

Constant Connectivity: Just Because You Can Doesn't Mean You Should

Warren Harrison

As I write this, news of the hack attack on George Mason University's computer systems, resulting in someone's access to the personal information of more than 32,000 students and employees, is just starting to circulate.

Last August, someone hacked into the systems at the University of California, Berkeley, and made off with almost 1.4 million Californians' names and social security numbers. However, mass identify theft through Internet-based hacking isn't exclusively limited to academic repositories. Between April 2002 and August 2003, 8.2 gigabytes of personal information were allegedly stolen from Acxiom, a customer information management service, during the course of 137 separate intrusions by hackers.



The effects of identify theft

The pain and inconvenience that identity victims feel is difficult to imagine unless it has happened to you, or someone close to you. It not only can affect the victim's financial standing and credit but can leave him or her with an embarrassing and difficult-to-explain criminal record if the imposter happens to commit a crime while posing as the victim.

In extreme cases, the police might issue a

warrant in the victim's name when the imposter fails to show up for a court date. Weeks or months later, the warrant comes to light during a routine traffic stop, and the innocent victim gets taken into custody, handcuffed, and booked into the county jail. Even if the physical description is somewhat inaccurate, as long as other information such as name, date of birth, driver's license, and social security number match, neither the officer nor the booking personnel usually have the discretion to ignore the warrant. Often there's no opportunity to explain the mix-up until the prisoner appears before a magistrate to explain his case. This is after being arrested, getting your car towed, and spending a night in a holding cell. Talk about adding insult to injury!

Where we're at

Today, virtually every computer I use has a persistent connection to the Internet: the computer in my home office, the one on my desk at the university, the computer into which I enter my students' grades, the workstation at my local public library. Even my department's high-speed photocopier is connected to the Internet. In fact, I challenge you to find a computer at your workplace that doesn't have an Internet connection.

The Netcraft annual Web server survey estimates more than 56 million active Web servers at the end of 2004, with more than

DEPARTMENT EDITORS

Bookshelf: Warren Keuffel,
wkeuffel@computer.org

Design: Martin Fowler,
fowler@acm.org

Loyal Opposition: Robert Glass,
rglass@indiana.edu

Open Source: 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

Tools of the Trade: Diomidis Spinellis,
dds@aueb.gr

STAFF

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

Group Managing Editor
Crystal Shif

Senior Editors
Shani Murray, Dennis Taylor, Linda World

Staff Editor Editorial Assistant
Rita Scanlan Brooke Miner

Magazine Assistant
Hilda Hosillos, software@computer.org

Art Director
Toni Van Buskirk

Technical Illustrator
Alex Torres

Production Editor Production Artist
Monette Velasco Carmen Flores-Garvey

Executive Director
David Hennage

Publisher
Angela Burgess
aburgess@computer.org

Assistant Publisher
Dick Price

Membership/Circulation Marketing Manager
Georgann Carter

Business Development Manager
Sandra Brown

Senior Production Coordinator
Marian Anderson

CONTRIBUTING EDITORS

**Thomas Centrella, Robert Glass,
Molly Mraz, Joan Taylor**

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.

911,000 new sites being added each month on average (http://news.netcraft.com/archives/2004/12/01/december_2004_web_server_survey.html). Remember, this is just the number of servers—it doesn't include computers connected to the Internet as clients.

As software developers, we continue to take advantage of this widespread connectivity. How many of us work for an organization that has migrated the bulk of its applications to communicate via HTTP with standard Web clients such as Mozilla and Internet Explorer? Of these, how many are hosted on machines with 24/7 connectivity to the Internet (as opposed to an isolated intranet)?

Do we really need to be as connected as we are?

If we think of the millions of machines now hosting HTTP server-client applications, how many really need 24/7 Internet connectivity? Being able to access your company's financial records or customer lists when you're at home on a weekend or halfway across the country on a business trip is certainly convenient. Allowing patients to see their medical records over the Web from home can make them feel warm and fuzzy, even if they don't know a scapula from a coccyx. My students can now access their grades online on the Tuesday after finals week rather than waiting until Friday to get their hardcopy grade reports by surface mail. But how valuable is this additional convenience?

Obviously, some systems exist only because of Internet connectivity. Amazon and eBay would be of little use otherwise—connectivity is their raison d'être. On the other hand, do I really need to be able to access my W2 form or check on my payroll deductions over the Web? Do I really need to be able to renew my driver's license from home using Internet Explorer?

Am I in favor of convenience? Sure. But at what cost? Are you willing to spend a night in jail or have your credit ruined in return for not having to go to the local motor vehicles office to renew your license? Is it worth the risk that

some high school kid, or a member of organized crime, or (for you paranoid types) a member of a shadowy, clandestine government agency just might get access to your information just so you don't need to visit your doctor to review your medical history? Is it really worth the risk to be able to transfer money from one bank account to another or pay your credit card bill from home to avoid a trip to the bank?

Well, yes, I want convenience, but security too!

I would agree with many readers that we should be able to have convenience and security. The fact is, however, I often don't have the former and almost never have the latter with the majority of Web-based systems I deal with.

The Pew Internet and American Life Project recently released a survey in which only 32 percent of the respondents agreed that by 2014 "network security concerns will be solved" (www.pewinternet.org/pdfs/PIP_Future_of_Internet.pdf). In fact, one respondent to the survey observed, "It is foolhardy to underestimate the fragility and vulnerability of any online system to attack and manipulation. Anything that can be made secure can be hacked."

We must face the fact that our systems and the information they contain aren't all secure. It's not that the administrators of these sites take security lightly or are incompetent. The fact is, people are only human. (You heard it here first!) Eventually someone's going to make a mistake. It happens in medicine, police work, construction, and commercial aircraft. Even on the most secure Internet-connected system in the world, if you accidentally type `chmod w+rw` instead of `chmod u+rw`, you probably have problems.

What are the chances that any given experienced system administrator or site developer will do this? I'd guess it's pretty slim. What if we have 56 million experienced system administrators? The probability seems a lot greater, I'd say. Couple this with the likelihood that a good percentage of the owners of these 56 million sites are not only inexperienced system administrators, they

don't even know they're online. Linux and XP both make it far too easy to start up an HTTP server without the system's owner really knowing what's going on.

If we can reduce that 56 million to only those systems that really need Internet access, we'd significantly reduce the probability of security holes due to mistakes and oversights.

Don't shut the Internet down!

I'm not suggesting we disconnect every computer from the Internet. It clearly serves many beneficial social purposes. But reading a blog or a book review online is a long way from having immediate online access to sensitive personal and financial information.


I urge you system architects to look hard at whether the system you're designing really needs to be accessible via the Internet. Is providing information over the Internet really a core mission for your application, or is it just an inexpensive "extra feature"? We can't simply say, "All systems will soon be connected to the Internet; there's nothing we can do about it." We're the ones developing the architectures and working with customers to define these sys-

tems' requirements. If it doesn't start with us, it won't start.

I urge network engineers to consider laying two network drops when they run a LAN: one for a "secure" internal LAN and one for an "open" LAN connected to the Internet through a firewall. You can control access through physical switches so that a given client can, at any point in time, connect to one or the other, but not both. Clearly, this adds a little incremental cost, but compare it with having to notify 1.4 million people that someone has stolen their personal information because your organization overlooked an unsecured machine.

I truly believe that when it comes to Internet connectivity, just because you can do it doesn't mean you should. It's not just your information at risk—it's mine, too.

Feedback welcome

What do you think? Is the convenience of many of these systems worth the risk to which they put your data? Are there any systems you know about that are needlessly connected to the Internet? Please write me at warren.harrison@computer.org. 

Coming Next Issue

Adapting Agile Processes

- Key Concepts in Agility and the Agile Manifesto
- Adaptive Agility: Managing Complexity and Uncertainty
- Primavera Gets Agile
- Project Management and Agile Methodologies: A Survey

Estimation

- Practical Guidelines for Better Software Effort Estimation
- Beyond Cost: The Drivers of COTS Application Value

See our Editorial Calendar at
www.computer.org/software/edcal.htm

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; 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
 Martin Fowler, ThoughtWorks
 Jane Hayes, University of Kentucky
 Warren Keuffel, independent consultant
 Suzanne Robertson, Atlantic Systems Guild
 Diomidis Spinellis, Athens Univ. of Economics and Business
 Richard H. Thayer, Calif. State Univ. Sacramento

ADVISORY BOARD

Stephen Mellor, Mentor Graphics (chair)
 Maarten Boasson, Quaerendo Invenietis
 Robert Cochran, Catalyst Software
 Annie Kuntzmann-Combelles, Q-Labs
 David Dorenbos, Motorola Labs
 Juliana Herbert, ESICenter UNISINOS
 Dehua Ju, ASTI Shanghai
 Gargi Keeni, Tata Consultancy Services
 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
 Deependra Moitra, Infosys Technologies, India
 Melissa Murphy, Sandia National Laboratories
 Grant Rule, Software Measurement Services
 Girish Seshagiri, Advanced Information Services
 Martyn Thomas, Praxis
 Rob Thomsett, The Thomsett Company
 Laurence Tratt, King's College London
 John Vu, The Boeing Company
 Simon Wright, SymTech
 Jeffrey Voas, independent consultant

MAGAZINE OPERATIONS COMMITTEE

Bill Schilit (chair), Jean Bacon, Pradip Bose, Doris L. Carver, Norman Chonacky, George Cybenko, John C. Dill, Frank E. Ferrante, Robert E. Filman, Forouzan Golshani, David Alan Grier, Rajesh Gupta, Warren Harrison, James Hendler, M. Satyanarayanan

PUBLICATIONS BOARD

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