

Why Study Computer Crimes?

A Personal Commentary

M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance / School of Business & Management
Program Director, MSIA / School of Graduate Studies
Norwich University, Northfield, VT 05663-1035 USA

Updated January 2009

Admiring Criminals?

In public discussion of crime techniques, someone always asks whether it's prudent to talk about crime so openly.

The arguments against such discussion fall into two classes. Won't people get ideas? That is, will discussing crime lead to more crime? And won't descriptions of how to commit a crime teach criminals how to be more effective? That is, will discussing crime make crime prevention harder?

Yes, it is possible that describing criminal acts will suggest to people on the borderline of honesty that they could carry out a similar crime. Copycat crimes are a well known consequence of newspaper stories about any unusual crime. The romantic image of crackers in such movies as *War Games* and *Sneakers* may indeed contribute to the delinquency of computer-literate minors.

However, when computer crime techniques are put in perspective, it is hard to believe that the overall effect is to encourage crime. When I teach the three-day *Information Systems Security* course on which this text is based, I repeatedly stress that the criminals who abuse information systems and use computers in their crimes are enemies of society. Embezzlers steal the life savings of innocent victims; thieves and swindlers and extortionists increase the costs of goods and services for everyone; and blackmailers victimize the weak and push them into despair.

After Craig Neidorf was accused in February 1990 of publishing stolen information about BellSouth 911 operations, security specialists engaged in vigorous debate about the issue of publishing computer crime techniques. Long articles in the *Communications of the ACM* provide extensive discussion by leaders in the field. Some argue to this day that no limitations should be imposed on the publication of any information; others feel that society has a right to restrict the dissemination of dangerous information.¹

As you read about computer crimes, be on guard against the seductive lure of crime. Some criminal techniques are so clever and so original that it's easy to fall into the trap of admiring the criminals. Remember that the criminals consider themselves better than you and me; they put themselves above the norms of decency and kindness that most of us strive for. Computer criminals are often intelligent, but at a fundamental level they are despicable and defective human beings.

¹ Denning, D. (1991). The United States vs. Craig Neidorf: a debate on electronic publishing, constitutional rights and hacking. *Communications of the ACM* (March 1991) 34(3):9 http://www.eff.org/Net_culture/Hackers/us_v_craig_neidoff.article

Why study crimes?

If that mantra doesn't sour your admiration for crooks, nothing will.

Full Disclosure

The second question concerns the danger of showing criminals weaknesses in security. Security practitioners have struggled with this problem for years. In the first place, much of the discussion to follow centers on carelessness and lack of training, not on criminality. Helping managers and employees tighten up their attention and improve their policies to reduce accidents will not aid criminals.

Another answer has been commonplace in military doctrine since some nameless protohuman decided to fight back against the local top carnivore: security is by its nature a defensive proposition. There are many ways of breaching barriers; the foe need find any one of the weak spots, but the defenders must guard the entire perimeter. Security professionals do the best they can given constraints of time and money, but people determined to overcome the defenses can spend as much time and effort as they wish to locate weak spots.

Another point in defense of teaching is that a course or discussion of counter-measures need not provide solace to the enemy. Discussing forgery techniques, for example, can go as far as mentioning that color copiers and scanners make it easy to counterfeit some currencies and official documents. However, it doesn't take a rocket scientist to realize that imaging technology can be abused. Simply pointing out the problem does not constitute a primer in the techniques, especially when coupled with admonitions to be more skeptical about official-looking documents of all sorts. The balance of risks and benefits seems clearly on the side of benefits.

Giving details sufficient for emulation is another matter, however.

A controversial example of providing too much information revolves around the publication of detailed source or object code for functional viruses. In 1991, someone published a book containing detailed instructions on how to create functional viruses. The book included source code. The publication of this manual caused a furor in the anti-virus product developers' community. Some prominent anti-virus workers proposed to assault the author; others reviled him to his face and on the electronic networks.

I and others feel that it is unnecessary to give such detailed instructions to people interested simply in defending themselves against viruses. Very few people will be able to use detailed information about virus code for constructive purposes. It is enough for most people to rely on shareware and commercial anti-virus products and let experts handle the dangerous code under conditions of tight security and isolation.

After all, no one seriously proposes that anthrax bacilli or polio virus be freely distributed for amateur microbiologists.

In March of 1993, I published a short opinion piece in *Network World* entitled, "Virus Code and the First Amendment." I argued that even if we admit that virus code is speech, it need not be protected by First Amendment rights to free speech. In any case, I proposed, virus code is not speech any more than punched paper tapes for milling machines are speech, and so the whole

Why study crimes?

issue of First Amendment rights for publishers of virus code is irrelevant. Publishing virus code irresponsibly or with malicious intent should be punishable.²

This article provoked the most mail I have ever received for a publication. Within days, my electronic mailbox on the Internet was inundated with vigorous discussion, mostly opposing my proposals on (I admit) reasonable grounds. The most striking argument among the 100K bytes of correspondence I received was that hiding knowledge is not an effective defense.

My own position is that I will not provide workshops in how to commit computer crimes. The information I provide in my writings and my teaching helps participants defend themselves but does not materially aid them in honing criminal techniques.

University Courses

A storm of criticism washed over a University of Calgary Professor in early summer of 2003 when he announced his intention to teach a fall course entitled “Computer Science 599.48: Computer Viruses and Malware.” Assistant Professor John Aycok shocked the antivirus world by including his intention to have his undergraduate students write some malicious code. Many experts objected on the following grounds:

- Writing malicious code was unnecessary in teaching how viruses, worms and Trojan horses work or how to fight them;
- Keeping the malicious code contained within the class of laboratory would be difficult or impossible;
- Some students would take the wrong message home about the ethical implications of creating malicious code;
- Students with experience writing malware would be unemployable by antivirus firms, always concerned about the widespread rumor that they engage in writing viruses for profit.

Supporters of the course scoffed at these arguments, assuring critics that the Laboratory would be well secured and insisting on the pedagogical value of such exercises. In addition, they stressed that virus writing would be only a small part of the course, which would also teach students about the history of malware, economic consequences of these programs, countermeasures, legal and ethical considerations, and wider principles of computer and network security.

After the course was over, there appeared to have been no breaches of security and University spokespersons insisted that they would offer the course again despite their critics.

It seems to me that writing real viruses may be less valuable to the students than analyzing a wide range of existing viruses and thinking about, designing, and implementing antivirus

² Updated in Kabay, M. E. (2004). Viruses Are Not Speech. http://www.mekabay.com/opinion/virus_not_speech.htm and http://www.mekabay.com/opinion/virus_not_speech.pdf

Why study crimes?

mechanisms. However, given the relatively minor part that this exercise plays in the overall course, it also seems to me that critics may have overreacted.

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.³

³ Dr Aycock provoked yet another storm when he proposed to teach students how to write spam generators and spyware in his new "CPSC 599.63 Spam and Spyware" course (see <http://pages.cpsc.ucalgary.ca/~aycock/spam.html>). Type "Aycock spam spyware" into any search engine for many news articles about this case. Examples include Mello, J. P. (2005). Malware 101: University offers course on spyware. <http://www.technewsworld.com/story/40479.html>

Why study crimes?

For further reading about the University of Calgary virus course, see

Fisher, D. (2003). University of Calgary to Offer Virus-Writing Class.

< http://www.eweek.com/print_article/0,1761,a=42315,00.asp >

Fried, I. (2003). College plans virus-writing course.

< http://news.com.com/2102-1002_3-1010538.html >

Pryma K. (2003). Security Experts Blast Virus Class.

< <http://www.itbusiness.ca/index.asp?theaction=61&sid=52619#> >

Read, B. (2004). How to Write a Computer Virus, for College Credit: Experts debate whether a course at the U. of Calgary is a useful tool or a risky invitation. *The Chronicle of Higher Education -- Information Technology* 50(19):A33 (January 16, 2004).

< <http://chronicle.com/free/v50/i19/19a03301.htm> >

