrictions are too stringent, thus preventing the application from working correctly. Yet too much flexibility significantly raises the likelihood of a malware attack, since too much deviant traffic is allowed access to the system.8 On the other hand, the lack of flexibility can prevent perfectly harmless and even necessary traffic from accessing the device. This is particularly a concern when software upgrades behave in ways that an IPS is unable to recognize. Although the software may be completely valid and even integral to the device's functioning, the IPS will prevent the system from accepting it. Consequently, the device may grow more susceptible to malware attacks over time for the simple reason that it is not receiving timely updates.

One way to circumvent the flexibility issue is to enable IPS programs to perform code analysis on suspicious traffic loads. Once the code has passed the IPS filtering system, it can gain access to a device's operating system.8 However, code inspection requires numerous comparative functions, by which the IPS filter compares suspicious traffic against previously validated coding formats.8 Yet, such an operation would require access to an existing library of code tables, which would consume considerable amounts of both power and memory. In light of this difficulty, "smartphones be able to access online code libraries that would enable the IPS to compare incoming traffic against online resources".8 Such a solution would both enhance security while also preserving smartphone resources. However, there are considerable proprietary and copyright issues in existence that currently make such a solution difficult to implement and is very reliant on having a good data connection which is not something everyone has around the world yet.

5.4 Sandbox

Other improvements in code analysis are currently in development. One package prototype, for instance, is the sandbox methodology, a multi-dimensional analysis tool that isolates and executes unusual traffic packets in a controlled environment.[15] Sandboxes work by creating a rootkit structure that essentially mimics the operating system of a mobile device.[15] Believing it has gained access, the software begins to execute its programming within the self-contained sandbox environment, where it undergoes careful scrutiny without creating any damage. Once the analysis has been completed, legitimate software is allowed to proceed to the actual operating system, while actual malware remains locked in the sandbox environment.[8] As an additional measure, the captured code is uploaded to an online malware database for future comparative purposes.[8] As other systems intercept the same malware, they need merely compare its coding against that stored in the malware library. Ultimately, this method allows for malware detection in a manner that saves much needed computing power while also avoiding the potential risks associated with additional sandbox analyses. Unfortunately,malware writers have already learned their way around most sandbox protocols. For example, every sandbox package uses as a standard product identifier, and ID code consisting of a string of several digits.[15] For this reason, malware often comes with additional packets containing a built-in ID registry. Because the product IDs associated with these sandboxes are permanent, the malware need simply identify a product code in order to recognize that it is in a virtual environment.[15] Once this determination has been made, the malware is often able to conceal certain code strings and mask itself as ordinary software. Once released into the operating system, however, the malware carries out an entirely different set of protocols. For this reason, sandbox manufacturers are now striving to develop new masking techniques that conceal their product identifiers and thereby avoid malware detection.[15] Yet this approach also presents complications, since most operating systems will not accept software packets that come without a standard product identifier.

5.5 Application Monitoring System

While sandbox programmers work to create a more realistic virtual environment, other developers have been working in the domain of Application Monitoring. Application Monitoring Systems requires the use of specialized software that observes system behaviors and searches out specific anomalies that are usually indicative of malware.8 Such anomalies usually include the overconsumption of computing resources as well as uninitiated telephone calls, messaging, or Internet visits to sites that are not part of the device owner's online patterns. One example of an application monitoring system is VirusMeter, a prototypical application that sniffs out malware by looking for overuse of energy and memory sources.[14] VirusMeter works by developing profile of the owner's usage patterns and then comparing the device's activities against these patterns. Significant variations in system behavior can serve as an indicator of a potential viral infection.14 However, a virus does not always explain a shift in human behavioral patterns, which is why packages such as VirusMeter remain yet another an imperfect solution to the ongoing malware problem.8

Even so, VirusMeter and similar programs are on an important track. In order to combat malware more effectively, it will likely be necessary to take the device owner's usage patterns into greater account "user has his own unique and private operational patterns (e.g. while operating keypad or touch screen), which cannot be easily simulated by malware." [8]

5.6 Hidden Markov Model

The Hidden Markov Model (HMM) is able to determine whether a specific action has been initiated by the device owner or by a malware program. [8] Such programs might also include tracing functions that research the destination of outgoing calls and Internet visits, not only to determine whether malware is present in the system, but also the exact functions it is performing.[8] It may also be possible to identify malware by the file types it tries to access. Accessing and defacing critical files is a behavior common to almost all malware.

5.7 Mandatory Access Control

Some researchers have envisioned the implementation of a mandatory access control (MAC) system that functions as an internal safeguard against file defacement.[36] The MAC could feasibly be structured as an additional layer of code that serves in a locked door capacity, barring access to programs that fail to meet scripted protocols and policies.36 It might feasibly be injected at the system's root level, which would be beneficial for two reasons;

i. First, the MAC would be configured as part of the system's trusted computing base, rather than an add-on application with less dynamic functionality.

ii. Second, the additional coding and execution capacity would consume far less energy and memory under these circumstances.[8]

To date, however, an effective MAC has yet to be developed for smartphone utilization. While such programmable features may operate well in the PC environment, "kernel-level solutions, such as a built-in MAC application"8 are too difficult to be implemented on smartphones and other devices.8 Even so, efforts to develop an effective MAC defense structure remain ongoing.36 However, it may be necessary to redesign a device's entire operating system in order to achieve maximum benefit and functionality parameters.

6. Device And Infrastructure-Based Detection Methods

The MAC approach offers what is commonly known as a device-based detection method. Device-based detection is an anti-malware typology that utilizes programming built right into the operating system's basic architecture.[8] Device-based detection may someday serve as a template for installing sandbox systems that come without the product identifiers that malware is capable of sniffing out. While such an approach would have the advantage of utilizing fewer resources, it is nonetheless a costly route to take, and primarily because a reconfiguration of the device's basic operating system would be required.[8] Moreover, it could only be installed in brand new devices that are coming directly off the production line. Smartphones currently in use would have to accept these solutions in downloadable application format. To date, however, all downloadable malware detection platforms have shown themselves to be high energy consumers due to increased processing power requirements, leading to slower device response times; a problem that can be expensive for the end user and that can render a device unreliable. For this reason, the anti-malware community has shown greater interest in developing detection systems that rely upon the larger network infrastructure. Not only does the infrastructure-based solution consume less energy on the part of the individual device, but it also allows for the collection of malware data in a more thorough and organized manner.[8] One example of an infrastructure-based detection typology is a program that goes by the name of SmartSiren.[38]

SmartSiren operates by seeking out worms attempting to piggyback on SMS messaging traffic and Bluetooth network connections. The program generates a log of the device's communications activities and then develops a composite communications profile, which it then uses to seek out anomalies and abnormal usage patterns.[38] When malware is identified, SmartSiren sends out an alert to all devices that have possibly been infected through telephone exchange or messaging protocols. It also sends out advisory warnings to other smartphones found in the owner's contact list.[8] The logic behind this action is that these units may have been compromised by connecting with another infected device in the owner's contact list. However, the problem remains that infrastructural-based detection is far more costly than device-based strategies. The reason for this added expense is that so many elements are involved in the malware-detection process.[8] However; the infrastructural approach offers greater effectiveness and security because more information is disseminated across a larger number of smartphones. In order to reduce the substantial costs associated with infrastructure detection, some developers have been attempting to devise various infection probability models.[17] These models attempt to predict viral spread rates under various infection scenarios. The purpose of such models is not so much to guess which smartphones and servers will be affected so much as it is to predict how networks will behave when presented with a malware infection.[17] The value in these models lies in the fact that they can serve in an early warning capacity, enabling programmers to identify a possible network-wide malware infection before large scale damage has been accomplished.[17] Because malware detection is so costly for both devices and networks, some researchers have suggested that a hybrid approach would likely be of greatest benefit. Under the hybrid detection model, devices and infrastructure would coordinate resources to ferret out malware anomalies and send out prompt infection alerts.[8] Though several variants of hybrid detection have been suggested, most recommendations fall along the same general lines. Under the hybrid detection model, devices upload individualized communication logs to specialized servers that then scan these logs for irregular calling or texting patterns.[29] The complication here is that servers must establish a baseline of routine behaviors for both the device and its owner. Abnormal increases in communication behaviors can then be examined more closely as potential indicators of a malware outbreak.

7. Conclusion

One important component in determining how to handle malicious software on smartphones is to know whose responsibility it is to protect users from viruses and other malware. Some argue that the responsibility lies with the operating system companies while others argue that it is up to individual users to protect their devices.The true problem is in the mindset of users. Most people continue to view their smartphones as phones rather than as miniature computers. With that mindset, users do not feel the need to protect their devices from malicious software. After all, if that is the case, even efforts taken by Apple, Microsoft, and Android may not prevent users from downloading or installing viruses and other malware. As it is, even efforts by companies outside of Microsoft and Apple are unable to prevent malicious computer software, even with awareness of them and ample software to prevent and delete them.To combat this, Android, Apple, and Microsoft can help shift the mindset of users by treating mobile devices in the same way they treat computers. Raising awareness of protective measures and offering antivirus software and scanning apps can remind users that they must be on guard on their mobile devices, as well.The types of malware that hackers use to seize control of private smartphones are numerous and varied. Some operate as tools for financial theft, while others work to create zombie devices that obey the hacker's commands. Moreover, hundreds of malware variants are constantly striving to invade mobile devices and use them to gain access to mobile networks and interconnected devices. Malware's ability to snake across open networks, however, creates the possibility of potentially devastating fallout. The greatest threat is not to the individual consumer, however, but the growing network of interconnected devices and equipment known widely as the Internet of Things, an infrastructural array that is growing increasingly dependent upon automation and network communications.Thus, a variety of alternatives have appeared in response to the growing malware problem. These include items we have previously discussed such as personal firewalls, anti-viral packet filters and other network-based protections. However, these solutions are costly and tend to slow a device's operability, as do many of the novel device-based approaches to malware, including the sandbox and VirusMeter programs. Yet offloading anti-malware solutions to the communications infrastructure creates problems of its own, primarily those of cost-effectiveness. Therefore, I

suggest that developers should create models that will balance both individual and network based needs while placing a minimal drain on either.It is likely that as malicious software becomes a bigger threat to mobile devices, companies and individual, developers will provide solutions to prevent and combat infiltration. Just as computers offer antivirus software packages, mobile devices should begin to have specialized apps that protect users from viruses and malwares. This kind of apps should come preinstalled in the future.

8. References

1. Alazab, Mamoun, Sitalakshmi Venkatraman, Paul Watters, Moutaz Alazab and Ammar Alazab. "Cybercrime: The Case of Obfuscated Malware." In Global Security, Safety and Sustainability & E-commerce, 204-211. Edited by Christos K. Georgiadis, Hamid Jalakhanj, Elias Pimenidis, Rabih Bashroush, Ameer Al-Nemrat. Berlin: Springer, 2011.
2. Atzori, Luigi, Antonio Iera and Giacomo Morabito. "The Internet of Things: A Survey." Computer Networks 54, no. 15 (2010): 2787-2805.
3. AVG, Protect your phone and keep it running smoothlyhttp://www.vga.com/gb-en/for-mobile
4. Brockett, Patrick L., Linda L. Golden and Anji Song, "Managing Risk in Mobile Commerce." International Journal of Electronic Business 10, no. 2 (2012): 167-184.
5. Casey, Eoghan and Benjamin Turnbull, "Digital Evidence on Mobile Devices," in Digital Evidence and Computer Crime. Edited by Eoghan Casey. Waltham,MA:Elsevier,2011. http://bit.ly/1lSMJld.
6. Dredge, Stuart. "iOS malware can sneak through Apple's approval process, researchers show." The Guardian, August 19, 2013. http://www.theguardian.com/technology/appsblog/2013/aug/19/ios-malware-apple-iphone-ipad-jekyll
7. Eadicicco, Lisa. "Apple iOS App Store Gets First Virus: Learn About the App that Steals Your Contacts and Spams Your Friends." International BusinessTimes,July6,2012.http://www.ibtimes.com/apple-ios-app-store-gets-first-virus-learn-about-app-steals-your-contacts-and-spams-your-friends
8. Elfattah, Marwah, M.A., Aliaa A. A. Youssif, and Ebada Sarhan Ahmad. "Handsets Malware Threats and Facing Techniques." International Journal of Advanced Computer Science and Applications 2, no. 12 (2011): 42-48.
9. Enck, William. "Defending Users against Smartphone Apps: Techniques and Future Directions" In Information Systems Security: Lecture Notes in Computer Science, Volume 7093, 49-70. Edited by Sushil Jajodia and Chandan Mazumdar. New York: Springer, 2011
10. Felt, Adrienne Porter, Matthew Finifter, Erika Chin, Steve Hanna, and David Wagner. "A Survey of Mobile Malware in the Wild." In SPSM'11: Proceedings of the First ACM Workshop on Security and Privacy in Smartphones and Mobile Devices, 3-14. Edited byXuXian Jiang. New York: ACM, 2011.
11. Friedman, Jon and Daniel V. Hoffman, "Protecting Data on Mobile Devices: A Taxonomy of Security Threats to Mobile Computing and Review of Applicable Defenses." Information Knowledge Systems Management 7, nos. 1-2 (2008): 159-180.
12. Grace, Michael, Yajin Zhou, Qiang Zhang, Shihong Zou, and Xuxian Jiang. "RiskRanker: Scalable and Accurate Zero-Day Android Malware Detection." In MobiSys'12: Proceedings of the 10th International Conference on Mobile Systems, Applications, and Services & Co-Located Workshops, 281-294. New York: ACM, 2012.
13. Graziano, Dan. "Protect your Android device from malware." CNET, June 25, 2014. http://www.cnet.com/how-to/protect-your-android-device-from-malware/
14. Hoffman, Johannes, Stephen Neumann, and Thorsten Holz. "Mobile Malware Detection Based on Energy Fingerprints – A Dead End?" In Research in Attacks, Intrusions, and Defenses: 16th International Symposium, RAID 2013, Rodney Bay, St. Lucia, October 23-25, 2013 Proceedings, 348-368. Edited by Salvatore J. Stolfo, Angelos Stavros, and Charles V. Wright. Berlin: Springer, 2013.
15. Issa, Anoirel. "Anti-virtual Machines and Emulations." Journal in Computer Virology 8, no. 4 (2012): 141-149.
16. Jeon, Woongryul, Jeeyeon Kim, Youngsook Lee, and Dongho Won. "A Practical Analysis of Smartphone Security." In Human Interface and the Management of Information: Interacting with Information, 311-320. Edited by Michael J. Smith and Gavriel Salvendy. Berlin: Springer, 2011.
17. Karyotis, Vasileios, Anastasios Kakalis anSymeon Papavassiliou. "Malware Propagative Mobile Ad Hoc Networks: AsymptoticBehavior Analysis."

Journal of Computer Science and Technology 23, no. 3 (2008): 389-399.
18. Kelly, Gordon. "Report: 97% of Mobile Malware is on Android. This is the Easy Way You Stay Safe." Forbes, March 24, 2014. http://www.forbes.com/sites/gordonkelly/2014/03/24/report-97-of-mobile-malware-is-on-android-this-is-the-easy-way-you-stay-safe/
19. Lookout, Locked Down: Password Protecting YourPhone.https://blog.lookout.com/blog/2011/10/05/locked-down-password-protecting-your-phone/
20. Mayberry, Rick. "Does my Windows Phone need virus protection?" The Telegraph, March 30, 2013.http://www.telegraph.co.uk/technology/news/9952940/Does-my-Windows-Phone-need-virus-protection.html
21. Mills, Elinor. "Malware found lurking in apps for Windows Mobile." CNET, June 4, 2010. http://www.cnet.com/news/malware-found-lurking-in-apps-for-windows-mobile/
22. Modi, Chirag, Dhiren Patel, Bhavesh Borisaniya, Hiren Patel, Avi Patel, and Muttukrishnan Rajarajan. "A Survey of Intrusion Detection Techniques in Cloud." Journal of Network and Computer Applications 36, no. 1 (2013): 42-57.
23. O'Connell, Andrew,Stats & Curiosities from the Harvard Business Review (Boston: Harvard Business Review Press, 2013), 35.
24. Play,Google,NoRootFirewall https://play.google.com/store/apps/details?id=app.greyshirts.firewall&hl=en
25. Rashid, Fahmida Y, eWeek, IT Security & Network Security News: 10 iOS Security Apps to Protect Your iPhone, iPad from Hackers. http://www.eweek.com/c/a/Security/10-iOS-Security-Apps-to-Protect-Your-iPhone-iPad-from-Hackers-492794/
26. Riccardi, Marco, Roberto Di Pietro, Marta Palanques, and Jorge Aquila Vila. "Titan's Revenge: Detecting Zeus via Its Own Flaws." Computer Networks 57, no. 2 (2013): 422-435.
27. Robertson, Jordan. "What a Heartbleed Attack on an Android Phone Looks Like." Bloomberg, April 29, 2014.http://www.bloomberg.com/news/2014-04-29/what-a-heartbleed-attack-on-an-android-phone-looks-like.html
28. Scheck, Justin. "Stalkers Exploit Cellphone GPS." The Wall Street Journal, August 3, 2010. http://on.wsj.com/1zmZyg5.
29. Schmidt, Aubrey-Derrick, Florian Lamour, Christian Scheel, Seyit Ahmet Camtepe and Sahin Albayrak. "Monitoring Smartphones for Anomaly Detection," Mobile Networks and Applications 14, no 1 (2009): 92-106.
30. Turkanovic, Muhamed and Gregor Polancic. "On the Security of Certain E-Communication Types: Risks, User Awareness and Recommendations." Journal of Information Security and Applications 18, no. 4 (2013): 193-205.
31. Valentino-Devries, Jennifer. "IPhone Stored Location in Test Even If Disabled." The Wall Street Journal, April 25, 2011. http://on.wsj.com/UxIVi7.
32. van der Hof, Simone and Bert-Japp Koops. "Adolescents and Cybercrime: Navigating Between Freedom and Control." Policy and Internet 3, no. 2 (2011): 1-28.
33. Vasiu, Ioana and Lucian Vasiu. "Break on Through: An Analysis of Computer Damage Cases." Journal of Technology, Law, and Policy 14, no. 2 (2014): 158-201.
34. Worstall, Tim. "Apple Explains Why iOS Don't Need No Steenkin' Anti-Virus." Forbes, June 4, 2012.http://www.forbes.com/sites/timworstall/2012/06/04/apple-explains-why-ios-dont-need-no-steenkin-anti-virus/
35. Wang, Xiao Sophia, Haichen Shen, and David Wetherall, "Accelerating the Mobile Web with Selective Offloading." In MCC'13: Proceedings of the 2nd, 2013ACM SIGCOMM Workshop on Mobile Cloud Computing, 45-50. Edited by Mario Gerla and Dijiang Huang. New York: ACM, 2013.
36. Xie, Liang, Xinwen Zhang, Ashwin Chaugule, Trent Jaegar and Sencun Zhu. "Designing System-Level Defenses against Cellphone Malware." In SRDS'09: 28th IEEE International Symposium on Reliable Distributed Systems, 83-90. Los Alamitos, CA:IEEE Computer Society.
37. Yeboah-Boateng, Ezer Osei and Priscilla Mateko Amanor. "Phishing, SMishing & Vishing: An Assessment of Threats against Mobile Devices." Journal of Engineering Trends in Computing And Information Science 5, no. 4 (2014): 297-307.
38. Zarch, Seyed Hasan Mortazavi, Farhad Jalitzadeh and Madihesadat Yazdanivaghef. "Data Mining for Intrusion Detection in Mobile Systems." ISOR Journal of Computer Engineering 6, no. 5 (2012): 42-47.