By Mark B. Schmidt *and* Kirk P. Arnett

SPYWARE: A Little Knowledge is a Wonderful Thing

With the increased dependence on networks and the near ubiquitous availability of the Internet, there is a new paradigm in place for the proliferation of spyware, viruses, and other malware. In fact, much attention has been given to spyware in popular literature with reports from multiple sources indicating that spyware has perhaps reached 90% home user PCs [2].

There is reason to believe this penetration is also high for PCs used in business, government, and academia. This broad reach is not only disturbing, but also perplexing as spyware is relatively new and the knowledge of spyware has been reported in the *Wall Street Journal, PC Magazine,*

ComputerWorld, and many other media sources in the last few years. Hence, we have a 90% infection rate from a relatively new type of malware, and far too little is known about this threat.

Spyware's reach is deep. Indeed, *InfoWorld* columnist Wayne Rash reported his teenage daughter's home-based computer slowed after being invaded by more than 1,400 uninvited programs. Rash also noted similar problems with his boss's office computer [5]. To stop, or at least substantially reduce, spyware's threat to private and efficient computing several protections must come into place. Software vendors, who have already made a great start, must provide low-cost and uncomplicated tools for spyware detection and removal; and they must continuously update those tools. Their diligence will be tested by the purveyors of spyware. Both home and office users must be better educated as to the prevention and elimination of this nuisance, and they must help their lesser-prepared colleagues.

Finally, pressure must be placed on the creators of spyware to ensure they maintain a sense of fairness and are more forthcoming in informing potential computer users of what their particular breed of spyware can and will do, and the conditions under which this may happen. Although some legislative efforts are under way and will certainly continue, legislation, without the three antecedents noted here, will not solve the problem. Stafford and Urbaczewski note that "laws and regulations are rudimentary and little progress is being made" [6]. Society has struggled for some time with efforts to legislate good citizenship to all computer users.

Brief Historical Perspective

According to CNET, the term spyware, as it relates to computers, first appeared Oct. 16, 1995 in a Usenet post poking fun at Microsoft's business model [9]. Zone Alarm Labs reportedly used the term in 1999 regarding their firewall product. Steve Gibson is credited with creating the first anti-spyware program, OptOut, in 2000. Regardless of the source, they all allow a conclusion that spyware is relatively new. *ComputerWorld's* first report of spyware in January 2001 relates a story of a computer gamemaker (EGames) agreeing with the Michigan Attorney General's office to remove third-party software that caused unsolicited ads to be sent to game owners [8]. By June of that year "spyware" appeared in a *PC Magazine* headline. Clearly, spyware represents a relatively new phenomenon for many computer users.

The first virus "in the wild" is reportedly the 1986 Brain virus released by two Pakistani brothers. As the story goes, the brothers analyzed the boot sector of a floppy disk and developed a method of infecting it. The virus was then spread in popular MS-DOS systems by the classic sneaker net method where copying and sharing data and programs from floppy disks was accomplished by walking from one computer to the other. The Brain virus was predated by Cohen's (1984) experiments, but Cohen's virus was not released to the public [3]. At any rate, we can mark the mid-1980s as a beginning for computer viruses.

	Perception of Self	Perception of Others	Interpretation
Frequently update anti-virus.	4.23	3.00	One update more than others.
Malware can be obtained by sharing disks.	5.00	4.03	Others are less likely to think that malware can be obtained by disk sharing.
Malware can be obtained by email.	5.49	4.65	Others are less likely to think that malware can be obtained via email.
Malware can be obtained via the Internet.	5.50	4.62	Others are less likely to think that malware can be obtained via the Internet.
Viruses are difficult to detect.	3.58	4.26	Others think it is more difficult to detect viruses.
Viruses are difficult to remove.	3.83	4.47	Others think it is more difficult to remove viruses.
Spyware is difficult to detect.	3.52	4.39	Others think it is more difficult to detect spyware.
Spyware is difficult to remove.	3.66	4.44	Others think it is more difficult to remove spyware.

T-tests of respondent perceptions—self versus others.

Measuring User Perceptions Of Spyware

We believe that a measure of computer user knowledge relative to spyware is important. To accomplish this, we found and then slightly modified a survey reported in *Computers and Security* in 1993 [4] used to measure computer user knowledge regarding computer viruses. The historical perspectives noted here tell us that spyware is roughly four years old, while computer viruses were approximately 10 years old when the 1993 survey was conducted.

However, we found today's students far more knowledgeable of malware than were their 1993 counterparts. For instance, 6% of the college students surveyed had been aware of the recent spyware phenomenon for less that a year and all of them reported an awareness of computer viruses for more than two years. In contrast, the 1993 study revealed that 18.4% of the students had known about computer viruses for less than one year, yet viruses (at the time) had

existed for at least a decade. So, knowledge of malware has increased markedly over the past 10 years, yet we conclude there remains a long path to raise awareness for everyone.

The survey respondents consisted of 150 upper-division college students, who were selected from six different classes taught by six different instructors. Approximately 60% were male and almost 30% were MIS or CS majors and are referred to here as technology-aware respondents. Almost 95% of these students had been using computers more than six years.

Surprisingly, although 94% of the 150 respondents indicated they knew about spyware for at least a year and 63% for two or more years, only 61% had found spyware. This percentage of spyware discoveries seems low and indeed contradicts a study reported by the Associated Press and ABC News in 2004.

The study found that 77% of the respondents reported their home computers were safe, yet when home visits and inspections took place, 80% of the computers had spyware [1]. A possible explanation is that our respondents do not personally own computers but rather use computers provided in public access locations or are owned by friends.

A majority (61%) of respondents indicated they have detected the presence of spyware on their computers. When asked to describe the damage done by spyware, many indicated that it "slowed down" the system. Some specific comments offered by respondents include:

- Spyware was tracking Web sites and giving email address book out;
- Hijacked Web page, password stealers running in background;
- Slowing programs, shutting down computer, interfering with Internet;
- Prevented me from opening Internet Explorer;
- Certain programs wouldn't open;
- Caused Internet Explorer to not function correctly; and
- After removing the spyware, Internet Explorer would not access Web pages.

These comments indicate the respondents were knowledgeable regarding the nefarious effects of spyware without necessarily knowing the specifics of how spyware is obtained or prevented, although it is clear from discussions that some of them were well aware of which spyware had specific effects and of what types of Internet downloads might be ill advised.

The comparisons reported here show that technology-aware respondents are different in terms of both knowledge and perceptions of the implications of spyware. In addition, they show it is the respondent's peer group (someone else), not the respondent, that requires more knowledge.

Prevention, detection, and remediation efforts **WILL PLAY A PIVOTAL ROLE IN SAFE AND SECURE COMPUTING** *in the foreseeable future.*

The accompanying table shows t-tests comparisons (all the t-tests indicated highly significant findings, $P < .001$) of these perceptions of the respondent versus those the respondent believes others have regarding detection and removal of spyware. The scale endpoints span from strongly disagree (1) to strongly agree (6).

The implications of these findings are twofold. On one hand, they seem to indicate that respondents are highly aware of the implications of malware, while they also seem to indicate there is a general lack of awareness in the larger population of others. Alternatively, these results may simply indicate that many people consider themselves more knowledgeable than their cohorts.

For those who teach or will employ the technology-aware college student the survey results have some good news. These respondents are significantly ($P < .001$) more knowledgeable of problems associated with spyware. The survey data shows that technology-aware respondents are more likely to update anti-virus software more frequently (4.89) than others (3.95). Further, these technology-aware majors have a significantly ($P < .001$) stronger (and anticipated) disagreement as compared to other majors on the following issues:

The problem remains and **THE BEST PROGNOSTICATIVE EFFORTS INDICATE THAT PROBLEMS ASSOCIATED WITH SPYWARE AND OTHER MALWARE WILL CONTINUE.**

- Malware damage is irreversible;
- Malware has a minimum effect in the workplace;
- Spyware is difficult to detect;
- Spyware is difficult to remove; and
- Helpdesk is responsible for spyware detection and removal.

Directions for the Future

As spyware and other malware proliferate, it will become increasingly important to achieve an adequate level of protection. But, it has been suggested that even organizations with large IS budgets and staff are underprepared, if not totally unprepared, to deal with the threats posed by malware and other security threats [7]. Indeed, companies like America Online are now offering malware protection as part of their standard service plans and they can show dramatic reductions in spam, for instance.

Universities offer free use access to top brand antivirus software and spyware detection and removal tools. In fact, some organizations require as policy that these tools be installed on all computers that are connected to the network. Yet, the problem remains and the best prognosticative efforts indicate that problems associated with spyware and other malware will continue. Consequently, prevention, detection, and remediation efforts will play a pivotal role in safe and secure computing in the foreseeable future.

Many of today's upper-division college students are well aware of prevention, detection, and remediation efforts, but others are ill prepared to deal with current threats on the home or business front. The survey shows that technology-aware students are very aware of protection strategies and they believe that software tools have made spyware detection and removal less difficult than in the past. Educators, managers, and business owners alike must be passionate about mitigating the threats of spyware and, in so being, their passion will help increase the knowledge levels of their peers. C

References

1. Associated Press. Security for Internet users deemed weak. ABC News; abcnews.go.com/Business/wireStory?id=195579, (Oct. 25, 2004).
2. Baig, E. Keep spies from sulking in your PC. *USA Today* (Jan. 22, 2004).
3. CKNow.com. Virus history; www.cknow.com/vtutor/vthistory.htm (as of Dec. 9, 2004).
4. Jones. M.C., Arnett, K.P., Tang, J.T.E., and Chen, N.S. Perceptions of computer viruses a cross-cultural assessment. *Computers & Security 12*, (1993), 191–197.
5. Rash, W. Spyware everywhere. *InfoWorld*; www.infoworld.com (subscriber email Sept. 9, 2004).
6. Stafford, T.F. and Urbaczewski, A. Spyware: The ghost in the machine. *Commun. AIS 14* (2004), 291–306.
7. Straub, D.W. and Welke R.J. Coping with systems risk: Security planning models for management decision making. *MIS Quarterly 22*, 4(Dec. 1998) 441–470.
8. Weiss, T.R. Egames settles with Michigan to remove ad software. *ComputerWorld;* www.computerworld.com/securitytopics/security/privacy/story/0,10801,56152,00.html (Jan. 11, 2001).
9. Wienbar, S. The spyware inferno. CNET News; news.com.com/2010-1032-5307831.html (Aug.13, 2004).

Mark B. Schmidt (mbschmidt@acm.org) is an assistant professor of information systems in the Business Computer Information Systems department in the G.R. Herberger College of Business, at St. Cloud University, St. Cloud, MN.

Kirk P. Arnett (karnett@cobilan.msstate.edu) is a professor of Information Systems in the College of Business and Industry, Department of Management and Information Systems at Mississippi State University.