

Passwords and Passion

Warren Harrison

I still remember encountering my first zealot: my dental hygienist. After taking one look at what she must have considered my horribly misshapen maw, she excitedly began listing the corrective procedures that she felt were absolutely necessary. “We can cap the front teeth and add a set of braces to take care of that overbite ... but you’d only have to wear them at night ...” she began.



“I’m just here for a cleaning,” I responded. My hygienist looked at me with a mix of astonishment and offense—astonished that I cared so little for my oral fitness (since I wasn’t interested in paying thousands of dollars to cap my perfectly functional teeth) and somewhat offended that I didn’t take her advice to heart.

It took some reflection to fully understand that our world views differed radically. My hygienist, who dealt daily with cosmetic oral curses such as chipped teeth, overbites, and coffee stains, obviously viewed one’s teeth as the center of one’s soul. I, on the other hand, resented the 30 minutes stolen from my otherwise-packed schedule to be subjected to my annual cleaning. I was happy as long as I could eat a Milk Dud without losing a filling and I didn’t have any teeth that wobbled *too* badly when I brushed.

Security zealots

Recently, I read about a survey conducted by Sophos (www.sophos.com/pressoffice/news/articles/2006/04/passwordadvice.html) that

asked, “Do you use the same password for multiple Web sites?” Their admittedly unscientific results confirmed what most of us would expect: 41 percent of the respondents said they always use the same password, 45 percent said they have a few different passwords, and 14 percent said they never use the same password on multiple Web sites. My guess is that those 14 percent either don’t have an Internet connection or are “security professionals.”

Since that day in the dental hygienist’s chair, I’ve encountered numerous other zealots in fields ranging from religion to automobile tires. But I flashed back to my dental hygienist when I discussed the Sophos survey results with some of my “security professional” acquaintances. They expressed the same mixture of astonishment and offense (well, maybe not so much astonishment) as she did that day years ago.

As with almost every other zealot I’ve encountered over the years, I concluded that these folks just don’t get it. Sure, good (at least functional) teeth, tires that won’t spontaneously explode, and the privacy of my personal data are important to me. But most people aren’t going to commit a huge amount of resources to achieve these goals. Maybe they should, but they won’t—if they did, everyone would brush and floss twice a day, have their tires rotated every 3,000 miles, and voluntarily change their passwords every two weeks. I might be out in left field here, but I don’t think any of these are common behaviors.

User overhead

The problem is that where the “security professional” sees prudent, responsible behavior,

DEPARTMENT EDITORS

Bookshelf: Warren Keuffel,
wkeuffel@computer.org

Design: Rebecca Wirfs-Brock,
rebecca@wirfs-brock.com

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: Neil Maiden,
N.A.M.Maiden@city.ac.uk

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

Assistant Editor Editorial Assistant
Brooke Miner Molly Mraz

Magazine Assistant
Hilda Carman, software@computer.org

Art Director
Toni Van Buskirk

Technical Illustrator
Alex Torres

Production Artist
Carmen Flores-Garvey

Executive Director
David Hennage

Publisher
Angela Burgess
aburgess@computer.org

Associate Publisher
Dick Price

Membership/Circulation Marketing Manager
Georgann Carter

Business Development Manager
Sandra Brown

Senior Production Coordinator
Marian Anderson

CONTRIBUTING EDITORS

**Cheryl Balthes, Robert Glass, Annette Ibrahim,
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.

users simply see overhead that gets in the way of performing whatever task they're trying to do.

For example, the US National Archives (www.archives.gov/frc/cips/password-rules.html) has several rules for their passwords. Passwords must contain exactly eight characters, including one or more of each of these three classes:

- letters,
- numbers, and
- special characters <e>, @, #, \$, and </e>.

Passwords cannot contain

- repeating letters or numbers (such as aa, DD, or 22),
- common words and abbreviations, or
- any portion of the user ID.

Finally, users must

- change their passwords at least every 90 days and
- not reuse their last three passwords and current password.

You can just imagine the joy users feel when they first encounter this set of rules, since the systems are so much more secure than unprotected files. It's very likely that users are told to never, ever write their password down in case some nefarious coworker might misappropriate it and, moreover, that discovery of such a misdeed can result in disciplinary action. And just in case someone might try to masquerade as a user and call in claiming to have forgotten his or her password, users must no doubt request new passwords in person with multiple forms of picture ID.

Indeed, users who are simply trying to get their jobs done will likely be falling all over themselves with glee at how secure this data is. We can barely imagine their joy when informed that the passwords on the eight different systems they must use to perform their various daily tasks must all be different to ensure that if one account is compromised, the others won't be. Surely any information worker would be

giddy with happiness over working in such a secure environment.

Of course, the reality is that users will complain. They'll find ways to circumvent the mandatory periodic password changes so that they won't have to memorize yet another password. (My favorite is to simply make three successive password change requests to get back to that clever password I memorized two years ago.) If they do forget their password, which they're almost certain to do, they'll simply borrow a coworker's account until they can make time in their busy schedules to hike over to Operations and beg for a new password. In spite of the security staff's good intentions, users are more likely to view complicated password rules and mandatory change schedules as simply more bureaucratic overhead rather than as an important part of system security.

A technology whose time has passed?

In fact, usernames and passwords are relatively ancient technology. They were never designed to protect access to sensitive information. In the early days of computing, they served simply to organize files and manage resources (for example, managing quotas and charging for time-sharing services). In this era, fellow computer users were viewed as colleagues and not adversaries. Virtually every Unix system had a guest account (that wasn't password protected), and virtually all files were world-readable. Passwords were actually maintained in clear-text files (albeit not world-readable ones) and compared directly to whatever the user typed in.

In the early days of computing, typical users connected through serial connections (direct dial-ups or hardwired 9,600-baud serial cables) and had only one or two accounts to deal with. No one worried about packets shuttling through intermediate network nodes of unknown pedigree. In fact, the primary hurdle most hackers had to contend with in those days was discovering a telephone number connected to a modem.

It should be no surprise, then, that when the World Wide Web arrived, lit-

tle thought was given to security. For example, not only did a GET request send the form contents in the clear, they were also stored in a world-readable log file. Amazingly, this was the default mechanism for submitting a form. Unless the Web page author chose to use the METHOD = POST parameter in the FORM tag, you could count on whatever you entered in a form being stored in a log file for the world to see. Similarly, basic authentication would by default send usernames and passwords in the clear.

Of course, that was then and this is now. What most amazes me is how well username and password technology has adapted to ever-increasing security demands. But we're almost certain to hit a wall sometime soon in terms of what we can expect from this paradigm.

Evolving technology on questionable foundations

To some degree, the evolution of usernames and passwords from a file organization and resource management mechanism to a barrier between our financial assets and criminals worldwide represents many of the computing issues we face in the 21st century. Rather than recognizing the need for a new approach to doing things, we continue to tweak old technology to (temporarily) meet our needs.

For example, as the number of Internet users and devices increases, we're quickly running out of IP addresses. At one time, static IP addresses were the norm, and you could associate a specific device with a specific activity on the Internet. However, as we began to run out of IP addresses, dynamic addressing appeared to temporarily fix the problem. Now, as Internet use soars, even dynamic IP addressing doesn't provide enough address space for everyone who might want to connect to the Internet (for example, using the traditional Class ABC method, China has only 22 million IP addresses for a population of 1.3 billion people). Classless interdomain routing, or CIDR, is an evolution in IP addressing and is expected to correct this limitation while still maintaining a

32-bit IP address. But will it be enough once cell phones, automobiles, and refrigerators begin to be assigned IP addresses?


The File Allocation Table (FAT) file system is another example of technology being tweaked to accommodate new environments long after it should have been retired. Continuing to maintain the FAT file system to enable backward compatibility severely limited Windows' ability to provide true file-system-level access control. It was at least partially responsible for many of the security issues we encountered as we moved from stand-alone desktop systems to 24/7 connected environments. Even today, although Windows XP defaults to NTFS (New Technology File System), we can still bully it into creating a FAT file system if the drive is small enough.

Do we need evolution or revolution?

Numerous authentication schemes have been proposed—smart cards, biometrics, and others. But to some extent, these are really just evolutions of the username and password paradigm. They all end up sending a message from the client to the server telling it that the client is really who it says it is. As different tweaks are applied to provide security for yet another year, we might do well to consider revolutionary schemes for user authentication.

What might these schemes be? I honestly don't know. I do know, however, that if all you have is a hammer, the whole world looks like a bunch of nails. As long as security zealots continue to labor under the fantasy that the typical user views security as part of his or her job, security will continue to be the weak link in the promise of the Internet.

What do you think?

How much time do users in your organization spend dealing with system security issues? Have you ever missed a deadline or had to work in crisis mode because of your organization's system security policies? Please write me at warren.harrison@computer.org. 

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
stemcco@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@ieeee.org

Requirements: Roel Wieringa, University of Twente; roelw@cs.utwente.nl

Quality: Stan Rifkin, Master Systems; sr@master-systems.com

Experience Reports: Wolfgang Strigel, QA Labs; strigel@qalabs.com

EDITORIAL BOARD

Grady Booch, IBM

Christof Ebert, Alcatel

Nancy Eickelmann, Motorola Labs
Jane Hayes, University of Kentucky
Warren Keuffel, independent consultant

Neil Maiden, City University, London

Diomidis Spinellis, Athens Univ. of Economics and Business

Richard H. Thayer, Calif. State Univ. Sacramento

Rebecca Wirfs-Brock, Wirfs-Brock Associates

ADVISORY BOARD

Stephen Mellor, Mentor Graphics (chair)

Maarten Boasson, Quaerendo Invenietis

J. David Blaine, Blaine Consultancy

Robert Cochran, Catalyst Software

Annie Kuntzmann-Combelles, Q-Labs

David Dorenbos, Motorola Labs

Kaoru Hayashi, SRA

Simon Helsen, SAP

Juliana Herbert, ESICenter UNISINOS

Dehua Ju, ASTI Shanghai

Gargi Keeni, Tata Consultancy Services

Karen Mackey, Cisco Systems

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

Suzanne Robertson, Atlantic Systems Guild

Grant Rule, Software Measurement Services

Girish Seshagiri, Advanced Information Services

Martyn Thomas, Praxis

Rob Thomsett, The Thomsett Company

Laurence Tratt, King's College London

Jeffrey Voas, SAIC

John Vu, The Boeing Company

Simon Wright, SymTech

CS PUBLICATIONS BOARD

Jon G. Rokne (chair), Michael R. Blaha, Mark Christensen, Frank E. Ferrante, Roger U. Fujii, Phillip Laplante, Sorel Reisman, Bill N. Schilit, Linda Shafer, Steven L. Tanimoto, Wenping Wang

MAGAZINE OPERATIONS COMMITTEE

Bill N. Schilit (chair), Jean Bacon, Pradip Bose, Arnold (Jay) Bragg, Doris L. Carver, Kwang-ting (Tim) Cheng, Norman Chonacky, George Cybenko, John C. Dill, Robert E. Filman, David Alan Grier, Warren Harrison, James Hender, Sethuraman (Panch) Panchanathan, Roy Want