VIRTUOUS HACKERS: DEVELOPING ETHICAL SENSITIVITY IN A COMMUNITY OF PRACTICE

Paula Roberts and Jenny Webber
University of South Australia
paula.roberts@unisa.edu.au

ABSTRACT

It is estimated that losses due to computer break-ins by malicious 'crackers' (who might be external intruders or disgruntled employees intent on personal gain or revenge) are costing companies billions of dollars each year. But former hackers are now assisting the computer security industry to track down such intruders, and to develop sound security practices in order to ward off future attacks. It is argued that in recent times computer programming has moved from a craft-based, bricolage activity to a scientific approach which has led to a knowledge gap developing between the former fraternity of hackers and the computer security industry. The current inadequacies of the security industry have made this co-operation with hackers necessary but problematic, that is, should hackers who have developed their unique skill by breaking into company and government systems now be used for the rightful purposes of strengthening computer security? However, this relationship might also suggest that the hacker ethos, which has developed through the membership of a 'community of practice', and which has as its cornerstone the moral custodianship of computers and the information they contain, may represent the best way of developing ethical practice in the computer industry.

INTRODUCTION

Some former hackers, the virtuosos from the heyday of thrill-seeking computer break-ins, are now assisting system operators to establish and maintain sound security practices by testing system vulnerability with their own specialized knowledge, thus helping to foil the activities of a minority of malicious, criminal hackers known as 'crackers'.

The size of the computer security problem is difficult to quantify, although some estimates suggest that, in the United States, it might amount to billions of dollars per year (Behar, 1997), or 'about 4% of the GNP in most industrialized nations ... (a)ccording to some Lloyd's underwriters and several confirming research studies' (Taylor, 1999: 75). These investigations take into account losses due to both external intrusion and internal sabotage by current employees. The motivation for such break-ins may have its origins in the technical challenge of breaching a company's information security, or the potential for personal gain, notoriety, revenge, or advancement of ideological beliefs.

The detection and prosecution of hackers has always been difficult because many companies who have been subject to security break-ins are oblivious to such damage. Other businesses which have detected breaches of their information systems, have chosen not to disclose such events, fearing public embarrassment and the commercial damage associated with a loss of consumer confidence if the weaknesses of their corporate computer systems are revealed.

In the United States an earlier government response to hacking was to introduce increasingly punitive measures for those few hackers who were detected and brought to account (Sterling, 1992: Roush, 1995), and to institute often unwinnable legal proceedings in efforts to establish public scapegoats in the hacker fraternity (Denning 1991; Sterling 1992). These court encounters were not successful in curbing hacking, but did provoke legal and ethical 'freedom of information' debates between those who argued for the privacy of information and others who supported free access to computer systems and their information (Denning 1991).

Behar (1997) notes that security issues have come into sharper focus as greater corporate dependence on e-mail and networks has been matched by increasing amounts of economic espionage from crackers. This increased vulnerability to attack has been paralleled by government requirements that companies take responsibility for keeping their own data secure, in the knowledge they will be held liable also for losses incurred by 'downstream' companies who are damaged by the host company's lax computer security.

In response to these developments, former hackers are now being enlisted by corporations and security companies to test the vulnerability of corporate information systems (Sprenger 2000). But the use of hackers, whose own penetration of computer systems has mostly been accomplished by stealth and in breach of the law, raises ethical issues, particularly the question of whether the seemingly unethical should lead the computing profession to a new-found ethical emphasis on computer security and the custodianship of information.

In response to this dilemma, it could be argued that the former hackers have an ethos that is grounded in the ethical use of computers. For example, for no apparent pecuniary gain, some hackers have spent large amounts of their own time in obsessively tracking down malicious intruders and bringing them to account for the damage they have caused not only to organizations but to the ethos of the former hacking fraternity (see Stoll, 1991; Shimomura, 1996). Both Stoll who pursued the German intruders, and Shimomura who tracked down the infamous Kevin Mitnick, have documented their individual quests which represent years of personal persistence in bringing these crackers to justice, in the face of denial and indifference from U.S. Defense Department

systems managers and the American F.B.I. Here is evidence of a hacker-based ethics, not imposed by professional codes of conduct, but one which is based on an intrinsic set of values and beliefs, inspired by an inherent respect for computers and the information they contain, and the abhorrence of those who do not share this respect.

This new stage in the folklore of hacking suggests a 'bottom-up' formulation of computer ethics that is based less on universal principles than on an ethical sensitivity which develops through the use of computers. This personal ethos indicates also the appropriateness of not an 'add on' approach in the teaching of computer ethics, but of an encouragement of a sense of moral responsibility for computer systems from the earliest stages of a student's use of computers (Roberts 1994; Roberts & Webber 1999).

There are parallels here in the training of artisans in pre-industrial times, a training embedded in a craftsman/apprentice relationship, which encouraged not only a transfer of skills but also the development and then guardianship of the ethos of the craft for future generations. Thus, contemporary computing 'apprentices' should be assisted in developing a moral sensitivity for the systems they use, and for the safety of the information which computers store. It could be argued that the remnants of the former hacker fraternity are revealing what computer ethicists may well have overlooked, that this sensitivity might best grow in a community of practice which has a common respect for the tools of the computer age.

The ethos of hacking: computing as a valued human practice

Levy (1984) and Roush (1995) describe an earlier generation of hackers who, from the 1960s, enjoyed stretching the capabilities of programmable systems, and who then moved on to penetrating corporate and academic computer systems with the aim of testing 'how far down the Establishment's electronic corridors they could creep before anyone would take notice' (Roush 1995:36). This first flush of hacking paled in later years with the growth of the Internet and electronic mail, when networking meant that if 'two or three sysadmins found out about an operating system hole or a common system weakness, pretty soon everyone who cared knew about it and plugged it' (Roush (1995: 36). At the same time law-enforcement crackdowns became an increasing deterrent to hackers who had outgrown the adolescent computing culture and had moved on to real-life concerns such as career and family responsibilities, making the risk of imprisonment for the sake of an ideal, a possibility which could no longer be contemplated.

Roush (1995) interviewed a number of present-day hackers and found they displayed a similar ethos to those former computer virtuosos whose 'common badge' was a sense of superiority to the bureaucrats whose systems they could so easily infiltrate. Likewise, Roush contends these new hackers are inspired by the thrill of unearthing system weaknesses, but they also set strict personal limits for their on-line adventures and hold in contempt those crackers who aim to damage a system and benefit from its vulnerability.

Roush reports that 'Knightmare', a member of this new hacker fraternity has, in his book *Secrets of a Super Hacker*, defined a 'set of ideals' which constitute an ethos of mature, 'responsible' hacking. This ethic is explained as 'never harming any computer, software, system or person, nor profiting from a "hack", but instead informing computer managers of their systems' weaknesses. Thus a 'true hacker' has 'the ability to steal money, information, software, and hardware and to commit sabotage and espionage, but chooses to do none of these things' (Roush, 1995:35).

In examining the evolution of this hacker ethos, it is interesting to consider how might this adolescent computing elite, (most often working in isolation and classed as 'loners'), have gained such a strong sense of community and group identity which would lead to a collectively formed set of values and ideals. It is likely that these commonly held beliefs grew from communication across the personal and electronic hacker networks and then became incumbent upon the members of the hacker fraternity. Thus an ethos grew which was intimately related to the specialized, high level computing expertise of these elites, and developed both from a personal desire for expertise, and from an obsessive love of computers.

Sherry Turkle, a professor of computing at the Massachusetts Institute of Technology, has studied the behaviour of undergraduate hackers in the MIT computer labs where they lived and programmed computers for 22 hours a day, unwashed and unhealthy, and giving every impression that 'machines had replaced people in their lives' (Turkle, 1988). However, this dark side of the hackers' craft of programming has been described elsewhere by Turkle and her colleague, Seymour Papert, as 'bricolage', that sensitive yet playful, hobby-like approach to gaining skill which is the mark of a true craftsman (Turkle & Papert, 1990). This passion for their computing craft was accompanied in these students by a contempt for government and corporate computer systems which, in the hackers' view, constituted a misuse of information technology by contradicting the constitutional rights of citizens in respect of the freedom of information.

Thus the hacker community's ethos has reflected both an intrinsic desire to preserve and extend its own conduct and expertise, and an external motivation to attack and expose the vulnerability of institutionalized computer data systems. This latter motivation is based on a passionate distaste for private data stores, and an ideal of the

public freedom of information; beliefs which hackers, and their advocates, have defended in the courts (Denning 1991).
Arnold (1997: 14-15) discusses the concept of sport as a valued and virtuous human practice which involves membership of a community and the development of a group identity. His analysis is useful in understanding both the evolution and the virtue of the hackers' ethos. Arnold argues that, despite sport's 'more recent perverted and unsavoury connections' ... '(w)hen sport is pursued for its own sake, its rules willingly followed and its finest conventions upheld, sport becomes an enobling and worthwhile form of life'.
Blum (1994: 146) (cited in Arnold 1997: 15) discusses the relationship between virtue and community in the writings of MacIntyre (1984: 10) and argues that virtues can only be learned and sustained in a community of practice. Thus, the ethics of virtue are not seen as an alternative to the ethics of universality, but as complementary, that is, while based upon universal ethical principles the commonly held views of the practice community are indigenous and characteristic to its particular activities. Furthermore, 'a practice, like a profession, is characterized as much by the way its participants conduct themselves as in the skills they develop and the purposes to which they are committed'.
Thus, if hacking is perceived by hackers as an elite practice, with internal goals and standards which are pursued in a moral way for their own sake, then a member of the hacking practice-community would be expected to only ever apply their elite technical expertise to responsible hacking, and not to malicious hacking. Members would also be required to track down and expose deviates (crackers), who by their behaviour were damaging both the integrity of the practice-community, and the wider society.

The hacker crackdown

Sterling (1992: xiii) documents government attempts to curb hacking which in 1990 involved 'a nationwide crackdown on illicit computer hackers, with arrests, criminal charges, one dramatic show trial, several guilty pleas, and huge confiscations of data all over the United States'. The 'show trial' to which Sterling referred was the United States vs. Craig Neidorf legal proceedings against the hacker, Neidorf, which are detailed by Dorothy Denning (1991). Denning is a professional cryptographer and computer security expert who had for some time studied the hackers of the digital underground from an anthropological perspective. In this research, according to Sterling (1992: 286), Denning discovered that

> these computer-intruding hackers, who had been characterized as unethical, irresponsible, and a serious danger to society, did in fact have their own subculture and their own rules. They were not particularly well-considered rules, but they were, in fact, rules. Basically, they didn't take money and they didn't break anything.

Denning was engaged by Neidorf's defence team as an expert witness in a trial which set out to find a public scapegoat in the hacker fraternity and which charged Neidorf with '10 felony counts carrying a maximum penalty of 65 years in prison' (Denning, 1991: 26). The Neidorf case was as much about constitutional rights of freedom of speech as it was hacking, and involved charges brought against Neidorf's electronic newsletter, *Phrack*, in which details of the Bell telephone system had been published.
It was subsequently proved that the Bell information was not classified, and, in fact, was freely available to consumers, and, in this regard, *Phrack* did not give away any secrets. The charges that *Phrack* was also a primer for breaking into computer systems were also shown to be false, as Denning was able to point to other publications, for example Stoll's 1991 publication, which gave much more explicit information about systems' entry. The case against Neidorf collapsed on the third day, but although Neidorf was freed of all criminal charges, the trial cost of $100,000 was incurred by him and his family (Denning, 1991: 28).
One outcome of the trial was the establishment of the Electronic Frontier Foundation whose aim is the protection of constitutional rights within the electronic media. However, as Denning cautions, all published data carries with it the need for legal and ethical judgement, particularly

> 'in the case of hacker publications (where) the majority of readers are impressionable young people who are the foundation of the future. Articles which encourage illegal break-ins or contain information obtained in this manner should not simply be dismissed as proper just because they are protected under First Amendment rights' (Denning, 1991: 31).

Further outcomes of the hacker crackdown were the individual national legislative procedures such as the U.K. Computer Misuse Act, which established punitive measures for a range of hacking offences, including the introduction of viruses. However, with so far no international agreement on legislation, and the unlikely possibility of enforcement of such legislation, as the *Love Bug* virus incident in 2000 showed, malicious or foolhardy hacking is not likely to be contained by legislative procedures alone.

Sleeping with the enemy: the digital underground and the computer security industry

Roush (1995: 38) argues that as computer-related crime is growing more sophisticated, more varied, and more costly to society, information-security experts and law-enforcement agencies need to turn to the expertise of 'good' hackers as a significant knowledge source to assist their attempts to stem the onslaught of destructive computer intrusions.

Taylor (1999) contends that the computer security problem is more complex than simply recruiting hackers. Firstly the vulnerability of current computer systems is due in great measure to the neglect by academia and industry of research and development in computer security. In particular, security flaws, (and the reasons they are not eliminated) reflect the gulf between programming's expectations and its achievements. Crackers, taking advantage of this situation, are simply using trivial holes left by inexperienced programmers who were not taught the limitations of computer systems. In academia. where computer security is under-theorized apart from cryptography, the situation now is 'like teaching how to fly airplanes but not teaching pilots that engines sometimes fail', (Cohen, in Taylor 1999:87).

Also under-valued by industry and academia is practical knowledge of the vulnerability of computer systems, wisdom gained only by hands-on experience and experimentation. As computing has evolved from a craft culture to a scientific reliance on standardized procedures, deficiencies in computer security and software development have made apparent the problems caused by this change from a 'craft' to a 'scientific' approach in the education of computing personnel. The scientific approach emphasizes a formal design methodology and internal consistency that aims to prove the efficacy of a program at the design stage, while the craft approach, (typical of the attitudes towards computing of the early creative, if less-than-disciplined, hackers) is more attuned to the realities of the software's ultimate use.

The departure from a craft approach may have contributed to marginalizing hackers away from a core of influence in computing as industry has moved to more rigorously researched knowledge, but the spurning of the hackers' potential contribution to computer security may relate also to a developing ethical sensitivity within the industry. Whilst the knowledge of the early hackers was once valued despite its doubtful methods of acquisition, what was then accepted in the academic pursuit of knowledge appears to be no longer tolerable in the present-day academic or commercial environments of computing. A mainstay of the hacker ethos is that information should be free, and therefore illicit access to computer systems is not inherently wrong, but others question the ethics of this hacker activity, for example, Thompson (1984: 763) argues 'the acts performed by these kids are vandalism at best and probably trespass and theft at worst'.

However, others contend that the likelihood of harm from the hackers is exaggerated, and is outweighed by their potential to provide useful information about security weaknesses. For example, Kapor (1991), Murray (1992) and Spafford (1992) argue for the ethical, instrumental value and use of the hackers' experience, particularly their knowledge of the psychology of crackers and other computer felons which will aid the security industry and thereby bring great benefits to society.

These opposing views are reflected in enduring arguments at various levels, ethical and practical, which are common to information ethics in general, and are matters on which academia, industry and society are yet to reach a set of agreed standards. Because of such disputes, Stichler (1998: 180) notes that information ethics, has at times become moribund. In similar vein, MacIntyre (1984: 6) has argued, 'It is precisely because there is in our society no established way of deciding between these claims that moral argument appears to be necessarily interminable... Hence perhaps the slightly shrill tone of so much moral debate'.

Stichler (1998: 179-180) provides a pointer useful to the hacker issue:

> in the debate over the ethics of information distribution, utilitarian positions focus on maximising social benefits and tend to favour a market system based on private ownership; while deontological positions focus on the right to information access and tend to favour a more socialistic system emphasising equality of distribution and public ownership. In cases where rights conflict, where one person's (or corporation's) intellectual property rights conflict with another's right to access, deontologists often have no convincing way of deciding the right course of action and are thus forced to fall back on utilitarian considerations as the only practical means of reaching a decision.

For the argument in this paper, it is useful to return to MacIntyre (1984) and his discussion of the virtues, particularly its application for an understanding of the virtues of the good hacker community. MacIntyre argues that 'the essential function of the virtues is clear. Without them, without justice, courage and truthfulness, practices could not resist the corrupting power of institutions' (1984: 194).

The origins of the activity of hacking itself stem from the craft-like, bricoleur quality of programming, and it is the hackers' holistic approach to computing which explains hacking's lasting appeal to subsequent generations (Taylor, 1999:88). The fundamental disagreement over the implications of the craft aspects of hacking is one of

the underlying factors in the dispute between the digital underground and the computer security industry, and, at the same time, the strongest reason why hacking is likely to survive in some form or another, even as programming develops towards more science-based methods.

More important still is hacking's contribution to an applied computer ethics which is based not only on universal principles but which has, as its cornerstone, a moral respect for computers and their information, which grows as computing expertise develops. This dichotomy mirrors the skills/ethos base of the craft guilds of pre-industrial times, which was handed down to future generations through the craftsman/apprentice relationship. This is a strong argument for an integrated approach to the teaching of computing ethics in mainstream computing subjects (Roberts, 1994; Roberts & Webber, 1999), so that as a skill develops it is accompanied by a growing moral sensitivity for the social responsibility that skill also entails.

CONCLUSION : HACKING - VISIONS OF A NEW COMPUTER ETHICS?

The titles of two early, but still prominent, primers on hacking, Levy's *Hackers, Heroes of the Computer Revolution* (1984) and Sterling's *The Hacker Crackdown* (1992) reflect the changing attitudes towards hackers over this period. From a former tolerant acceptance of adolescent precocious computing skill, attitudes hardened with an awareness in the late 1980s and early 1990s of the sinister threat to computer systems posed by a more recent development in hacking, the actions of malicious crackers. However, law enforcement and its increased penalties for hacking have proved ineffectual and very few cases of illegal computer entry are detected or reported.

Almost ten years after the publication of Sterling's book, the computing profession and society are still faced with the ethical dilemma of whether the hackers' unique knowledge of the vulnerability of computing systems (which has been gained by the seemingly unethical acts of system break-ins) should be harnessed by the computer security industry for the common good.

Obviously, there is no easy theoretical solution to this quandary. However, in practice, former hackers are now working to halt computer crime by joining forces with the security industry (see, for example, Sprenger, 2000). These efforts may not yet bring about public respectability for the hacker fraternity, but the hidden value of the hackers' personal ethos, which values computers and their ethical use, may provide the substance for a new computer ethics which transcends professional codes and guides the general computer user. This appears society's best hope in limiting the damage and cost of malicious computer break-ins.

REFERENCES

Arnold, P.J. (1997) **Sport, Ethics and Education**, London: Cassell.

Behar, R. (1997) 'Who's reading your e-mail'. **Time**, February 3, 64-67.

Blum, L.A. (1994) **Moral Perception and Particularity**. Cambridge: Cambridge Univ Press.

Denning, D.E. (1991) 'United States vs Craig Neidorf: A debate on electronic publishing, constitutional rights and hacking'. **Communications of the ACM**, Vol. 34, 3:24-32.

Kapor, M. (1991) 'Civil liberties in cyberspace: When does hacking turn from an exercise of civil liberties into crime?' **Scientific American**, September.

Levy, S. (1984) **Hackers: Heroes of the Computer Revolution**. Harmondsworth: Penguin.

MacIntyre, A.C. (1984) **After Virtue: A Study in Moral Theory**, 2nd Edn. Notre Dame: Notre Dame University Press.

Murray, W. (1992) 'On computer security and public trust' in T.W. Bynum, W. Maner, & J.L. Fodor, (eds.) **Teaching Computer Ethics**. New Haven, CT: Research Center on Computing and Society.

Roberts, P.M. (1994) 'The place and pedagogy of teaching ethics in the computing curriculum' **Australian Educational Computing**, May.

Roberts, P.M. & Webber, J. (1999) 'Visual Truth in the Digital Age: Towards a Protocol for Image Ethics' **Australian Computer Journal**, Vol. 31, 3: 78-82.

Roush, W. (1995) 'Hackers: Taking a byte out of computer crime'. **Technology Review**, April: 32-40.

Shimomura, T. (1996) **Take-Down: The Pursuit and Capture of Kevin Mitnick, America's Most Wanted Computer Outlaw - By the Man Who Did It**. New York: Hyperion.

Spafford, E.H. (1992) 'Are computer hacker break-ins ethical? **Journal of Systems Software**. 17:41-47.

Sprenger, P. (2000) 'Tiger teammates, hacking bright' **Information Age**, August/Sept: 32.

Sterling, B. (1994) **The Hacker Crackdown: Law and Disorder on the Electronic Frontier**. Harmondsworth, UK: Penguin.

Stichler, R.N. (1998) 'Ethics in the Information Market'. In R.N. Stichler & R. Hauptman (eds.) **Ethics, Information and Technology Readings**, pp.169-183. Jefferson, NC: McFarland & Co.

Stoll, C. (1991) **The Cuckoo's Egg**. New York: Doubleday.

Taylor, P.A. (1999) **Hackers: Crime in the Digital Sublime**. London: Routledge.

Thompson, K. (1984) 'Reflections on trusting trust'. Turing Award Lecture. **Communications of the ACM**. Vol. 27, 8: 761-3.

Turkle, S. (1988) 'Computational reticence: Why women fear the intimate machine'. In C. Kramarae, (ed.) **Technology and Women's Voices**. New York: Routledge & Kegan Paul.

Turkle, S. & Papert, S. (1990) 'Epistemological pluralism: styles and voices within the computer culture'. **Signs: Journal of Women in Culture and Society**, Vol. 16, 1.