3-2011

Perceived or Real Risks Using Smartphones

S. Ann Wilson
Nelson Rusche College of Business, Stephen F. Austin State University, wilsonsa@sfasu.edu

Michael York
Nelson Rusche College of Business, Stephen F Austin State University

PERCEIVED OR REAL RISKS USING SMARTPHONES

Ann Wilson, Stephen F. Austin State University
Michael York, Stephen F. Austin State University

Introduction

Smartphones have blurred the line of capability usually prescribed to traditional telephones by their becoming the premier multi-tasking devices of today's world. Since current smartphones have their own dedicated operating system, Bluetooth capabilities, constant network connection, PC connectivity, and internet capability, smartphones are experiencing security risks just as computer systems have done for many years. This paper will examine the history of mobile technology and its integration into people's daily lives. Furthermore, smartphone capabilities will be investigated for their potential vulnerabilities due to lack of consumers' precautions and smartphone usage.

Review of Literature

According to Tom Farley (2005), "by the late 1980s, the American wireless industry began searching for a higher capacity system" (p. 30). The frontrunner seemed to be a time based, or time division multiple access (TDMA), technology. This digital system became IS-54. CDMA, code division multiple access, appeared to enter the market too late to have any foundation in the industry, but that would all change in time.

IS-54 became the official digital standard for the cellular network for America in 1990. With IS-54 an operator could "convert any of its analog voice channels to digital. Customers got digital service where available and analog where it wasn't" (Farley, 2005, p. 31). Then in 1991, Pacific Telephone decided to invest in Qualcomm, the company that developed CDMA. The investment paid dividends; in 1993, CDMA was approved as an alternative digital standard, and was called IS-95. This system, too, used a two mode system, digital when possible and analog otherwise. Farley (2005) noted, "In 1996 NextWave PCS launched the first American [CDMA/] IS-95 system and the next ten years might well be called the Triumph of CDMA" (p. 32). At first glance, it appeared that this new network would help with the ability to make calls from anywhere; but as Bi, Zysmann & Menkes (2001) noted, "a more profound feature is the significant improvement of its data and multimedia capabilities" (p. 110).
It is through the growth and application of the CDMA and GSM systems that allows the smartphone to be practical today, and as Bi, et al. (2001) state, "it is interesting to observe that these seemingly simple ideas have since revolutionized wireless communications" (p. 110). Finally, in 1996, the advent of the smartphone made its appearance with the Nokia Communicator 9000, which "had a QWERTY keyboard and built in word processing and calendar programs. Besides sending and receiving faxes, the 9000 could check email and access the internet in a limited way" (Farley, 2005, p. 32). Due to the increased functionality and its ability to connect to the internet, the smartphone has become vulnerable to viruses. D. Shih, Lin, Chiang, and M. Shih (2008) note that "the first computer virus that attacks mobile phones is VBS.Timofonica which was found on May 30, 2000" (p. 479).

Since viruses have now invaded smartphones, the first precaution consumers can take is educating themselves in the areas that a virus can infect the phone. These areas include multimedia messaging system (MMS), Bluetooth, internet, syncing/docking, and peripherals. MMS messages are sent over the provider's cellular network, typically virus free, to exchange media files. However, Töyssys and Helenius (2006) note that, "malicious software can spread via MMS messages by attaching a copy of itself and sending it to some device capable of receiving MMS" (p. 111). Cheng, Wong, Yang, and Lu (2007) reaffirm this by pointing out that "the most well-known virus of such a kind is *CommWarrior*" (p. 259). *Cabir*, the first smartphone virus, spread via Bluetooth (Töyssys, 2006, p. 111). However, a weakness of spreading the virus by the means of Bluetooth is that it must be in discoverable mode, which often times out, and the user must accept and install the incoming file. Similar to computers, smartphone users have the risk of downloading a virus from the internet that is masquerading as a game or some other application the user may find enticing. Since current smartphones are nearly always connected to the internet, it only amplifies the seriousness of the issue because it allows the virus to be in constant communication with the host. The *Crossover* virus was spread through syncing, when, "smartphones are connected to a computer in order to synchronize calendar events and new contacts," notes Cheng et al. (2007, p.260). However, for this type of attack to succeed, the user's computer first must be infected. The final way a smartphone can be infected is through peripherals or removable media.

This research indicates that with several possible infection methods, an anti-virus program for a consumer's smartphone seems like a wise choice. However, the program has the challenge of working within the capabilities of the smartphone while not hogging too many resources or draining battery life. It is perhaps due to these current limitations and drawbacks, that more consumers don't have an anti-virus program installed on their smartphone.

Purpose

The purpose of this paper is to examine the increased availability and use of smartphones and consumers' experience with real or perceived vulnerabilities and lack of precautions that lead to an increase in vulnerabilities. This will be determined through a survey evaluating smartphone usage, awareness, and concern.

Design of the Study

Students, faculty, and alumni of a mid-size Texas public university were asked to complete an anonymous online questionnaire. The questions covered demographic information and primarily included a 1 – 5 rating scale for the questions, with 1 being low and 5 being high. The survey questions include:

1. Demographic information
2. Do you have a smartphone?
3. How many years have you had a smartphone?
4. What operating system does your current smartphone run?
5. Have you ever, to your knowledge, had private information stolen due to smartphone usage?
6. How concerned are you about having private information stolen from your smartphone?
7. Are you aware of any smartphone viruses?
8. Do you use an anti-virus program on your smartphone?
9. How concerned are you about getting a virus on your smartphone?
10. Do you download apps on your smartphone?
11. Do you read the User Agreement license for apps you download?
12. What is your smartphone primarily used for?

Findings

The total number of respondents completing the online survey was 120. In some isolated cases, answers were left blank. The results of the administered survey questionnaire are summarized as follows:

Gender

Male	95 (48.5%)
Female	101 (51.5%)

Age

Under 18	1 (0.5%)
18-22	110 (56.1%)
23-29	38 (19.4%)
30-45	29 (14.8%)
46 or older	18 (9.2%)

Have a Smartphone?

Yes	120 (61.5%)
No	75 (38.5%)

Years Owning Smartphone

< 1 Year	24 (19.4%)
1-2 Years	51 (41.1%)
2-5 Years	40 (32.3%)
> 5 Years	9 (7.3%)

OS on Smartphone

Android	28 (23.3%)
iPhone OS	56 (46.7%)
Palm OS	2 (1.7%)
Blackberry	21 (17.5%)
Symbian OS	0 (0.0%)
Windows	8 (6.7%)
Other	6 (5.0%)

Private Information Stolen from Smartphone?

Yes	1 (0.8%)
No	119 (99.2%)

Concern of Private Information Stolen from Smartphone?

Not at all	11 (9.2%)
Not very	39 (32.5%)
Neutral	21 (17.5%)
Somewhat	30 (25.0%)
Very	19 (15.8%)

Aware of Smartphone Viruses?

Yes	12 (10.2%)
No	106 (89.8%)

Use an Anti-virus Program on Smartphone?

Yes	18 (15.4%)
No	99 (84.6%)

Concern of Getting Virus on Smartphone?

Not at all	14 (11.9%)
Not very	37 (31.4%)
Neutral	27 (22.9%)
Somewhat	28 (23.7%)
Very	22 (10.2%)

Download Apps on your Smartphone?

Yes	94 (80.3%)
No	23 (19.7%)

How Often Do You Read the User Agreement License for Apps?

Never	47 (40.5%)
Rarely	37 (31.9%)
Sometimes	15 (12.9%)
Often	9 (7.8%)
Always	8 (6.9%)

What is Your Smartphone Primarily Used for?

Personal	62 (53.4%)
Business	1 (0.9%)
Both	53 (45.7%)

The following significant responses were found:

Gender Regarding Concern of Having Private Information Stolen:
There were 58 male respondents, of which 20 (34.4%) answered to be at least somewhat concerned of having private information stolen. There were 62 female respondents, of which 29 (46.8%) answered to be at least somewhat concerned of having private information stolen. Based upon these responses, females are 12.4% more likely to be concerned regarding private information being stolen from their smartphones.

Gender Regarding Awareness of Smartphone Viruses:
There were 57 male respondents, of which 8 (14.0%) answered yes to being aware of a smartphone virus. There were 61 female respondents, of which 4 (6.6%) answered yes to being aware of smartphone virus. Interestingly, despite twice as many males as females being aware of viruses, this doesn't seem to affect their concern of having information stolen, as shown in the previous comparison.

Operating System Regarding Concern of Getting a Virus:
There were 28 respondents that have the Android OS, of which 8 (28.5%) were either not very or not at all concerned. There were 56 Apple iOS respondents, of which 28 (51.9%) were either not very or not at all concerned. When asked for an explanation on their reasoning, several iOS users responded along the lines of "Apple is good about not [getting] any viruses," as summed from a respondent. This perception is perhaps a carry over from the Apple's marketing of Macs not getting viruses; a separate study would need to be conducted to confirm this suspicion.

Age Regarding Concern of Having Private Information Stolen:
There were 18 respondents in the 30-45 range, with 10 (55.6%) being at least somewhat concerned about having private information stolen from their smartphones. Compared to the average percentage of respondents with this age group removed, 32.8%, respondents within the 30-45 range are much more likely to be concerned of having private information stolen.

Summary of Results

Of 120 respondents, 1 (0.8%) was aware of having private information stolen from her smartphone. Based upon the survey responses, current concern of having private information stolen is unsupported and there is not a reason for concern at the present. However, as the functionality and the number of users grow in the future, so does the chance of smartphones becoming targets for viruses and data theft. At current, it is inconclusive regarding the concern and the chances of getting a virus on a smartphone. Presently, the risks associated with smartphones are almost nonexistent; however, the risks are perceived out of extreme caution and vulnerabilities that may become more exposed as smartphones become as ubiquitous as computers.

References

Bi, Q., Zysman, G.L., Menkes, H. (2001). Wireless mobile communications at the start of the 21st century. *Communications Magazine,* 39(1), 110-116. doi:10.1109/35.894384

Cheng, J., Wong, S., Yang, H., Lu, S. (2007, June). SmartSiren: Virus detection and alert for smartphone. The 5th International Conference on Mobile Systems, Applications, and Services, San Juan, Puerto Rico. doi:10.1145/1247660.1247690

Farley, T. (2005). Mobile telephone history. Telektronikk, 101(3), 22-34. Retrieved from http://www.cems.uwe.ac.uk/~rwilliam/CSA_course/mobile_phone_history.pdf

Shih D., Lin B., Chiang H., Shih M., (2008) Security aspects of mobile phone virus: a critical survey. *Industrial Management & Data Systems*, 108(4), 478-494.

Töyssy, S., Helenius, M. (2006). About malicious software in smartphones. *Journal in Computer Virology, 2*(2), 109-119. doi:10.1007/s11416-006-0022-0