

User Confidence—and the Software Developer

Warren Harrison with Guest Contributor Terry Bollinger

More and more everyday functions can be done online. I can shop, pay my bills, transfer funds between bank accounts, buy stock, and perform all manner of everyday business online. Not only does this save time in my already busy day, but it also contributes to a vibrant and healthy software



industry because each of these applications needs someone to develop and maintain them.

Recently however, my friends and I have been inundated with spyware—applications that lurk in the background and capture everything from keystrokes to the URLs of Web sites I visit. While I'm obviously concerned about my personal information getting into others' hands, I'm equally concerned about the effect of widespread security threats such as spyware and viruses on the confidence of online users who, like myself, have started to do more and more of their everyday business online. Many people have already quit making online purchases because of such threats. How long will it be until a lack of confidence in In-

ternet security will stall the strides that have been made over the past decade in establishing an online society?

Amazingly, even when the criminals who are helping bring down the Internet are caught, they're often given ridiculously light sentences. In some cases, they have even parlayed their criminal behavior into well-paying jobs. For example, as I write this, I just read an Agence France-Presse news story reporting that Securepoint, a German computer security company, has hired the accused (and self-confessed) author of Sasser—the worm that was responsible for infecting as many as 18 million computers and causing untold economic damage. There was even a fan club of sorts that was soliciting money for the worm's accused author (<http://support-sasser.homepage.dk>).

There's no doubt: the Internet as we know it is in grave danger.

As I pondered these issues, Terry Bollinger, *IEEE Software's* past associate editor in chief for construction, was having his own encounters with spyware. I asked Terry to share his experiences and thoughts with you. I hope you find his tale as interesting as I did.

In his own words: Terry deals with spyware

Despite having a very tightly configured system at home, somehow I was hit with a keylogger. Keyloggers are worse than having a high-resolution video camera focused on your keyboard because they're much more effective at capturing every key you enter. Fortunately, the software incarnations of these password-

DEPARTMENT EDITORS

Bookshelf: Warren Keuffel,
wkeuffel@computer.org

Construction: Andy Hunt and Dave Thomas,
(andy, dave)@pragmaticprogrammer.com

Design: Martin Fowler,
fowler@acm.org

Loyal Opposition: Robert Glass,
rglass@indiana.edu

Open Source Software: Christof Ebert,
christof.ebert@alcatel.com

Quality Time: Nancy Eickelmann,
nancy.eickelmann@motorola.com,
and Jane Hayes, hayes@cs.uky.edu

Requirements: Suzanne Robertson,
suzanne@systemsguild.com

STAFF EDITORS

Senior Lead Editor
Dale C. Strok
dstrok@computer.org

Group Managing Editor
Crystal Shif

Senior Editors
Shani Murray and Dennis Taylor

Staff Editor Assistant Editor
Rita Scanlan Rebecca Deuel

Editorial Assistant
Brooke Miner

Magazine Assistant
Hilda Hosillos, software@computer.org

Art Director
Toni Van Buskirk

Cover Illustration Technical Illustrator
Dirk Hagner Alex Torres

Production Editor Production Artist
Monette Velasco Carmen Flores-Garvey

Executive Director
David Hennage

Publisher Assistant Publisher
Angela Burgess Dick Price

Membership/Circulation Marketing Manager
Georgann Carter

Business Development Manager
Sandra Brown

Senior Production Coordinator
Marian Anderson

CONTRIBUTING EDITORS

**Robert Glass, Thomas Centrella,
Anne Lear, Molly Mraz, Keri Schreiner**

Editorial: All submissions are subject to editing for clarity, style, and space. Unless otherwise stated, bylined articles and departments, as well as product and service descriptions, reflect the author's or firm's opinion. Inclusion in *IEEE Software* does not necessarily constitute endorsement by the IEEE or the IEEE Computer Society.

To Submit: Access the IEEE Computer Society's Web-based system, Manuscript Central, at <http://cs-ieee.manuscriptcentral.com/index.html>. Be sure to select the right manuscript type when submitting. Articles must be original and not exceed 5,400 words including figures and tables, which count for 200 words each.

stealing critters aren't as transparent as the companies who make them claim. (Yes, they do sell them openly, to my amazement.) Symptoms of keylogger infestations include odd hesitations and pauses while you're doing simple operations such as typing text or opening and closing folders, although viruses and bugs in your operating system can also cause such behaviors.

Obviously, the consequences of home PCs getting hit with active keyloggers can be catastrophic. Do you do online banking? Have you entered a keyword to access your bank accounts lately? Would you be upset if you found your life savings missing the next time you log into your bank?

As you'd expect, I've changed a lot of passwords since my little visit from a keylogger. But the important part of my message is this: Even though I don't know how my PC got hit, I know almost exactly when it happened based on earlier checks and an instant-start identification of the problem. My system probably nailed the keylogger before it had a chance to do any serious damage. (I changed my passwords anyway.)

Are you curious about how my system caught the keylogger so quickly?

Competing for your trust

How can I be so sure I caught it early? Because I used a trio (now a quartet) of spyware checkers that collectively gave me a much higher level of trust than would be possible if I'd been relying on only one checker.

But why use three or four? Wouldn't it be easier just to use one that seems to work well? It would be easier, yes—but not necessarily safer. The real problem is this: How do you construct a reasonable case for trust when your sources aren't fully certified, as is often the case in leading-edge software products such as virus checkers?

Although by no means a total solution, my own approach was simple: Seek help from diverse sources and let them check each other out just as thoroughly as they check out my system. The result is a competition to be honest, in which unethical behavior by a member of the checker community is

likely to be screamed about from the highest housetops by their competitors. These vendors are competing in a market where trust is a substantial part of what they're selling.

My multitool strategy benefited substantially from the fact that three of the tools were free for home use and the fourth was quite cheap. Cost counts, and ultra-low costs enable strategies that might not be practical for large, costly systems. Also, during the selection process itself, running multiple spyware checkers is a great way to get an idea of who might be a "wolf in sheep's clothing," as some spyware pretends to be spyware checkers. The advantages of cross-checking extend into operational use: if any one of the group goes bad for whatever reason, cross-checking makes it easier for the other tools (and you) to notice the transition.

Make vendors compete for your trust

To decide on the four programs, I used them to see what they could find out about my system and each other. There were some revelations. For me, the most unpleasant surprise was that my top-end, professional Internet security and antivirus package sat like a stony statue on its pricey pedestal, refusing to say anything significant about the goings-on. Keyloggers? No problem! After all, they're not viruses—just little tools for taking over systems directly, without having to bother with the hassle of writing a virus.

That experience taught me a lesson about relying too much on tool reputations as my primary criteria for trust and system safety. I'm now convinced that it's a lot better to keep a variety of similar applications engaged in a constant knock-down, drag-out brawl, so that none of them can start getting sloppy without the others taking notice.

The other lesson is more ominous: If you use a standard PC, you really, really should do some spyware checks, and soon. If you are trusting in antivirus software and firewalls alone, you're going to be sadly let down. You could find, as I did, that you can have a fully

virus-free system that's so bloated with resource-hogging adware that on a good day it works like a turtle and on a bad day it doesn't work at all.

A spyware detector quartet

By now you're wondering what quartet of tools I selected, so here they are. A word of caution: watch out for similar names. Several products try to fool people into thinking they're another product, and some of those products are themselves spyware. Check the names and sites for exact matches before downloading any of these products.

Spybot Search & Destroy

This is THE free spyware checker right now and a must for finding spyware. It's remarkably fast and the most thorough of all the checkers I tested. (Each spyware checker finds some spyware that the others do not, no matter how thorough they are.)

Be sure to use the URL below for this one, as there's a product that has spoofed this real one in prominent ads. The spoof product is shabbily, even dangerously done (it tries to delete nonspyware files), and it tries to con you into paying money when the real and tremendously more effective product is free.

Spybot Search & Destroy has an optional feature called Tea Timer. If you don't mind being interrupted occasionally by alerts about suspicious activities, this is a powerful and useful feature to activate. It warns you immediately if a program is trying to change critical entries in your registry. If you suspect your system has been compromised, activating Tea Timer is a must, as it can help you identify and isolate the source of your problems. (True geeks: Check out FileAlyzer and RegAlyzer at the same URL.)

Download: www.safer-networking.org/en/download/index.html.

SpywareBlaster

This is my most recent addition. Unlike the others, it's not a scanner but rather a roadblock to keep a huge range of spyware from getting into your system in the first place. You only need to run it once to get the blocking

effect, although it's wise to update weekly to add blocks for new spyware.

An outstanding way to complement SpywareBlaster is to use a more conservative and more rigorously standards-compliant browser, such as the recently released, free Firefox 1.0PR browser (www.mozilla.org/products/firefox). This surprisingly powerful and easy-to-use browser locks out many problems in its default configuration and can be made safer and even more specific by settings for it from SpywareBlaster.

Download: www.javacoolsoftware.com/spywareblaster.html.

Lavasoft Ad-Aware SE Personal Edition

This is free for personal use but requires a fee for commercial use. It's thorough, but considerably slower than Spybot S&D and thus might be more appropriate for overnight checks if you have many files. Ad-Aware seems to go deeper into the registry and file structures, so it sometimes catches things the other checkers miss.

Download: www.lavasoftusa.com/support/download.

Webroot Spy Sweeper

A free trial is available, but this one does cost a modest amount of money—and in my opinion, it's well worth it. For example, Spy Sweeper has some useful shields that warn you instantly when a piece of software is trying to install something into your startup files. If you install Spy Sweeper and then download and install some of the more popular free multimedia players, you can watch as the multimedia installer tries multiple times to plant a hidden boot-time startup program on your computer without first asking for your permission. It's enlightening.

Download: www.webroot.com.

Maximizing multitool benefits

I should also mention two process issues for maximizing spyware checkers' effectiveness.

First, when you download checkers, be sure to keep copies of them around, such as on a CD. Why? Because some forms of spyware try to shut off spy-

EDITOR IN CHIEF

Warren Harrison

10662 Los Vaqueros Circle
Los Alamitos, CA 90720-1314
warren.harrison@computer.org

EDITOR IN CHIEF EMERITUS:
Steve McConnell, Construx Software
stevemcc@construx.com

ASSOCIATE EDITORS IN CHIEF

Education and Training: Don Bagert, Rose-Hulman Inst. of Technology; don.bagert@rose-hulman.edu
Design: Philippe Kruchten, University of British Columbia; kruchten@ieee.org
Requirements: Roel Wieringa, University of Twente; roelw@cs.utwente.nl
Management: Don Reifer, Reifer Consultants Inc.; dreifer@earthlink.net
Quality: Stan Rifkin, Master Systems; sr@master-systems.com
Experience Reports: Wolfgang Strigel, QA Labs; strigel@qalabs.com

EDITORIAL BOARD

Christof Ebert, Alcatel
Nancy Eickelmann, Motorola Labs
Richard Fairley, OGI School of Science & Engineering
Martin Fowler, ThoughtWorks
Jane Hayes, University of Kentucky
Andy Hunt, Pragmatic Programmers
Warren Keuffel, independent consultant
Karen Mackey, Cisco Systems
Deependra Moitra, Infosys Technologies, India
Suzanne Robertson, Atlantic Systems Guild
Richard H. Thayer, Calif. State Univ. Sacramento
Dave Thomas, Pragmatic Programmers

ADVISORY BOARD

Stephen Mellor, Mentor Graphics (chair)
Dave Aucsmith, Microsoft
Maarten Boasson, Quaeendo Invenietis
Robert Cochran, Catalyso Software
Annie Kuntzmann-Combelles, Q-Labs
David Dorenbos, Motorola Labs
Enrique Draier, MAPA LatinAmerica
Dehua Ju, ASTI Shanghai
Tomoo Matsubara, Matsubara Consulting
Dorothy McKinney, Lockheed Martin Space Systems
Bret Michael, Naval Postgraduate School
Susan Mickel, Lockheed Martin
Ann Miller, University of Missouri, Rolla
Dave Moore, Vulcan Northwest
Melissa Murphy, Sandia National Laboratories
Grant Rule, Software Measurement Services
Girish Seshagiri, Advanced Information Services
Martyn Thomas, Praxis
Laurence Tratt, King's College London
John Vu, The Boeing Company
Simon Wright, Integrated Chipware
Jeffrey Voas, Cigital

MAGAZINE OPERATIONS COMMITTEE

Bill Schilit (chair), Jean Bacon, Pradip Bose, Doris L. Carver, George Cybenko, John C. Dill, Frank E. Ferrante, Robert E. Filman, Forouzan Golshani, David Alan Grier, Rajesh Gupta, Warren Harrison, Mahadev Satyanarayanan, Nigel Shadbolt, Francis Sullivan

PUBLICATIONS BOARD

Michael R. Williams (chair), Michael Blaha, Mark Christensen, Roger Fujii, Sorel Reisman, John Rokne, Bill Schilit, Linda Shafer, Steven L. Tanimoto, Anand Tripathi

Welcome

As 2004 winds to a close, we wish to announce a number of changes among our volunteer staff. Both Ann Miller, our associate editor in chief for management, and Christof Ebert, our associate editor in chief for requirements, will change roles within the magazine. Christof now manages our new column on open source software, and Ann is moving to our Advisory Board. Also, Dave Thomas and Andy Hunt, who have managed our Software Construction column for the last three years, are stepping down to pursue new projects. We'd like to take this opportunity to thank Ann, Christof, Andy, and Dave for their many valuable contributions to *IEEE Software*.

We also have some new additions as we approach 2005. Don Reifer (of Reifer Consultants, Inc.) will return to the magazine after stepping down as Manager column editor last year to become our new associate editor in chief for management. Roel Wieringa (University of Twente) will serve as our new associate editor in chief for requirements. In addition, Diomidis Spinellis (Athens University of Economics and Business) is joining the Editorial Board to introduce a new column called Tools of the Trade, and Laurence Tratt (King's College London) and Bret Michael (Naval Postgraduate School) have just joined our Advisory Board. We'd like to welcome Ann, Christof, Don, Roel, Diomidis, Laurence, and Bret to their new roles on the magazine.

For more information about our new volunteers, see www.computer.org/software/experts.

ware checkers, just as some viruses try to shut off virus checkers. If a checker seems to stop working for no apparent reason, reinstall it, perform a fresh scan, and see what you find.

Second, if you've never done spyware checks before, I strongly recommend taking the time and effort to perform complete system scans using all the active scanning tools of the quartet: Spybot S&D, Ad-Aware, and Spy Sweeper. If all three find spyware, it's a good idea to repeat the cycle until they find no further hits or traces.

We welcome letters from those of you who find spyware infestations with any of these tools. If you find interesting, ominous, or surprising hidden spyware problems in your system, please let us know about them. Write to us at warren.harrison@computer.org and terry@terrybollinger.com. ☺

Terry Bollinger's biography appears on p. 18.



Went to find himself.

Left you 300K lines of C++ using macros to look like Pascal, and a Linux box you can't boot.

www.scitools.com

Tools that help you understand and maintain impossibly large bodies of source code.