Technical Information Paper-TIP-10-105-01
Cyber Threats to Mobile Devices

Overview

Today's advanced mobile devices are well integrated with the Internet and have far more functionality than mobile phones of the past. They are increasingly used in the same way as personal computers (PCs), potentially making them susceptible to similar threats affecting PCs connected to the Internet. Since mobile devices can contain vast amounts of sensitive and personal information, they are attractive targets that provide unique opportunities for criminals intent on exploiting them. Both individuals and society as a whole can suffer serious consequences if these devices are compromised. This paper introduces emerging threats likely to have a significant impact on mobile devices and their users.

Introduction

As mobile device technology evolves, consumers are using it at unprecedented levels. Mobile cellular technology has been the most rapidly adopted technology in history, with an estimated 4.6 billion mobile cellular subscriptions globally at the end of 2009.[1] Furthermore, technological advances have fueled an unprecedented portable computing capability, increasing user dependence on mobile devices and skyrocketing mobile broadband subscriptions. Mobile broadband connections rose by more than 850% in 2008,[2] exceeding the number of fixed broadband subscribers.[3] Mobile devices have become an integral part of society and, for some, an essential tool. However, the complex design and enhanced functionality of these devices introduce additional vulnerabilities. These vulnerabilities, coupled with the expanding market share, make mobile technology an attractive, viable, and rewarding target for those interested in exploiting it.

[1] International Telecommunication Union. The World in 2009: ICT Facts and Figures. 2009. Retrieved February 3, 2010 from http://www.itu.int/ITU-D/ict/papers/2009/Europe_RPM_presentation.pdf.
[2] GSM Association. Global Mobile Broadband Connections Increase Tenfold Over The Past Year. 2008. Retrieved February 4, 2010 from http://gsmworld.com/newsroom/press-releases/2008/870.htm.
[3] International Telecommunication Union.

In the past, malicious activity targeting mobile phones was relatively limited compared to that of PCs. The proprietary nature and limited functionality of the hardware and software architectures previously used by individual mobile phone manufacturers made this market a less than ideal target for mass exploitation. Current mobile devices have much greater functionality and more accessible architectures, resulting in an increase in malicious activity affecting them. These smartphones include the Apple iPhone, Google Android, Research in Motion (RIM) Blackberry, Symbian, and Windows Mobile-based devices.

Due to the similar functionality of mobile devices and PCs, the distinction between the two has blurred. Mobile devices have become equally susceptible to malicious cyber activity and will likely be affected by many of the same threats that exist for PCs on the Internet. The variety of sensitive information available from a mobile device is also potentially greater and more enticing than that of a traditional mobile phone or computer. Users are more likely to take advantage of the portability and convenience of mobile devices for activities such as banking, social networking, emailing, and maintaining calendars and contacts. The features of mobile devices also introduce additional types of information not typically available from a PC, such as information related to global positioning system (GPS) functionality and text messaging.

A multitude of threats exist for mobile devices, and the list will continue to grow as new vulnerabilities draw the attention of malicious actors. This paper provides a brief overview of mobile device malware and provides information on the following threats to mobile devices:

- Social engineering;
- Exploitation of social networking;
- Mobile botnets;
- Exploitation of mobile applications; and
- Exploitation of m-commerce.

Mobile Malware

Malicious actors have created and used malware targeted to mobile devices since at least 2000. The total number of malware variants significantly increased in 2004 with the public release of Cabir source code.[4] Cabir is a Bluetooth worm and the first widespread sample of mobile malware. It runs on mobile phones using the Symbian Series 60 platform and spreads among Bluetooth-enabled devices that are in discoverable mode. The worm causes a phone to constantly attempt to make a Bluetooth connection, subsequently draining the battery. While this worm was an inconvenience to device users, today's mobile malware is more insidious and often has more severe effects on devices and their users.

A recent and more nefarious example of mobile malware is the Ikee.B, the first iPhone worm created with distinct financial motivation. It searches for and forwards financially sensitive information stored on iPhones and attempts to coordinate the infected iPhones via a botnet command and control server.[5] This worm only infects iPhones that have a secure shell (SSH) application installed to allow remote access to the device, have the root password configured as "alpine"—the factory default—and are "jailbroken." A jailbroken iPhone is one that has been configured to allow users to install applications that are not officially distributed by Apple. Although Ikee.B has limited growth potential, it provides a proof of concept that hackers can migrate the functionality typical to PC-based botnets to mobile devices. For example, a victim iPhone in Australia can be hacked from another iPhone located in Hungary and forced to exfiltrate its user's private data to a Lithuanian command and control server.[6]

Spy software also exists for mobile devices, including some programs being sold as legitimate consumer products. FlexiSpy is commercial spyware sold for up to $349.00 per year. Versions are available that work on most of the major smartphones, including Blackberry, Windows Mobile, iPhone, and Symbian-based devices. The following are some of the capabilities provided by the software:[7]

---

[4] Ken Dunham, et al. Mobile Malware Attacks and Defense. 2009. Burlington, MA: Syngress Publishing, Inc.
[5] F-Secure. Worm:iPhoneOS/Ikee.B. 2009. Retrieved February 16, 2010 from http://www.f-secure.com/v-descs/worm_iphoneos_ikee_b.shtml.
[6] Phil Porras, et al. An Analysis of the IKEE.B (DUH) iPhone Botnet. 2009. Retrieved February 3, 2010 from http://mtc.sri.com/iPhone/.
[7] Flexispy Ltd. FlexiSpy Homepage. 2010. Retrieved February 17, 2010 from http://flexispy.com/.

- Listen to actual phone calls as they happen;
- Secretly read Short Message Service (SMS) texts, call logs, and emails;
- Listen to the phone surroundings (use as remote bugging device);
- View phone GPS location;
- Forward all email events to another inbox;
- Remotely control all phone functions via SMS;
- Accept or reject communication based on predetermined lists; and
- Evade detection during operation.

FlexiSpy claims to help protect children and catch cheating spouses, but the implications of this type of software are far more serious. Imagine a stranger listening to every conversation, viewing every email and text message sent and received, or tracking an individual's every movement without his or her knowledge. FlexiSpy requires physical access to a target phone for installation; however, these same capabilities could be maliciously exploited by malware unknowingly installed by a mobile user.

Cross-platform mobile malware further complicates the issue. The Cardtrp worm infects mobile devices running the Symbian 60 operating system and spreads via Bluetooth and Multimedia Messaging Service (MMS) messages. If the phone has a memory card, Cardtrp drops the Win32 PC virus known as Wukill onto the card.[8] Two proof-of-concept Trojans, Crossover and Redbrowser, further show how widespread attacks could simultaneously hit desktops and mobile devices.[9] Both Trojans can infect certain mobile devices from PCs.

SMS, MMS, Bluetooth, and the synchronization between computers and mobile devices are all examples of potential attack vectors that extend the capabilities of malicious actors. Inherent vulnerabilities exist in modern mobile device operating systems that are similar to those of PCs and may provide additional exploitation opportunities. For example, the most recent Apple security update for iPhone OS 3.1.3 provided fixes for scenarios where playing a maliciously crafted mp4 audio file, viewing a maliciously crafted Tagged Image File Format (TIFF) image, or accessing a maliciously crafted File

[8] Cyrus Peikari. Analyzing the Crossover Virus: The First PC to Windows Handheld Cross-infector. 2006. Retrieved February 17, 2010 from http://www.informit.com/articles/article.aspx?p=458169&seqNum=3.
[9] Bill Brenner. Proof-of-concepts heighten mobile malware fears. 2006. Retrieved February 17, 2010 from http://searchexchange.techtarget.com/news/article/0,,sid43_gci1171168,00.html.

Transfer Protocol (FTP) server could result in arbitrary code execution.[10] To help mitigate malicious activity affecting known vulnerabilities, users should install security patches and software updates as they become available.

Social Engineering

One of the more common methods of spreading malware on the Internet is through social engineering. Most malicious activity is often successful because users are deceived into believing it is legitimate. Exploitation by social engineering is extremely lucrative and will likely significantly increase in the mobile market.

Phishing is the criminal act of attempting to manipulate a victim into providing sensitive information by masquerading as a trustworthy entity. This technique is a well-established, significant cyber threat, and mobile devices provide unique opportunities for phishing, including variants such as vishing and smishing.

Vishing is the social engineering approach that leverages voice communication. This technique can be combined with other forms of social engineering that entice a victim to call a certain number and divulge sensitive information. Advanced vishing attacks can take place completely over voice communications by exploiting Voice over Internet Protocol (VoIP) solutions and broadcasting services.[11] VoIP easily allows caller identity (ID) to be spoofed, which can take advantage of the public's misplaced trust in the security of phone services, especially landline services. Landline communication cannot be intercepted without physical access to the line; however, this trait is not beneficial when communicating directly with a malicious actor.

Smishing is a form of social engineering that exploits SMS, or text, messages. Text messages can contain links to such things as webpages, email addresses or phone numbers that when clicked may automatically open a browser window or email message or dial a number. This integration of email, voice, text message, and web browser functionality increases the likelihood that users will fall victim to engineered malicious activity.

[10] Apple Inc. About the security content of iPhone OS 3.1.3 and iPhone OS 3.1.3 for iPod touch. 2010. Retrieved February 3, 2010 from http://support.apple.com/kb/HT4013.
[11] Ken Dunham.

Regardless of the communication medium, users must ensure that any exchange of information occurs between their intended parties. Links contained in suspicious or unsolicited emails and text messages should be avoided, and to help prevent disclosing sensitive information to an unintended party via voice communication, users can initiate the phone call to a known, trusted number.

Exploitation of Social Networking

Social networking sites, such as Twitter and Facebook, have become mainstays of electronic information sharing. Information sharing often occurs with an unwarranted, inherent trust among users, as they blindly share and accept data from unauthenticated parties. Uniform Resource Locators (URLs) are constantly being exchanged within social networks as users share items of interest. Since a Twitter user is limited to 140 characters when posting an update, sharing a brief statement accompanied by a traditional URL may be impossible. The capability to significantly shorten a URL is provided by several different websites and is often integrated in social networking applications to happen automatically. Shortened URLs are invaluable in this case because they allow a URL with 137 characters to be shortened to 17 characters. For example:

> http://brainstormtech.blogs.fortune.cnn.com/2010/02/12/help-wanted-obamas-twitterer-filibusterers-need-not-apply/?source=cnn_bin&hpt=Sbin
>
> becomes http://u.nu/72q95.

These services provide value, but they also make cyber criminals' goals much easier to achieve. Since the original URL is completely replaced, a user cannot know the destination of the shortened link without clicking on the link. Legitimate URLs are indistinguishable from those that are malicious, providing phishers with an effective cover. This tactic could lure a victim into unwittingly downloading malware or visiting a fraudulent site. It is highly likely that unsuspecting users would not think twice before clicking on the URLs.

Over the course of 2009, Facebook and Twitter experienced a 112% and 347% increase in mobile users, respectively.[12] This growing trend in mobile social networking provides an avenue for the exploitation of mobile devices.

[12] Mike Melanson. Twitter Sees 347% Growth in Mobile Browser Access. 2010. Retrieved March 23, 2010 from http://www.readwriteweb.com/archives/twitter_sees_347_growth_in_mobile_browser_access.php.

Mobile Botnets

A botnet is a set of compromised computers, or bot clients, running malicious software that enables a "botherder" or "botmaster" to control these computers remotely. A botherder or botmaster can design a botnet to perform certain actions, such as information stealing or launching a denial of service, and issues commands to the bot clients from a command and control (C2) server. Since mobile networks are now well integrated with the Internet, botnets are beginning to migrate to mobile devices, as seen with Ikee.B.

Due to their ability to support rich content, MMS messages have a body field where Extensible Markup Language (XML) messages can be hidden.[13] Waledac, a web-based Internet botnet, uses XML messages to communicate. Unlike with Internet communication, Internet Protocol (IP) addresses are not used when exchanging SMS or MMS messages. Instead, mobile devices have an International Mobile Subscriber Identity (IMSI) and Mobile Subscriber Integrated Services Digital Network Number (MSISDN). These numbers are used to authenticate, register, and identify mobile network subscriptions by mapping the device to a phone number. The IMSI is embedded in the device hardware or contained on a removable card such as a Removable-User Identity Module (R-UIM) card in Code Division Multiple Access (CDMA) networks or a Subscriber Identity Module (SIM) card in Global System for Mobile Communications (GSM) networks. The MSISDN represents a phone number and is used to route communication to the subscriber. Domain Name System (DNS) also does not exist on mobile networks, making the use of advanced networking techniques such as fast flux and multi-homing impossible in mobile networks.[14] However, since mobile devices can have constant connections to the Internet, they can potentially be utilized like any other computer while maintaining all of their functionality within a mobile network.

Mobile devices using the Internet may be assigned dynamic private IP addresses that are inaccessible from the Internet, preventing a botmaster from communicating directly with a compromised host. Web-based botnets circumvent this obstacle by having bot clients poll web servers for further instructions. Any additional obstacles presented by using SMS or MMS messages to communicate could also be circumvented by adapting a web server to accommodate SMS and MMS functionality by creating a proxy that understands

[13] Anne Ruste Flo and Audun Josang. Consequences of Botnets Spreading to Mobile Devices. 2009. Retrieved February 2, 2010 from http://nordsec2009.unik.no/papers/RFJ2009-NordSec.pdf.
[14] Anne Ruste Flo and Audun Josang.

this type of communication and has a connection to the Internet. The capability to run a web server on the iPhone has existed since at least mid-2007.[15]

Compromised text messaging services could have severe consequences. In the aftermath of the recent earthquakes in Haiti, reputable charity organizations experienced a massive surge in text message donations. For example, a mobile device user could donate $10 to the American Red Cross by texting HAITI to 90999. In less than 48 hours, donations reached $5 million and accumulated at a rate of $200,000 per hour.[16] A mobile botnet could be configured to send text messages to a donation number set up for nefarious purposes. The donations could be small enough that a victim may not recognize the extra charge on his or her bill. The same concept could potentially be exploited in voting scenarios that leverage mobile devices or to carry out distributed denial of service attacks.

Exploitation of Mobile Applications

Mobile applications, commonly called apps, provide enhanced convenience and functionality. Developers have created myriad mobile applications for various uses and activities, which is contributing to the proliferation of modern mobile devices. Anyone can potentially develop and distribute mobile applications with little oversight, making apps a potential attack vector for cyber criminals.

Several major banking institutions provide legitimate mobile applications that allow customers to conveniently check balances, pay bills, transfer funds, or locate automated teller machines (ATMs) and banking centers. However, banks are not the only ones creating banking-related apps. In early 2010, Google found potentially fraudulent banking applications in their Android Market. An anonymous developer known as "09Droid" sold a collection of banking applications that were not authorized by the banks for which they were seemingly developed.[17] It is unclear if the apps were used to gain access to users' confidential banking information. 09Droid published applications for

[15] Jesus Diaz. iPhone Can Now Serve Web Pages, Run Python, Open Source Apps. 2007. Retrieved February 13, 2010 from http://gizmodo.com/282139/iphone-can-now-serve-web-pages-run-python-open-source-apps.
[16] Amy Feldman. Haiti Earthquake Provokes Wave of Text Donations. 2010. Retrieved February 13, 2010 from http://www.businessweek.com/investor/content/jan2010/pi20100114_236518.htm.
[17] Dan Raywood. Google finds apparently fraudulent banking applications on its Android Marketplace. 2010. Retrieved February 1, 2010 from http://www.scmagazineuk.com/google-finds-apparently-fraudulent-banking-applications-on-its-android-marketplace/article/161047/.

approximately 40 different banking institutions, all of which Google removed from the Android Market.[18]

A similar incident occurred when Symbian unwittingly distributed the Sexy Space mobile worm as a legitimate, digitally signed application.[19] This malware steals subscriber, device, and network information from victims and has the capability to build a botnet. It propagates via spam text messages that are sent from a compromised device to the victim's contacts. The messages, exchanged at the expense of the victims, contain a link to a website hosting malicious applications that will infect the phone if executed. Currently, the Sexy Space mobile worm affects only Symbian mobile devices.

The validation and approval process for mobile applications varies by vendor. The following table provides a brief description of the policies of some of the more popular vendors.

[18] F-Secure. Warning On Possible Android Mobile Trojans. 2010. Retrieved February 13, 2010 from http://www.f-secure.com/weblog/archives/00001852.html.
[19] John Leyden. Sign mobile malware prompts Symbian security review. 2009. Retrieved February 23, 2010 from http://www.theregister.co.uk/2009/07/23/sms_worm_analysis/.

Vendor	Application Store	Application Development Policy
Apple	App Store	Apple requires developers to enroll in the iPhone Developer Program. Every application submitted to the App Store is evaluated by at least two reviewers for bugs, instabilities, unauthorized content, and other violations.[20]
Google	Android Marketplace	No requirements exist for publishing applications in the Android Marketplace. Once developers register, they have complete control over when and how they make their applications available to users.[21]
Microsoft	Windows Marketplace for Mobile	Developers must register with Windows Marketplace for Mobile. All applications sold on Windows Marketplace for Mobile must meet technical standards, be code signed, and pass policy checking and geographic market validation before they can be certified.[22]
RIM	Blackberry App World	Developers must create a vendor account to submit applications to the Blackberry App World. RIM reviews all submitted applications for content suitability and performs technical testing to ensure applications abide by the Blackberry App World Vendor Guidelines.[23]
Symbian	Horizon	Symbian Horizon is a publishing program and directory of Symbian Signed applications. To publish applications here, developers must obtain a Publisher ID and run the full Symbian Signed Test Criteria on applications before they can be made publicly available.[24]

[20] Philip Elmer-DeWitt. 40 staffers 2 reviews 8,500 iPhone apps per week. 2009. Retrieved February 23, 2010 from http://brainstormtech.blogs.fortune.cnn.com/2009/08/21/40-staffers-2-reviews-8500-iphone-apps-per-week/.
[21] Google Inc. Android Market Homepage. 2010. Retrieved February 23, 2010 from https://www.google.com/accounts/ServiceLogin?service=androiddeveloper.
[22] Microsoft Corporation. Windows phone Homepage. 2010. Retrieved February 23, 2010 from http://developer.windowsphone.com/Help.aspx?id=0e4efb7b-2e57-4ff5-b381-117281fc903b.
[23] Research in Motion Limited. Blackberry App World FAQ Homepage. 2010. Retrieved February 23, 2010 from http://na.blackberry.com/eng/developers/appworld/faq.jsp.
[24] Symbian Foundation. Symbian Horizon FAQ Homepage. 2010. Retrieved February 23, 2010 from http://horizon.symbian.org/index.php?option=com_content&view=article&id=52.

Many applications are regularly submitted to vendors for use on these platforms, including some that are malicious. Currently, the Apple App Store contains over 100,000 applications and receives about 10,000 new submissions each week. Apple has received applications that will steal personal data or are otherwise malicious and has rejected them during the review process.[25] As the volume of applications rises, it could be difficult to maintain high confidence in their integrity, regardless of the platform or policy.

Exploitation of M-commerce

M-commerce, or mobile e-commerce, is another growing trend with mobile devices. Consumers can use mobile devices from any location to research product information, compare prices, make purchases, and communicate with customer support. Retailers can use mobile devices for tasks such as price checks, inventory inquiries, and payment processing. For example, Apple Retail Store employees use modified versions of the iPod Touch that allow them to scan barcode labels and accept credit card payments from customers.[26]

The ability to read credit cards with a mobile device is not limited to retailers alone. A quick search for "credit card" in the Apple App Store reveals a number of different applications for accepting credit card payments. Third-party iPhone attachments for swiping credit cards are also available. "Square" is a small device that plugs into the iPhone's headphone jack and can transfer credit card swipe information to the supporting application. It also allows users to authorize payments in real-time via text message.[27] The Mophie "marketplace" is another credit card reader for the iPhone that will be available soon.[28]

Smartphones' credit card reader functionality has the potential to enable criminal activity such as "skimming" and "carding." Skimming is the theft of credit card information using card readers, or skimmers, to record and store victims' data. This activity is often

[25] Arik Hesseldahl. Apple's Schiller Defends iPhone App Approval Process. 2009. Retrieved February 13, 2010 from http://www.businessweek.com/technology/content/nov2009/tc20091120_354597.htm.
[26] Gary Allen. Exclusive look at Apple's new iPod touch-based EasyPay checkout. 2009. Retrieved Feburary 17, 2010 from http://www.appleinsider.com/articles/09/11/03/exclusive_look_at_apples_new_ipod_touch_based_easypay_checkout.html.
[27] Square, Inc. Square Homepage. 2010. Retrieved February 17, 2010 from https://squareup.com/.
[28] mStation Corporation. Mophie Homepage. 2010. Retrieved February 17, 2010 from http://www.mophie.com/product-p/1125_mp-ip3g-blk.htm.

accomplished in conjunction with otherwise legitimate transactions. Carding is the process of testing the validity of stolen credit card numbers. It can be done on websites that support real-time transaction processing to determine if the credit information can be successfully processed. The capability of a single compact hand-held device to perform each of these tasks will further enable malicious intentions.

Conclusion

The user's limited awareness and subsequent unsafe behavior may be the most threatening vulnerabilities for mobile devices. It is critical to understand that a mobile device is no longer just a phone and cannot be treated as such. Unlike the previous generation of mobile phones that were at worst susceptible to local Bluetooth hijacking, modern Internet-tethered mobile devices are susceptible to being probed, identified, and surreptitiously exploited by hackers from anywhere on the Internet.[29] Many mitigation techniques for mobile devices are similar to those for PCs. US-CERT recommends the following best practices to help protect mobile devices:

- Maintain up-to-date software, including operating systems and applications;
- Install anti-virus software as it becomes available and maintain up-to-date signatures and engines;
- Enable the personal identification number (PIN) or password to access the mobile device, if available;
- Encrypt personal and sensitive data, when possible;
- Disable features not currently in use such as Bluetooth, infrared, or Wi-Fi;
- Set Bluetooth-enabled devices to non-discoverable to render them invisible to unauthenticated devices;
- Use caution when opening email and text message attachments and clicking links;
- Avoid opening files, clicking links, or calling numbers contained in unsolicited email or text messages;
- Avoid joining unknown Wi-Fi networks;
- Delete all information stored in a device prior to discarding it; and
- Maintain situational awareness of threats affecting mobile devices.

Anti-virus software exists for some mobile devices, which is one component of a layered defense. However, it can only assist in protecting against known threats. Users need to understand the threats and proactively take steps to avoid them. A high degree of

[29] Phil Porras.

vigilance is necessary to successfully prevent and mitigate future threats to mobile devices.

Additional Resources

- US-CERT Cyber Security Tip ST06-007 – Defending Cell Phones and PDAs Against Attack
- US-CERT Cyber Security Tip ST05-017 – Cybersecurity for Electronic Devices
- US-CERT Cyber Security Tip ST04-020 – Protecting Portable Devices: Data Security
- US-CERT Cyber Security Tip ST06-001 – Understanding Hidden Threats: Rootkits and Botnets
- US-CERT – Virus Basics and Frequently Asked Questions

References

Apple Inc. About the security content of iPhone OS 3.1.3 and iPhone OS 3.1.3 for iPod Touch. 2010. Retrieved February 3, 2010 from http://support.apple.com/kb/HT4013.

Gary Allen. Exclusive look at Apple's new iPod touch-based EasyPay checkout. 2009. Retrieved Feburary 17, 2010 from http://www.appleinsider.com/articles/09/11/03/exclusive_look_at_apples_new_ipod_touch_based_easypay_checkout.html.

Bill Brenner. Proof-of-concepts heighten mobile malware fears. 2006. Retrieved February 17, 2010 from http://searchexchange.techtarget.com/news/article/0,,sid43_gci1171168,00.html.

Jesus Diaz. iPhone Can Now Serve Web Pages, Run Python, Open Source Apps. 2007. Retrieved February 13, 2010 from http://gizmodo.com/282139/iphone-can-now-serve-web-pages-run-python-open-source-apps.

Ken Dunham, et al. Mobile Malware Attacks and Defense. 2009. Burlington, MA: Syngress Publishing, Inc.

Philip Elmer-DeWitt. 40 staffers 2 reviews 8,500 iPhone apps per week. 2009. Retrieved February 23, 2010 from

http://brainstormtech.blogs.fortune.cnn.com/2009/08/21/40-staffers-2-reviews-8500-iphone-apps-per-week/.

Amy Feldman. Haiti Earthquake Provokes Wave of Text Donations. 2010. Retrieved February 13, 2010 from http://www.businessweek.com/investor/content/jan2010/pi20100114_236518.htm.

Flexispy Ltd. FlexiSpy Homepage. 2010. Retrieved February 17, 2010 from http://flexispy.com/.

F-Secure. Warning On Possible Android Mobile Trojans. 2010. Retrieved February 13, 2010 from http://www.f-secure.com/weblog/archives/00001852.html.

F-Secure. Worm:iPhoneOS/Ikee.B. 2009. Retrieved February 16, 2010 from http://www.f-secure.com/v-descs/worm_iphoneos_ikee_b.shtml.

Google Inc. Android Market Homepage. 2010. Retrieved February 23, 2010 from https://www.google.com/accounts/ServiceLogin?service=androiddeveloper.

GSM Association. Global Mobile Broadband Connections Increase Tenfold Over The Past Year. 2008. Retrieved February 4, 2010 from http://gsmworld.com/newsroom/press-releases/2008/870.htm.

Arik Hesseldahl. Apple's Schiller Defends iPhone App Approval Process. 2009. Retrieved February 13, 2010 from http://www.businessweek.com/technology/content/nov2009/tc20091120_354597.htm.

International Telecommunication Union. The World in 2009: ICT Facts and Figures. 2009. Retrieved February 3, 2010 from http://www.itu.int/ITU-D/ict/papers/2009/Europe_RPM_presentation.pdf.

John Leyden. Sign mobile malware prompts Symbian security review. 2009. Retrieved February 23, 2010 from http://www.theregister.co.uk/2009/07/23/sms_worm_analysis/.

Mike Melanson. Twitter Sees 347% Growth in Mobile Browser Access. 2010. Retrieved March 23, 2010 from

http://www.readwriteweb.com/archives/twitter_sees_347_growth_in_mobile_browser_access.php.

Microsoft Corporation. Windows phone Homepage. 2010. Retrieved February 23, 2010 from http://developer.windowsphone.com/Help.aspx?id=0e4efb7b-2e57-4ff5-b381-117281fc903b.

mStation Corporation. Mophie Homepage. 2010. Retrieved February 17, 2010 from http://www.mophie.com/product-p/1125_mp-ip3g-blk.htm.

Cyrus Peikari. Analyzing the Crossover Virus: The First PC to Windows Handheld Cross-infector. 2006. Retrieved February 17, 2010 from http://www.informit.com/articles/article.aspx?p=458169&seqNum=3.

Phil Porras, et al. An Analysis of the IKEE.B (DUH) iPhone Botnet. 2009. Retrieved February 3, 2010 from http://mtc.sri.com/iPhone/.

Dan Raywood. Google finds apparently fraudulent banking applications on its Andriod Marketplace. 2010. Retrieved February 1, 2010 from http://www.scmagazineuk.com/google-finds-apparently-fraudulent-banking-applications-on-its-android-marketplace/article/161047/.

Research in Motion Limited. Blackberry App World FAQ Homepage. 2010. Retrieved February 23, 2010 from http://na.blackberry.com/eng/developers/appworld/faq.jsp.

Anne Ruste Flo and Audun Josang. Consequences of Botnets Spreading to Mobile Devices. 2009. Retrieved February 2, 2010 from http://nordsec2009.unik.no/papers/RFJ2009-NordSec.pdf.

Square, Inc. Square Homepage. 2010. Retrieved February 17, 2010 from https://squareup.com/.

Symbian Foundation. Symbian Horizon FAQ Homepage. 2010. Retrieved February 23, 2010 from http://horizon.symbian.org/index.php?option=com_content&view=article&id=52.

Document FAQ

What is a TIP? A Technical Information Paper (TIP) is issued for a topic that is more informational in nature, describing an analysis technique, case study, or general cyber security issue. Depending on the topic, this product may be published to the public website.

If this document is labeled as UNCLASSIFIED//FOR OFFICIAL USE ONLY (U//FOUO), can I distribute it to other people? Per the U//FOUO warning, this document may be shared with personnel who have a valid "need to know" within your federal agency. With the case of a TIP, this is defined as a person or group that has a direct role in securing federal networks. If necessary, please contact US-CERT for clarification or specific distribution inquiries.

Can I edit this document to include additional information? This document is not to be edited, changed or modified in any way by recipients. All comments or questions related to this document should be directed to the US-CERT Security Operations Center at 1-888-282-0870 or soc@us-cert.gov.