Rootkits and What we Know:
Assessing US and Korean Knowledge and Perceptions

November 2006
Revised May 2007

***Kirk P. Arnett kpa1@msstate.edu**
Professor of Information Systems
Management and Information Systems
Mississippi State University
POB 9581, Mississippi State, MS 39762
(662)325-1999

Mark B. Schmidt mbschmidt@stcloudstate.edu
Associate Professor of Business Computer Information Systems
213 G.R. Herberger College of Business
St. Cloud State University
St. Cloud, MN 56301
(320) 308-4988

Allen C. Johnston ajohnston@uab.edu
Assistant Professor of Management Information Systems
1530 3rd Avenue South
University of Alabama Birmingham
Birmingham, AL 35294
(205)-934-8800

Jongki Kim jkkim1@pusan.ac.kr
Associate Professor of Management Information Systems
Division of Business Administration
College of Business
Pusan National University
Pusan, 609-735 Republic of Korea
+82-51-510-2582

HJ Hwang hjhwang@cu.ac.kr
Professor of MIS and Dean of External Relations & Cooperation
Catholic University of Daegu
+82-53-850-3007, 3428(office)

*** Corresponding author**

Rootkits and What We Know:
Assessing US and Korean Knowledge and Perceptions

ABSTRACT

Respondents from eight Korean and U.S. higher education institutions were surveyed as to their knowledge and experience with various forms of computer malware. The surveys provide insight into knowledge of rootkits that have become coffee lounge discussion following the once secretive Sony rootkit news break in late 2005 and then the rash of accusations and acknowledgements of other rootkits that followed. The surveys provide an empirical assessment of perceptions between students in the two countries with regard to various forms of malware.

The two groups are similar in many respects but they exhibit significant differences in self-reported perceptions of rootkit familiarity. U.S. respondents report higher levels of familiarity for all assessed malware types, including the fictional "Trilobyte" virus. A timeline-based comparison between virus and rootkit knowledge reveals that relatively little is known about rootkits today. This highlights dangers related to existing knowledge levels but presents hope for solutions and an accelerated rootkit awareness curve to improve worldwide malware protection.

Keywords
Rootkit, virus, spyware, malware, cross-culture

INTRODUCTION

Korea and the U.S., along with the rest of the Internet enabled world, continually battle a growing number of computer attacks. The source of these attacks may be domestic or foreign. The attacks may be from government or terrorist sponsored organizations for intelligence gathering or they may be from criminal groups or individuals intent on financial gains. The attacks may be against personal, business, education, or governmental computer assets. Regardless of the source or target, each country must prepare for current attacks as well as attacks that will surely occur in the future. For maximum effect, the preparation must be to protect personal, business, and governmental assets, and the preparation must span the globe.

Countries around the globe need skilled persons to battle against attacks, and these countries certainly have attackers who are on the opposite side of the battle field. Each country houses hackers who create malware and each country trains computer hackers for offensive as well as defensive cyber attacks. Despite its lack of sophisticated digital infrastructure, North Korea has attacked both South Korean and U.S. governmental computer installations. The capabilities of graduates from Kim il Sung's North Korean hacker training academy, where students undergo five years of specialty courses for hacking careers, are said to be comparable to the best U.S. CIA trained hackers (Digital, 2005).

During this decade, U.S. Soldiers have been indicted for breaking into South Korean computer systems (Stars, 2001). We don't know whether or not this was government sponsored, but we do know that attacks are not only one-to-many or many-to-one events. Rather, cyber attacks are characterized as events in which many sources are involved in attacking many targets. South Korea's Ministry of National Defense said a five percent budget increase was allocated mainly for projects such as "the buildup of the core capability needed for coping with advanced scientific and information warfare." The report also revealed that South Korea's military has 177 computer training facilities and had trained more than 200,000 "information technicians" (Kramarento, 2003). Training efforts such as these are a necessary strategy for any country that is a part of today's malware infested landscape.

A relatively new form of malware is a rootkit. Although well known in the Unix arena, rootkits are now rapidly expanding in Windows environments. Even the newest software developments may not be immune to rootkits as Polish security researcher Joanna Rutkowska demonstrated blue pill – a proof of concept rootkit to circumvent pre-release Microsoft Vista security. A rootkit is a piece of software that allows its user to gain top level (root) privileges where the rootkit is installed. A rootkit is not a virus or a worm but it may deliver a virus or worm. Once installed, if a backdoor mechanism is made available to the attacker, the rootkit will allow the attacker to "own" the machine. Co-author of the now famous rootkit.com website, Jamie Butler, says that it is this stealth nature of a rootkit that is the real danger as a "rootkit is software used to hide other software from the user and security tools, to evade detection" (Williamson, 2007). The result is, because they are unknown, rootkit infections may last longer and therefore do more damage for longer periods than could a single worm or virus.

Our belief is that rootkit threat levels are not understood and our purpose is to describe the findings from a cross-cultural study. The research goal is to assess the knowledge levels and perceptions of Korean and U.S. college students regarding rootkits and more traditional malware with an eye toward identifying possible problems or solutions that might surface. The organization is to first examine selected relevant literature regarding Korea and the U.S. in today's digital world. Rootkits are then examined as to their current status and potential threat level. The study methodology is briefly described and the data comparisons are presented and discussed. Finally, the limitations that should be considered in interpreting the results are suggested and courses of action for these and other countries are recommended.

RELEVANT LITERATURE

F-Secure reports the Winevar e-mail worm was found in-the-wild in Korea at the end of November 2002 (Hulme, 2002). Apparently it was intentionally released by the virus writer during South Korea's Anti-Virus Researcher's Asian conference. The Korean born W32/Buchon@mm mass mailer also delivers a keylogger. The Slammer virus that affected Windows machines running SQL Server was especially destructive in Korea, resulting in a massive DoS attack. At its time, the Code Red Worm, which was originally designed to attack White House computers (Lemos, 2001), infected at least 225,000

computers elsewhere and shut down Internet services in Korea for several hours in 2001. Korea and the U.S. have well known security firms to combat malware, they each have virus writers who release viruses in the wild, and they engage in training attackers and defenders for cyber warfare.

Korea is deemed to be more risk averse than the U.S. An evaluation of software risks by (Peterson and Kim 2003) found there were few differences between the U.S. and Japan, yet a number of differences were found between the U.S. and Korea. Specifically, a lack of experienced IS development personnel was perceived to be a greater risk factor in Korea than in the U.S. This difference adds some weight to Hofstede's five cultural differences studies among more than 50 countries (ITIM 2006). Although Hofstede's findings have been questioned, they are based on a large and broad-based data source on country cultural differences. Hofstede measured Korea's dimension of uncertainty avoidance index (or UAI) as its highest dimension at 85; whereas, the U.S. UAI is relatively quite low at 46. This substantial difference indicates that individuals in South Korea would be more likely to be subject to and to accept tight rules and controls than would U.S. people who, according to the index, would have fewer rules and controls and would have a greater level of tolerance for variety. These two studies indicate that differences might be expected in terms of student perceptions of the extent of and potential for malware damage.

As this research examines perceptions and understanding from participants in two countries, cultural values that might affect participant learning and perceptions are relevant. Koreans have high educational achievements; so a natural query is to determine the factors that lead to these high achievements. Kim and Park (2006) outline limitations of prior studies that emphasize biological bases and educational structural features to explain high educational achievements among Koreans noting that, despite prior assumptions with regard to Korean education limitations, anomalies exist as Korean students "outperform their Western counterparts in reading, mathematics, and sciences" (p.287).

Their explanation employs an indigenous psychological approach. With this approach they find that Koreans 1) view education as a part of self cultivation which is a way to achieve personal, social, and occupational success, 2) believe ability is acquired through persistent effort and discipline, and 3) consider that parental influence, which occurs for life, is essential for success. Along with other findings, a cultural difference is that there is no self-serving bias – Koreans believe that success is due to effort and failure is due to lack of effort and ability (Kim and Park 2006). Based on these findings, it is expected that knowledge or understanding of the rootkit phenomenon might be stronger for Koreans because of their efforts to learn about rootkit malware and to increase their depth of knowledge about malware in general. This would be aligned with learning and acquiring knowledge.

Calhoun, Teng, and Cheoan (2002) note that cultural values are often designed into technologies, but they are not always accepted in the receiving society because of cultural differences. Specifically EIS and GDSS provide examples of this rejection. Their

findings from survey data regarding perceptions of technology use in decision making behavior indicates that some behaviors change while others do not. Yet, it is well known the Koreans are world leaders in egames, which is an indication of higher skills and knowledge of at least some computer skills in decision-type games. This expertise and familiarity should lead to more exposure to and/or better understanding of computer malware.

Today's always on connections and wireless capabilities have increased vulnerabilities for computer and Internet users. An empirical study for a model of hacking identified a positive correlation between broadband capacity and cyber attacks (Bento and Bento 2004). This positive correlation is prevalent in high broadband use countries such as the U.S. and Korea. However, in terms of wireless technologies, South Korea has taken a lead. Also, a study of cellular technologies by Shim (2005) found that South Korea was a test bed for hi-tech cellular technologies. Korean mobile carriers had planned to roll-out the world's first handset-based satellite digital multimedia broadcasting (DMB) services via cellular phones. Shim also suggests that a young generation of cellular phone users in Japan and Korea associate the use of modern cellular phones with their social status (Shim 2005).

Korea and the U.S. share common ground with regard to Internet usage. For instance, according to (Internet World 2005) there is a 67.0% penetration of Internet users in South Korea and a 68.1% penetration in the U.S. Both countries have roughly the same extent of, but rapidly expanding, broadband usage so they both have large numbers of "always-on" Internet connections that can be compromised. Indeed, computer viruses are strong in Korea as "the country boasts the world's highest per-capita Internet penetration with about 12 million of the total 15.5 million households hooked up to the always-on Internet" (Korean 2005).

The similarities and differences between the two countries and others should be explored in today's malware threat environment. Such studies have been made in the past for computer viruses, but none have been published to examine more modern threats such as rootkits in these countries. Previously cited studies indicate that the knowledge of the rootkit threat might be expected to be greater in Korea than in the U.S. because of users who would be more "high tech" and technology/Internet savvy (Calhoun et al. 2002; Shim, 2005; Korean 2005) and who place high importance on learning (Kim and Park 2006). Rootkits have gained increased attention following the late 2005 revelation that Sony had installed rootkit software to monitor usage of their CDs. As such, it is reasonable to question what college students, who will be the business leaders of tomorrow, know about rootkits. This assessment should not be isolated to one, or even a few countries, as today's malware is frequently worldwide, gives zero day warnings, and spreads in minutes.

ROOTKITS: STATUS AND POTENTIAL

A 2006 eWeek.com article entitled "When's a Rootkit Not a Rootkit? In Search of Definitions," describes a vendor-neutral movement to find an unambiguous way to

describe rootkits (Naraine, 2006). Rootkits were once almost exclusively associated with Unix-based hosts. Now they are gaining the attention of Windows users across the globe. Sony's use of rootkits on CDs has no doubt greatly added to this attention. But, even before Sony's debacle, rootkits were growing in the Windows world as Roberts (2005) warned in "Microsoft on Rootkits: Be afraid, be very afraid!" Further, Roberts' article is far from a lonely voice, as Seltzer (2005) predicts that this trend to focus on Windows based machines will continue in the foreseeable future.

A Rootkit is software that is designed to hide files, processes, or registry data, most often in an attempt to mask intrusion and to surreptitiously gain administrative rights to a computer system. When used in this malicious manner, rootkits can provide the mechanism by which various forms of malware, including viruses, spyware, and Trojans, attempt to hide themselves. Rootkits are not worms or viruses, but they can be delivered by worms and viruses. Moreover, rootkits can be extremely difficult to detect and remove. As described by Dillard (2005) rootkits target the extensible nature of operating systems, applying the same principles for value added application development as found in legitimate software.

In May of 2007, Johanna Rutkowska announced with a colleague her plans to open a new firm, ***Invisible Things Lab***, obviously tailored from the rootkit moniker, and also to present previously unreleased code, techniques, and ideas at a Black Hat Briefings conference later in the year (Naraine, 2007). Also Symantec announced a merger with storage software vendor Veritas which, according to analysts, will enhance Symantec's rootkit detection capabilities because of Veritas' strength in deep raw disk scans, which are said to be one of the ways to uncover rootkits which traditional malware prevention techniques are missing. Yet rootkits are here. They are often hidden, and the authors who hide them are currently ahead of the defenders. This malware is exceedingly dangerous and will likely plague users for some time to come.

As rootkits become more prevalent, they are becoming a part of today's blended malware. Within the modern computer security paradigm, rootkits represent an under-reported, under-estimated threat to computer security. Their newness, stealth nature, and potential to lead to complete system compromise make them extremely dangerous. We need to learn more about rootkits, and this knowledge needs to quickly saturate a critical mass of users. An appropriate starting point is to gauge what college students know and believe about rootkits today.

METHODOLOGY AND MEASUREMENTS

To measure knowledge and perceptions we conducted student surveys which resulted in the accumulation of 199 surveys from five higher education institutions in Korea and 210 surveys from three institutions in the US. More than 80% of respondents from each group are full time college students, and as would be expected, the large majority of respondents from both countries are between 18 and 29 years of age. The survey instrument was first used in 1993 in *Computers and Security* (Jones et al. 1993) to gauge

user knowledge of computer viruses and then in 2005 *Communications of the ACM* (Schmidt and Arnett 2005) to report user knowledge of spyware.

The U.S. survey respondents are predominantly male (57%), with more than five years of computer experience (74.3%). For Korea, the respondents are almost evenly divided in gender and 88.1% of them have more than 5 years of computer experience. Not only are both groups well experienced with computers, most individuals own one or more computers (U.S. 93.8%, Korea 91.6%). Table 1 presents details of selected respondent demographics.

Table 1. Selected Profile of Respondents

	Response category	U.S. respondents	Korean respondents
Age	18 to 29	82.6%	95.5%
	30 to 39	8.0%	4.5%
	40 to 49	8.5%	0%
	50 to 59	1.0%	0%
	60 and over	0%	0%
Gender	Female	42.4%	50.7%
	Male	57.6%	49.3%
Computer experience	< 1 year	2.5%	.5%
	1 to 2 years	2.5%	0%
	2 to 5 years	20.6%	11.3%
	5 to 10 years	45.2%	51.2%
	> 10 years	29.1%	36.9%
Occupation	Full time student	81.5%	96.0%
	Part time student	7.3%	2.0%
	IT professional	6.8%	2.0%
	Other	4.4%	0%
How many personal computers (or laptops) do you own?	0	6.2%	8.4%
	1	47.1%	60.1%
	2	31.4%	24.6%
	3	7.1%	5.9%
	4 or more	8.1%	1.0%

The number of individuals who have heard of rootkits, and at least have an awareness of them, should be a measure of baseline knowledge. Responses indicate that only 16.2% of U.S. students and 10.4 % of Korean students have even *heard* of rootkits. Further, large percentages of the respondents have known of rootkits for less than one year (U.S. 82.1%, Korea 93.9%). These figures are alarming when compared to these individuals'

knowledge of computer viruses where in contrast, 77.2% of U.S. respondents and 69.5% of Korean respondents have known of viruses for five or more years. One surprise shown in Table 2 below is the difference between the percentages of respondents who know about spyware. Only (9.3%) of Korean users have known about spyware for more than three years while 28.% of U.S. respondents indicate that they have known about spyware for more than three years.. These findings indicate the newness of rootkits within the Microsoft Windows user domain.

The survey included five-point Likert scale responses (1 = Strongly Disagree, 3 = Neutral, 5 = Strongly Agree) for the research items to facilitate self-reported measures of perceptions among both U.S. and Korean survey respondents. These perceptions can be examined to determine differences between the two countries. As Figure 1 illustrates, regardless of country of origin, students report more knowledge of viruses (3.04) and spyware (3.15) than of rootkits (1.30). Also, students of both countries share similar perceptions of the knowledge possessed by their peers; believing them to know more about spyware and viruses than they do about rootkits (see Figure 2).

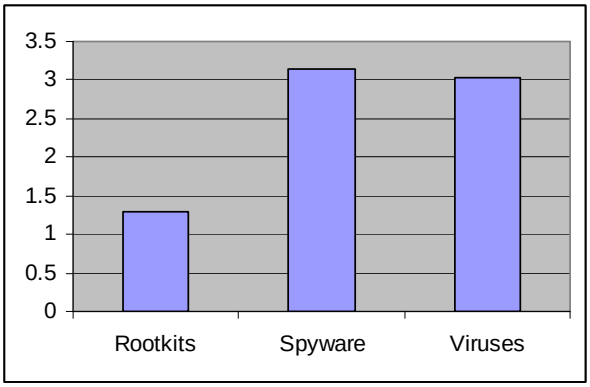

Figure 1. Relative Familiarity of Malware Types

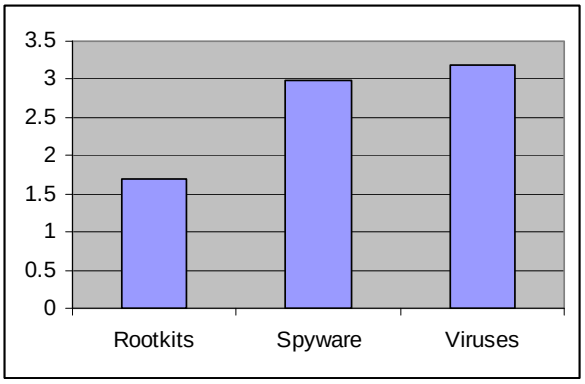

Figure 2. Perceptions of Peers' Familiarity of Malware Types

A comparison of responses provided by U.S. and Korean students suggests that there are significant differences in how the two student groups report their familiarity of rootkits, spyware, and viruses in general. For example, U.S. students report higher levels of familiarity with all three forms of malware than their Korean counterparts. As depicted in Table 2, this differential in perceptions is consistent for all forms of malware, and is significant for all variables ($p < 0.01$). Appendix 1 presents the ANOVA calculations. Included in the analysis is a fictitious threat, "Trilobyte," which was introduced to the study simply as a means for ascertaining the quality of the survey responses. U.S. students report higher levels of familiarity than Korean students with the "Trilobyte" virus, although neither group reports more than low to moderate familiarity. Interestingly, both groups believe their familiarity of the "Trilobyte" virus to be greater than that of rootkits. Also included in Table 2, perceptions of familiarity with the very real "Melissa" virus were different among the student groups, with U.S. students again reporting a higher level of familiarity.

Table 2. Comparison of U.S. and Korean Responses

Survey Question	U.S. Mean	Korea Mean
I am familiar with how rootkits work	1.44	1.15
I am familiar with spyware	4.13	2.10
I am familiar with computer viruses	4.21	1.78
I am familiar with the "Trilobyte" virus	1.95	1.40
I am familiar with the "Melissa" virus	2.79	1.70

Interpretation:
U.S. respondents report a higher level of rootkit awareness. While both groups report low perceptions of familiarity of how rootkits work, U.S. respondents report relatively higher levels. The reports of low familiarity may be indicative of limited exposure to the threat because of its newness and the stealth characteristics. It is expected that this level of familiarity will increase over the next few years as rootkits become more prevalent.

Similar to rootkit familiarity, U.S. respondents report relatively higher levels of spyware familiarity than their Korean counterparts. However, for spyware, the difference in reported levels of familiarity is much greater, with U.S. respondents reporting themselves as familiar and Korean respondents reporting themselves as unfamiliar. Factors that might contribute to this difference are increased interest in personal information theft by both hackers and owners of the information, particularly in the U.S. In effect the U.S. college student represents the low hanging, but valuable fruit of personal information.

The difference in familiarity between U.S. and Korean respondents is greatest for the general threat of computer viruses. This is somewhat surprising given the maturity of the threat because it seems that all college students should have had substantial exposure and mitigation information. This could be the result of widespread penetration of vulnerable Windows client machines in the U.S.

With regard to the trilobite virus, which is imaginary, U.S. respondents report relatively higher levels of familiarity than the Korean students. Because the virus in question is non-existent, it might be that Korean students want to be more certain, and thereby precise, in their answers because of educational cultural differences. Here, we speculate that U.S. students feel less constrained to be exact and thereby more willing to guess, even if the guess is mistaken. This is consistent with previous findings that Koreans are more risk averse and have very high levels of uncertainty avoidance relative to the U.S.

For the widely successful Melissa virus, it is somewhat discouraging that neither group of students report even moderately high levels of familiarity. As with the other forms of malware, U.S. students report a higher degree of familiarity. Perhaps this is due to the origin of the virus.

ISSUES, CONCLUSIONS AND LIMITATIONS

This section presents the issues that arise in view of the findings of study. The conclusions and limitations are highlighted as well.

Issues:

The limited awareness and knowledge of rootkits in both countries is especially alarming considering the recent "call to arms" against spyware and other forms of malicious malware. The *Communications of the ACM* recently devoted a special edition to the emergence and proliferation of the threat of spyware (Stafford 2005). However, within these articles no mention was made as to the presence of rootkit technology or new forms of blended threat. To solve this problem of limited awareness, proactive response must surface. What must occur next is a global intelligence and preparedness ramp-up by the IT community consistent with that which is occurring in the fight against spyware. Certainly, we are on the brink of another battle for control of personal computers and this battle is not restricted to certain geographic areas or countries.

The signature of a rootkit is to conceal its presence and activities. Consequently, anti-virus applications are often ineffective in that they cannot detect what they cannot see. Additionally, the manner in which rootkits are installed on systems further complicates their detection by traditional anti-malware software. Rootkits are often installed through

tactics such as social engineering or through exploits of operating system vulnerabilities. Traditional symptoms of malware infestation, such as replication activities, are simply absent from rootkit manifestations. Conventional malware detection mechanisms such as anti-virus and anti-spyware software are now firmly established in the security practices of IT management; however, they must be revisited as to their ability to address rootkit exploits.

Conclusions:

With the emergence of these blended threats, computer security managers must take actions above and beyond traditional anti-malware techniques and employ methods consistent with the requirements of advanced rootkit detection and removal. These actions must be taken everywhere. If one country's set of computers remain unprotected, their vulnerabilities will surely be compromised and used in the ever growing army of botnets against others. Partial protection among countries parallels locking the back door of your home and leaving the front door unlocked – the vulnerability still exists although it may not be as widespread.

Computer security measures such as network firewalls, email scanning, anti-malware utilities, intrusion detection applications, and intrusion prevention applications are synonymous with a holistic approach to IT security and should be regarded as a necessary first line of defense against rootkit infestation. Additionally, patches must be made available in a timely fashion. Attackers have the upper hand in exploiting vulnerabilities and their activities will likely dictate when patches should be developed and released to users. This is evidenced by the occasional Microsoft vulnerabilities where public pressure, and quick-fix patches created by other vendors, force Microsoft to issue patches before the scheduled "Patch Tuesday" release date. To successfully encourage the international user community to patch as needed, there must first be basic awareness and knowledge concerning the vulnerability. The user community should have basic awareness and knowledge of rootkits because of their damage potential and increasing movement into Windows computing environments.

Beyond the ramp-up of the IT community education efforts must be initiated, but these efforts must be widespread and tailored to the audience in order to combat the problem. Education will be needed for diverse groups such as lawmakers, consumers, home users, and IT professionals; and members of these groups will sometime overlap. Lawmakers are not traditional recipients of these education efforts but they should be included because of the international reach of malware and because of the scarcity of legal treaties that are intended to be global. Security vendors will need cooperative efforts, which are now only being seen in small numbers by current acquisitions and mergers, to strengthen their security offerings. Rootkits are not detected by traditional signature-based detection methods that are common now, and combined efforts that extend the time-tested detection methods may be used to improve software-driven combative efforts where client consumers and IT professionals each receive benefits. Corporate policy makers must be vigilant in their protection efforts. First they must gain awareness of the capabilities and characteristics of the anti-rootkit solutions. When appropriate solutions

or preventative tasks are promulgated by policy, they must be enforced and penalties must occur when these codified solutions and tasks are violated.

Limitations:
We believe this study presents a fair assessment of what college students in the two countries perceive concerning rootkits. The convenience samples were chosen by the authors, based on geographic proximity, and it could be argued that the findings are not generalizable to Korea and the U.S. as a whole. Also, the survey respondents are relatively young and most of them are full time college students who are not a part of the workplace where rootkits will surely cause business losses. However, these students are certainly experienced with computers and they indicate that they have access to one or more owned personal computers. It is further expected that they have a high level of skill in Internet surfing and digital downloads based on profiles of college students in other contexts. So, although this study is not without limitations, its currency and cross-country orientation should be valuable to those involved in training and/or education in the private or public sector. Furthermore, the results may serve as a baseline for researchers and security firms who examine awareness levels.

REFERENCES

Bento, Al and Bento, Regina. (2004) "Empirical Test of Hacking Framework: An Exploratory Study." *Communications of the AIS,* Volume 14: 678-690.

Calhoun, KJ, Teng, James TC, and Cheon, Myun J. (2002). Impact of National Culture on Information Technology Usage Behavior: An Exploratory Study of Decision Making in Korea and the USA. *Behavior and Information Technology, (21.4),* July/August 2002, 293-302.

Digital Chosunilbo. (2005). "N. Korea's Hackers Rival CIA, Expert Warns." http://english.chosun.com/w21data/html/news/200506/200506020014.html

Dillard, K. (2005). "What is a rootkit?" from *SearchWindowsSecurity.com*

Hulme, George V. (2002). "Rude Worm Insults, then Wreaks Havoc." http://www.itnews.com.au/newsstory.aspx?CIaNID=10532

Internet World Stats (2005). http://www.internetworldstats.com/stats.htm

ITIM International (2006). http://www.geert-hofstede.com/

Jones, MC., Arnett, KP., Tang, JTE., & Chen, NS. (1993). Perceptions of computer viruses a cross-cultural assessment. *Computers and Security, 12,* 191-197.

Kim, Uichol and Park, Young Shin (2006). "Indigenous psychological analysis of academic achievement in Korea: The influence of self efficacy, parents, and culture." *International Journal of Psychology, 41(4)* 287-292.

Korean Times (2005) Technology. “It’s English.” *The Korean Times* (2005) http://times.hankooki.com/lpage/tech/200512/kt2005120216444111780.htm

Kramarenko, Dmitri. (2003, January 25) “Hackers or Cyber-soldiers?” *Computer Crime Research Center*. http://www.crime-research.org/interviews/hacker0904/

Lemos, Robert. (2001) “Web Worm Targets White House.” *CNet News.com*

Naraine, Ryan (2006, January 18) eWeek.com “When’s a Rootkit Not a Rootkit? http://www.eweek.com/article2/0,1759,1913083,00.asp

Naraine, Ryan. (2007, May 15) “Rutkowska Announces Invisible Things Lab Startup.”*ZDNet,* http://blogs.zdnet.com/security/?p=199.

Peterson, Dane K. and Kim, Chung. (2003). “Perceptions on IS Risks and Failure Types: A Comparison of Designers from the United States, Japan and Korea.” *Journal of Global Information Management*. Jul-Sep 2003, Vol. 11 Issue 3, p19, 20p.

Roberts, P. F. (2005). “Microsoft on 'Rootkits': Be Afraid, Be very Afraid.” http://www.computerworld.com/securitytopics/security/story/0,10801,99843,00.html

Schmidt, M. B., & Arnett, K. P. (2005). Spyware: A Little Knowledge is a Wonderful Thing. *Communications of the ACM, 48*(8), 67-70.

Seltzer, L. (2005). Rootkits: The Ultimate Stealth Attack. *PC Magazine, 24,* 76.

Shim, JP. (2005) “Korea’s Lead in Mobile Cellular and DMB Phone Services.”, *Communications of the Association for Information Systems*. Vol. 15.

Stafford, T. F. (2005). Spyware. *Communications of the ACM, 48*(8), 34-35.

Stars and Stripes (2001, July 27), “S. Korea Indicts U.S. Service Member for Allegedly Hacking more than 50 Web Sites.” http://ww2.pstripes.osd.mil/01/jul01/ed072701g.html

Williamson, Matt. (2007). “A Conversation with Jamie Butler.” *ACM Queue*, February 2007. 16-23.

Appendix 1.

ANOVA results. Respondents provided answers on Likert scale with 1 "Strongly Disagree," 3 "Neutral," and 5 "Strongly Agree."

	N	Mean		Sum of Squares	df	Mean Square	F	Sig.
I am familiar with how rootkits work								
USA	209	1.44	Between Groups	9.13	1	9.1285	14.4552	**0.000**
Korea	199	1.15	Within Groups	256.39	406	0.6315		
Total	408	1.30	Total	265.52	407			
The "average" person at my institution is familiar with rootkits								
USA	210	1.94	Between Groups	25.61	1	25.6101	36.3942	**0.000**
Korea	199	1.44	Within Groups	286.40	407	0.7037		
Total	409	1.70	Total	312.01	408			
I am familiar with spyware								
USA	210	4.13	Between Groups	418.45	1	418.4463	357.6413	**0.000**
Korea	196	2.10	Within Groups	472.69	404	1.1700		
Total	406	3.15	Total	891.13	405			
The "average" person at my institution is familiar with spyware								
USA	210	3.85	Between Groups	331.75	1	331.7464	369.2223	**0.000**
Korea	195	2.04	Within Groups	362.10	403	0.8985		
Total	405	2.98	Total	693.84	404			
I am familiar with computer viruses								
USA	210	4.21	Between Groups	602.97	1	602.9662	841.5044	**0.000**
Korea	196	1.78	Within Groups	289.48	404	0.7165		
Total	406	3.04	Total	892.45	405			
The "average" person at my institution is familiar with computer viruses								
USA	210	4.12	Between Groups	381.74	1	381.7385	460.6763	**0.000**
Korea	196	2.18	Within Groups	334.77	404	0.8286		
Total	406	3.18	Total	716.51	405			
I am familiar with the "Trilobyte" virus								

USA	208	1.95	Between Groups	30.56	1	30.5612	34.1501	**0.000**
Korea	191	1.40	Within Groups	355.28	397	0.8949		
Total	399	1.69	Total	385.84	398			

The "average" person at my institution is familiar with the "Trilobyte" virus

USA	209	2.31	Between Groups	50.96	1	50.9615	62.1123	**0.000**
Korea	191	1.59	Within Groups	326.55	398	0.8205		
Total	400	1.97	Total	377.51	399			

I am familiar with the "Melissa" virus

USA	210	2.79	Between Groups	116.46	1	116.4585	112.5560	**0.000**
Korea	189	1.70	Within Groups	410.76	397	1.0347		
Total	399	2.27	Total	527.22	398			

The "average" person at my institution is familiar with the "Melissa" virus

USA	210	3.78	Between Groups	54.35	1	54.3472	33.8593	**0.000**
Korea	189	3.04	Within Groups	637.22	397	1.6051		
Total	399	3.43	Total	691.57	398			