Creating Viruses in a University Course (2)

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

In my last column, I discussed how University of Calgary Professor John Aycock has been including a bit of virus-writing in his course called "Computer Science 599.48: Computer Viruses and Malware."

I have been involved with the antivirus (AV) industry in a peripheral way since the early 1990s, when I was the recording secretary at the organizing meetings of the Antivirus Product Developers Consortium of the National Computer Security Association (NCSA; later ICSA and eventually TruSecure). I can personally attest to the intense emotions of people in the AV industry about virus writers: they detest them. Perhaps some of the vitriol thrown at Professor Aycock results from an emotional response rather than from a wholly rational appraisal of risks and consequences.

I wrote to the University of Calgary about this situation. Dr Ken Barker, Head of the Department of Computer Science, responded as follows:

>A thorough understanding of any material requires that we look at it from as many perspectives as possible. Students in high school learn that the most effective way to prepare an argument for a debate is to prepare to argue both the affirmative and negative sides. The most competent and insightful economists are those who can clearly articulate and understand both a fully free market system and a controlled socialist strategy to the economy. The better we understand something, even if we radically disagree with it, the more likely we are to provide effective mechanisms to counteract them. These analogies provide the context for the approach taken by the University of Calgary’s CPSC 599.48 course. A very small portion of the course is spent on understanding how viruses are created and deployed in an extremely protected environment while ensuring that the students have a complete understanding of the legal and ethical framework surrounding this kind of code. The students are thereby better prepared to learn how to best fight the plethora of viruses and malware found in the modern compute environment.

The cautionary approach demanded by our critics during the first offering of the course was incorporated into the way we delivered the material. The alarms raised by the anti-virus community were addressed carefully and diligently to ensure that the course would be offered in a safe and valuable way. After a careful review of the first offering and upon considering the ongoing need for this level of expertise, the University of Calgary believes that it is in the greater public good to continue to offer the course. <

I commend my colleagues for having responded constructively to the concerns of AV professionals and wish them well in their project. I sincerely hope that the reasoned approach they have adopted will indeed result in a net gain to security in the long run.

* * *

In the next couple of columns, I’ll address the question of whether writing virus code should be defined as illegal in the same way that possessing lock-picking tools without a license is defined
as illegal.

* * *

A Master’s degree in the management of information assurance in 18 months of online study from Norwich University – see <http://www3.norwich.edu/msia> for details.

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management 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>.

Copyright © 2004 M. E. Kabay. All rights reserved.

Permission is hereby granted to Network World to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.