Self-Inflicted April Fool Joke

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

As most readers know, I am the Program Director for the Master of Science in Information Assurance (MSIA) at Norwich University. Although I have turned over responsibility for teaching the curriculum to highly qualified instructors such as Peter Stephenson, David Bouvin, and Gary Bridges, and am working with curriculum developers Stephen and Chey Cobb, I still develop the quizzes and exams.

Last week my first quiz in the MSIA 1.3 seminar (Technical Defenses) blew up in my face. As usual, I had included some comic relief in the multiple-choice selections just to avoid boring the students (I detest multiple-choice exams, but they are useful in encouraging review and they’re quick for the students). You can imagine my surprise when the first students to take the quiz reported in shock that the “correct” answers were preposterous. Here are some of my favorites with the INCORRECT “correct” answers marked with an asterisk (you can figure out the REAL correct answers yourselves):

5. When an attacker obtains a copy of the encrypted password file and uses a password-cracking program on it to find valid passwords, this attack is an example of
   a) a capture-replay attack
   b) a hash-brown attack
   c) password sniffing
   d) an offline dictionary attack
   e) None of the above

8. How can an organization best discourage sharing of passwords?
   a) Electrocute the second concurrent user of a password.
   b) Establish effective methods of delegation for selected privileges of one user to another.
   c) Establish monetary prizes for all employees who report cases of password sharing.
   d) Fire every employee who uses someone else's password
   e) None of the above

15. When a workstation connected to a LAN reads all frames or packets going past it even though they are not addressed to it, the workstation is in
   a) promiscuous mode
   b) prostitute mode
   c) slut mode
   d) spy mode
   e) None of the above

[Students pointed out that the choices in question 15 could easily be offensive to many people, so I did change the language to neutral terms for the corrected quiz.]

18 A model for secure password-based authentication that eliminates the risk of capture-playback attacks is
How did this mixup happen? I easily traced it to two problems, one systemic and one technical. The most important problem – and one that will be corrected henceforth – is that I failed to impose quality assurance steps on the production of the quiz. The minor problem occurred because of an interesting aspect of MS-Excel worksheets: the persistence of formatting after the delete command. Here’s what happened.

In creating the quiz, I go through our teaching materials and write down questions and answers in a spreadsheet, marking the correct answers in boldface. Then I copy the questions and paste them into another worksheet and add a randomizer to be able to scramble the order of the questions. Unfortunately, when I pasted the questions into the randomizing worksheet, I pasted the _values_ of all the cells, completely forgetting that I had to keep the boldface formatting to track the correct answers. Because the apparently empty worksheet had already been used for a previous quiz, the boldface cells from the previous quiz’s correct answers bolded the wrong answers in the new quiz – and I didn’t notice.

When I sent the materials to our Webmaster to put the quiz up on our Prometheus teaching system, he did wonder about the “electrocute the second concurrent user” answer but, not being a security guy, simply installed the quiz without comment.

So there’s the joke on me: with all my whining about quality assurance and the importance of checking one’s work and dumping on other people for putting mistakes into production because they don’t use checklists, here I am, red-faced with both embarrassment and amusement at my own blooper.

Well, the corrected quiz is back up with all the correct answers in place (and a few questionable bits removed) and the students should be able to manage without further shocks to their delicate systems.

In the meantime, I’m working on a checklist.

* * *

NEW! 18-month online Master of Science in Information Assurance offered by Norwich University; see <http://www3.norwich.edu/msia> for full details.


M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mailto:mkabay@norwich.edu>; Web site at <http://www.mekabay.com/index.htm>.