p 2q 1A
RCJ

Passages from PP&E lecture notes to act as solution notes for the 2003 PP&E 4 mark question:

Richard C. Jennings

A. Computer cracking - some arguments

Argument 1: All information should be public

One argument is that all information should be public, which has as a corollary that there would be no problem of intellectual property and security if it were. This is a view that has survived from the early days of computing and software writing when the software hacks were willing to share their productions with anyone who would appreciate those productions. An interesting analogy here is the socialist view that all property should be public property. But all societies have some property that is not communally owned and in the 21st Century Western Society, information is increasingly not communally owned. And this, of course, gives rise to the problems of intellectual property and information security. Let us ask what grounds there are for saying that all information *should* be free. The basic claim is that in all aspects of our lives we need information. In deciding whether to dress for a balmy day or a cold rainy day, or in deciding whether to go into computing or into mechanical engineering, we need to know things like the weather report or the job prospects in different fields. Moreover, our very political system depends on freely accessible information. If we knew nothing of the candidates in elections, or if we only knew how wonderful one of them was, we would not be able to make a reasonable choice when we came to vote.

The flaw of this line of reasoning is that it doesn't apply to *all* information. Certainly we need to know about the candidates in an election, and we need to know much about the world to make decisions about what to do, both in the short term and in the long term. But there are other things that we value, or at least our society values, which are inconsistent with total freedom of information. There are three areas in which total freedom of information is probably not a good idea: areas concerned with individual privacy, national security, and information with economic value.

But if we consider just an instance of the general maxim that all information should be free, namely that all software should be free, then we avoid the above arguments. This means that to confront the more particular claim that all software should be public we need to develop a whole new line of argument. And this warrants another discussion in its own right.

Argument 2: Break-ins are beneficial by revealing security flaws

Another argument that is used to defend cracking is that it is a way of revealing the flaws in computer security systems. The cracker sees himself as performing the valuable service of discovering weaknesses in the systems that are supposed to limit access to authorized users. The cracker is seen as analogous to the Cambridge character who tries to wheel away bicycles that he passes in the street. When a bicycle turns out to be unlocked he wheels it a distance away so that the owner finds it but not where she left it. This is a kind of public service of warning unwary cyclists of the dangers of leaving their bicycles unlocked. It reveals flaws in her bicycle security system. But a less flattering analogy for the cracker can be made to the person who goes from room to room, or house to house, trying the doors to see if they are locked. Then, if they are locked he tries the windows, and failing there gets out his collection of keys and tries them in the door lock. Clearly, there are different images that we can develop for the cracker, and depending on the image we adopt, cracking will be more, or less, attractive.

But there is a more sinister problem with cracking. It is this. Typically cracking is not an individual activity, in general cracking is a cooperative activity practiced by groups of people who are linked through computer networks. They share techniques and knowledge with each other and often number among their members individuals who are "insiders" of different systems. In keeping with hacker ethics these networks of crackers are open networks. And the serious problem is that they are open also to those who would use the craft, knowledge and techniques of the crackers for more sinister ends, such as embezzlement and other sorts of computer crimes. It is for this reason that organizations with large networked computer systems need to keep upgrading their security systems, not so much to protect against the cracker *per se*, but to protect against the computer criminal who is riding on the back of the cracker. The cracker is like the molecular biologist who is playing around with organisms in order to find those which can crack into the cells of the human body, and who openly shares his

knowledge in a public discussion group with anyone who takes an interest in that sort of thing. The knowledge is not morally neutral, it can be used in dangerous ways to achieve questionable goals. At the end of 1998, after a three year study of global organized crime, the US Center for Strategic and International Studies warned that computer crackers could cripple the nations power grids and military command and control systems.[1] And within two months, then President Bill Clinton proposed a $1.46 billion initiative designed to protect the US against cyber-terrorism.[2]

Argument 3: Cracking is not harmful and is educational

Some crackers argue that in the process they are learning abouut how to use computers more effectively. They argue that they do no real harm, that they just break into systems and look at the files without disturbing them. But this argument overlooks some real harm that can arise from mere cracking. (1) As mentioned above, there is the harm that individuals with ulterior motives can do with the knowledge and techniques that crackers develop and disseminate. (2) There is potential harm in outside activities taking place inside operating systems - these activities can slow the system and even interfere with its correct operation with possibly dire consequences. (3) There is the less well defined harm that is causes when privacy is violated. We might consider whether we would feel harmed, or invaded, if someone came into our room and looked around, through our drawers and papers and so on. If we feel there is some harm in this case then we may also feel there is harm in crackers simply looking through our files, and, say, our e-mail folders. It certainly does seem that we all have rights to privacy and that cracking is a violation of those rights. Finally (4) there is the possible harm that can be done in the process of discovering how to crack into the system - damage that can be done before the right proceedures are discovered.

As for the reputed educational aspects of cracking, it seems clear that there are better ways of learning computing than cracking. The usual methods of reading, listening to lectures, doing practical classes, solving problems, and working through learning programmes provides a much broader and more systematic kind of knowledge than the esoteric knowledge of specific details that the cracker needs. Even if cracking did provide a good education, that good would have to be balanced against the harm that is created by promoting the culture of cracking.

The *Computer Misuse Act 1990* became law in June 1990. The law created three new offences:

I. Unauthorised entry into a computer system, with a maximum penalty of £2,000 fine or six months' imprisonment (the Law Commission suggested a maximum penalty of only three months imprisonment)
II. Unauthorised entry with intent to commit or assist in serious crime, with a maximum penalty of five years' imprisonment and an unlimited fine (the Law Commission suggested a maximum penalty of five years' imprisonment)
III. Altering computer-held data or programs without authorisation, also with a maximum penalty of five years' imprisonment and an unlimited fine (the Law Commission again suggested a maximum penalty of five years' imprisonment)

The law is generalized in two important ways.[3]

1. The act extends these crimes to include (a) conspiracy to commit these crimes, and (b) incitement to commit them. This means that if a computer literate friend follows your suggestion that he might solve his financial problems by getting into a major bank computing system and transferring some money from a big account to his own, then you will have broken the law as much as he did.
2. The law includes offences where at least one 'significant link' is in the UK. Thus if the bank is in New York and the entry is from Cambridge (UK), or if the bank is in London and entry is gained from Cheyenne (WY) the law is violated. Even if the entry is into a New York bank from Cheyenne (WY), but is done via a link in Cambridge (UK) the law is still violated.

---

1 Center for Strategic and International Studies, *Cybercrime... Cyberterrorism... Cyberwarfare... : Averting An Electronic Waterloo*, Panel Report, November 1998, ISBN 0-89206-295-9.

2 <http://www.epic.org/security/infowar/clinton-infowar-199.html>

3 Discussed in Duncan Langford (1995), *Practical Computer Ethics*, McGraw-Hill.