Dissecting the 'Hacker Manifesto'

S.M.Furnell, P.Dowland and P.W.Sanders

Network Research Group
School of Electronic, Communication and Electrical Engineering
University of Plymouth
Plymouth
United Kingdom

e-mail : sfurnell@hotmail.com

Abstract

Twelve years ago, a text was written within the hacking community which is widely referred to as the 'Hacker Manifesto'. This text, and the opinions that it offers, have since been widely embraced by the hacker community and the document is referenced from numerous sites on the Internet. This paper sets out to examine the content of the Manifesto and considers the validity of many of the messages that it imparts. The Manifesto is considered to present an undoubtedly pro-hacker message, without acknowledging other perspectives or the wider implications of the activities that it is advocating. The paper explores some of these issues, examining both the consequences of the Manifesto's dissemination and ways in which security professionals and society at large should respond. It is concluded that whilst the Manifesto obviously cannot bear the sole responsibility for promoting and encouraging hacker activity, it at best sends out an incomplete message that should be balanced with appropriate counter-argument.

Keywords : Hackers, Computer Abuse, Information Society.

Introduction

The definition of the term 'hacker' has changed considerably over the last 30 years. In the 1960s, hackers were the dedicated software and hardware gurus, and the term largely referred to persons capable of implementing elegant / technically advanced solutions to technologically complex problems. In the 1990s, however, the moniker implies something rather different and is commonly used to refer to persons dedicated to entering systems by identifying and exploiting security weaknesses. At the extreme are a subset (often distinguished by the term 'crackers') who perform openly malicious actions upon the systems they enter, such as deleting files, modifying data and stealing information. Such activities would be frowned upon by the traditional hackers from the 60s.

Modern-day hackers are one part of a so-called Computing Underground (Mizrach, 1997). This is something of a catch-all term, which encompasses a number of sub-groups that would generally be classed as undesirable by society at large. These include the aforementioned crackers, phreakers (who actively explore and/or control the telecommunications networks), virus writers and software pirates.

This paper considers the principles from which many hackers operate and the justifications that are often presented for their actions. Significant reference is made to the so-called ‘Hacker Manifesto’, which encapsulates many of their beliefs and is widely available within the hacker community.

The Hacker Manifesto

A popular element of hacker culture is a brief text entitled “The Conscience of a Hacker”, which is more widely known and referred to as the ‘Hacker Manifesto’. This was written in 1986 by a hacker who operated under the pseudonym of ‘The Mentor’ and who was a member of the notorious hacking group the Legion of Doom (Sterling, 1992). The full text is reproduced in figure 1.

> **The Conscience of a Hacker**
>
> by
> +++The Mentor+++
> Written on January 8, 1986
>
> Another one got caught today, it's all over the papers. "Teenager arrested in Computer Crime Scandal", "Hacker Arrested after Bank Tampering"... Damn kids. They're all alike.
>
> But did you, in your three-piece psychology and 1950's technobrain, ever take a look behind the eyes of the hacker? Did you ever wonder what made him tick, what forces shaped him, what may have molded him? I am a hacker, enter my world... Mine is a world that begins with school... I'm smarter than most of the other kids, this crap they teach us bores me... Damn underachiever. They're all alike.
>
> I'm in junior high or high school. I've listened to teachers explain for the fifteenth time how to reduce a fraction. I understand it. "No, Ms. Smith, I didn't show my work. I did it in my head..." Damn kid. Probably copied it. They're all alike.
>
> I made a discovery today. I found a computer. Wait a second, this is cool. It does what I want it to. If it makes a mistake, it's because I screwed it up. Not because it doesn't like me... Or feels threatened by me... Or thinks I'm a smart ass... Or doesn't like teaching and shouldn't be here... Damn kid. All he does is play games. They're all alike.
>
> And then it happened... a door opened to a world... rushing through the phone line like heroin through an addict's veins, an electronic pulse is sent out, a refuge from the day-to-day incompetencies is sought... a board is found. "This is it... this is where I belong..." I know everyone here... even if I've never met them, never talked to them, may never hear from them again... I know you all... Damn kid. Tying up the phone line again. They're all alike...
>
> You bet your ass we're all alike... we've been spoon-fed baby food at school when we hungered for steak... the bits of meat that you did let slip through were pre-chewed and tasteless. We've been dominated by sadists, or ignored by the apathetic. The few that had something to teach found us willing pupils, but those few are like drops of water in the desert.
>
> This is our world now… the world of the electron and the switch, the beauty of the baud. We make use of a service already existing without paying for what could be dirt-cheap if it wasn't run by profiteering gluttons, and you call us criminals. We explore... and you call us criminals. We seek after knowledge... and you call us criminals. We exist without skin color, without nationality, without religious bias... and you call us criminals. You build atomic bombs, you

> wage wars, you murder, cheat, and lie to us and try to make us believe it's for our own good, yet we're the criminals.
>
> Yes, I am a criminal. My crime is that of curiosity. My crime is that of judging people by what they say and think, not what they look like. My crime is that of outsmarting you, something that you will never forgive me for.
>
> I am a hacker, and this is my manifesto. You may stop this individual, but you can't stop us all... after all, we're all alike.
>
> +++The Mentor+++

Figure 1 : The 'Hacker Manifesto'

The Manifesto is still widely accessible, some twelve years after it was originally written. Ordinarily, this could be considered no great feat for a piece of literature. However, it is possibly more significant in the context of the technology field, where the pace of change frequently renders once leading edge thoughts obsolete after a few years. In fact, the Manifesto probably has wider exposure now than it did at the time that it was written. A search on the WWW yields numerous links to sites reproducing the text. Indeed, a search for the term "hacker" followed by "manifesto" yielded more hits than a search for "orange book" followed by "security" (560 versus 173 hits[1]). For the uninitiated, the Orange Book is the name commonly used to refer to the US Department of Defence Trusted Computer Systems Evaluation Criteria, a significant publication in the IT security field which was published at roughly the same time as the Manifesto (DOD, 1985). This crude example suggests that the hacker perspective is more widely available than specific security guidelines. In addition, the Manifesto has found its way into other forms of media outside the WWW. For example, segments from it have been quoted in the 1995 film "Hackers" (MGM, 1997). As such, the text cannot be easily dismissed as being merely the thoughts of one person and the material is worthy of further examination.

Dissecting the Manifesto

When reading the text of the Manifesto, the first thing that is clear is that it is not using the term 'hacker' in its original, 1960s sense, i.e. the system and coding gurus as described, for example, by Levy (1984). The perspective is instead that of persons gaining unauthorised access to computer systems (i.e., the modern, mass media definition). That said, however, the Manifesto only presents a restricted view of a hacker – as largely a curious explorer, pursuing knowledge and/or intellectual challenge. Fundamentally, however, even unauthorised exploration of a system is equivalent to trespassing and may still result in a breach of commercial confidentiality or personal privacy. Parallels are frequently drawn between cyberspace and the physical world (e.g. discussion of concepts such as 'community' occur in both contexts). If such comparisons are applied to notions such as property and privacy, it is clear that the incursions that some hackers would argue to be acceptable online would not be so easily justified in the real-world equivalent. For example, we could draw a parallel between an individual's web site and his/her home, or between a

[1] Results from Infoseek search conducted on 31 August 1998 using the search terms specified.

company's site and its high-street office or showroom. The hacker ethic would state that unauthorised entry into the system running such a WWW server would be acceptable as long as no damage is done. However, no one would be likely to be very tolerant of an intruder offering such excuses if found exploring in their home or office. Regardless of whether you agree with its sentiments, the views laid out in the Manifesto contradict the law in many countries. It would, for example, breach the section of the UK Computer Misuse Act relating to "Unauthorised access to computer programs and data" (HMSO, 1990).

The defence that a hacker may not set out to intentionally damage a system is actually a convenient over-simplification of the issue. Actions may have an unintentional / indirect impact that is not foreseen by the hacker. Many do not know in advance the nature of the systems that they are trying to penetrate or the tasks that they are performing (indeed, part of the challenge may be to find out). However, in a worst-case scenario, the mere presence of a hacker could result in undesirable consequences (e.g. degradation of system performance such that essential operations are not completed quickly enough - which could be potentially fatal in a real-time, safety critical system).

The Manifesto also overlooks the fact that some systems / information may be protected from the general populous for good reason. There is a strong argument, for example, that military systems should incorporate sufficient security in order to prevent casual users from being able to browse or modify their contents. If everyone were to be allowed unrestricted access, then this would implicitly include potentially undesirable or dangerous groups, such as terrorist organisations. Therefore, if society were to insist that all IT systems should be totally open, organisations such as the military would effectively be prevented from putting a great deal of their information online for fear of the potential consequences. Military and defence related sites, such as the US Air Force and the Pentagon, have actually proven to be an attractive target to hackers, with numerous incidents reported in the general media (Ungoed-Thomas, 1998). A standard defence in such cases is often simple curiosity rather than some more sinister purpose. However, the sharing of knowledge is one of the underlying principles of the hacker community and, as such, even if the hacker effecting the break-in chooses not to use the information irresponsibly, others who gain access through him/her may not be so reliable.

Moving on from the debate about simple exploration, a substantial body of evidence is available to prove that various other motivations frequently prevail. Examples include financial gain, espionage, malice / revenge or general mischief. Therefore, even if the "harmless exploration" proposition is accepted as one potential motivation, security is still required to ensure protection against these other cases.

Another motivation stated in the Manifesto is to enable the free use of services that would be "dirt cheap" were they not run by "profiteering gluttons". The main parties referred to here are telecommunications service operators, who provide the basic infrastructure through which hackers (and other users) are able to connect to remote systems. The observation that services could be cheaper may well be valid in some cases, especially where a key player is able to exploit a monopoly position. However, over time, market forces (primarily the emergence of competition) or legislation often redress the balance and result in charges being reduced to a more realistic level. By contrast, the activities of hackers are more likely to provoke a response solely in respect of the breach of security. As an aside, it may be observed that in the meantime, the hackers / phreakers are paying *nothing* for the service. Therefore, even if it eventually was to become “dirt cheap”, it is debatable whether many would be willing to depart from this desirable situation (their moral justification for not paying could then maybe switch to “We have the skills to avoid paying, so why should we need to?”).

The Manifesto frequently repeats the phrase “They’re all alike”. However, evidence suggests that this is far from the case – from the perspective of both their motivations and intellectual capabilities. For example, throughout the text there is an implicit assertion of intellectual superiority on the part of the hacker and of being misunderstood and generally failed by society on this basis. Whilst many hackers *are* undoubtedly intellectually gifted, competent problem solvers and lateral thinkers, this categorisation cannot be applied across the board. Furthermore, choosing to be a hacker does not automatically endow you with these characteristics. Many hackers succeed through sheer persistence, determination and, in many cases, an exceptionally high boredom threshold. A successful hack is often the result of doggedly attempting to apply the same technique to multiple systems until a weakness is found. Furthermore, unwitting assistance is often provided by system administrators, who have left their systems vulnerable to attack through inadequate attention to, or understanding of, security. Such circumstances are apparent in most of the hacker “case studies” that have been documented in the popular media (Stoll, 1989; Freedman and Mann, 1997).

The last paragraph includes the statement that “you can’t stop us all”. Depending upon ones interpretation, this has a rather menacing undertone and does not offer much reassurance that subscribers to the Manifesto represent a benign community. Based purely upon the text of the Manifesto, this particular inference may be seen as overstating the case and it could be argued that the Mentor intended a less threatening interpretation to be made. However, a further observation can be added which perhaps adds weight to the first proposition. Web sites that reproduce or link to the Manifesto frequently include links to other related materials as well. It has been observed by the authors that another text that sometimes shares “link space” with the Manifesto is the ‘Terrorist’s Handbook’ (Anonymous, 19xx). On this basis, it can be inferred that the two texts are considered to be of interest to a similar audience (at the very least, they both interest the creators of the various web sites on which they appear together). Such an association does not help the image of the hacker community, but it is nevertheless an interpretation that is open to be made by the casual web surfer.

Returning again to consider the Manifesto in isolation, it can be observed that it does offer some very positive views (e.g. advocating anti-racism and anti-war messages). However, you do not have to be a hacker in order to adopt these beliefs. Furthermore, the aforementioned assertion of intellectual superiority represents an attitude which itself could create a prejudicial society of a different type. Additionally, what the text plainly does not advocate is an anti-crime viewpoint. It is interesting to note that the seventh paragraph accuses society of cheating and lying, with the implicit interpretation to be made that such activities are incompatible with the hacker ethos. This, of course, tends to ignore the fact that many of the methods used by hackers to gain unauthorised access to systems, or their activities once having done so, would not be considered by most people to be fair and honest (e.g. deceiving people into parting with passwords via social engineering; planting Trojan Horse programs to enable data gathering or provide a backdoor).

Nowhere in the text does it make a statement about where to draw the line or where even hacker activity would be considered to be going too far. This has certainly been addressed / recognised in other hacker-originated material which, whilst emphasising themes such as free access to information, also advocates more responsible attitudes such as not inflicting intentional damage upon systems and not operating for personal financial gain. However, the promotion of such values does not always accompany the Manifesto and, therefore, many people will not receive the complete message.

Consequences of the Manifesto

The Manifesto cannot be criticised from the perspective of some of the general sentiments that it expresses – there are undoubtedly many parties who genuinely hold these beliefs (e.g. the Mentor). However, the problem is that the general dissemination of the text serves to invite and excuse a wider population. For example, it excuses people whose activities are conducted with complete disregard for their impact upon other individuals (e.g. breaching personal privacy or causing financial loss), by enabling them to convince themselves that their actions are compatible with the manifesto or a wider counterculture.

Despite hacker's motivations and justifications, their activities are not welcomed by society at large and their endeavours can be seen to cause measurable damage to organisations and individuals. For example, in the UK, the national Audit Commission conducts regular surveys into the levels of computer crime and abuse observed in various sectors (including, amongst others, healthcare, local government, manufacturing, financial institutions and retailing). The most recent results (Audit Commission, 1998) show that hacking accounts for around 11% of reported incidents, from a total of 510 incidents reported in 870 survey responses. These incidents were considered to have cost a total of £360,860 to the organisations involved. As an aside, the figures for both incidents and cost are more than doubled if other categories of malicious abuse, such as viruses, are also considered. The hacking incidents occurred across a variety of domains, with local government, healthcare and education representing the organisations most affected. One thing that is clear from this is that hacker activity affects more than just the aforementioned "profiteering gluttons". Indeed, domains such as healthcare often have difficulty in ensuring sufficient funding to satisfy demand for provision of their core services and can consequently do without the need to divert money and resources away from these to overcome security breaches.

Another basic problem that we perceive with the Manifesto is that it can create a negative impact of the implications arising from information technology when, at the same time, we are living in a society in which our dependency upon IT is only increasing. Furthermore, there are numerous additional opportunities that are being offered by IT that have the potential to improve or simplify our existing practices. An example of this is the area of electronic commerce (or e-commerce). This represents a significant area of interest within the industry at the time of writing and various opportunities have been identified. However, there are still a number of barriers (both practical and conceptual) that must be overcome before e-commerce will be widely embraced by mainstream business or private individuals and two of the greatest concerns are security and privacy (Ratnasingham, 1998). This can be illustrated using the example of credit card purchases, a form of commerce that is one of the most easily migratable to the online context, but also one where a great deal of concern over security has been expressed (Partridge, 1997). Now, in actual fact, the use of credit cards over the Internet may be no less secure than the uses to which they are put in other scenarios. Most of us think nothing of providing credit card details over the telephone or handing over the card itself to strangers serving us in shops or restaurants. However, all of these activities expose our accounts to risk and, indeed, fraud and abuse are known to occur (Hill, 1998). Nevertheless, the Internet is still perceived to be much less secure, and a likely reason for this is the public perception of hacker activity resulting from the level of exposure that it has been given in the mass media.

Indirectly, however, it could also be claimed that hacking activity, and the fear it engenders (well founded or not), does deliver some benefits. Using the credit card example again, it can be observed that concern over security has led to the development of the Secure Electronic Transaction (SET) standard, for secure credit card transactions over the Internet (SETCo, 1997). The ultimate adoption of such technologies should mean that Internet commence will actually be more secure than current practices.

Another area in which it may be argued that hackers are providing a service is when their activities are conducted in the context of ‘penetration testing’, authorised by the owners of a system in order to test its security. In this form of ‘ethical’ hacking, the work is often carried out by ‘tiger teams’ who break into systems and then explain to the systems operator how the hack was achieved and, where appropriate, the means by which the security hole can be ‘plugged’. These services are considered to be attractive by numerous organisations and it has even been speculated that US Department of Justice has looked to recruit hackers in order to conduct penetration tests on its networks (SECURE Computing, 1998). However, it is difficult to argue that this represents a genuinely positive contribution by hackers – if they did not exist at all, the penetration testing service would not be needed either.

Responding to the Manifesto

All of the above discussion leads to the obvious question of what can be done? The authors view is that we cannot, and should not, try to prevent the Manifesto’s dissemination. This would simply represent censorship, which would contradict not only any notion of a “hacker ethic”, but also more widely held public beliefs regarding freedom of information and individual choice. A more rational way to respond is by making the alternative point of view equally visible, without presenting it in such a heavy-handed manner as to imply “Big Brother” overtones. In short, there is a need to present a positive view of the information society, emphasising the need for trust and co-operation. Without this, development and progress will be stifled.

There are also a number of wider aspects to which consideration should be given. The first is in relation to the way that hackers are portrayed in the media and the resultant influence that this has upon public perception. Hacking is regarded by many as a glamorous occupation. The idea of an underground movement of amateur "criminals" breaking into computer networks, reading secret files and removing all traces of their presence may have a certain appeal. The media frequently portrays hackers in a different light to those who commit obviously malicious crimes. For example, the 1983 film "Wargames", in which the hacker is portrayed as a hero despite the potentially disastrous consequences of his actions. If the media is to adopt this stance, then there is rather less of a basis for future condemnation in cases where hacking activity causes damage of some kind.

It was observed earlier that the Manifesto includes a strong thread of intellectual superiority and, indeed, in respect of the school system, includes the following quote: "I'm smarter than the other kids, this crap they teach us bores me…". This is a potentially significant point in the sense that society has a general tendency to normalise people (preferring to recognise similarities rather than differences) and those falling outside the societal norms are often difficult to accommodate. Educational systems are often a good example of this, generally focusing upon meeting the needs of the 'normal' children, with the result that those with abilities significantly above or below the average sometimes receive inappropriate or insufficient support. If individuals feel disenfranchised by society, then it is not entirely surprising that they choose not to accept / respect the societal norms. Unfortunately, this point is far easier to recognise than it is to resolve.

Perhaps the most appropriate response is in terms of awareness. This may be considered from two perspectives. Firstly, is ensuring awareness of the Manifesto to persons outside the hacker community - not in the sense of encouraging them to adopt it, but to highlight the point that there are people who have. More important, however, is to ensure an awareness of the need for IT security and the appropriate ways of protecting a system. Significant resources are available in this respect (e.g., in terms of documentation, software and specialist services to assist with implementation), but there are still many systems in which security is overlooked or assigned a low priority. Unlike the issues of changing media and educational attitudes, these objectives are achievable at the organisational level, putting them within the reach of senior management to address. Whilst having to protect a system against hackers would not be necessary in an ideal world, it is one of the many realities of our IT-oriented society and is better faced than ignored.

Conclusions

This paper does not intend to imply that the Hacker Manifesto should bear the sole responsibility for promoting and endorsing hacker activity. Hacking occurred before the text was written and has developed in probably unforeseen ways since. Furthermore, there have been other, higher profile, contributions that have also presented hacking / the hacker in a positive light. However, the fact that the material suggests itself as a manifesto (i.e., something for a wider population to adopt and adhere to) means that its ultimate impact may be more profound.

The paper has not considered other widespread forms of computer abuse, such as viruses. These, of course, had not really been conceived when the Manifesto was written. It is interesting to conjecture whether, if they had been, they would have received endorsement or denunciation. It is certainly the case that virus writers have subsequently justified their own actions in similar terms, viewing them as a statement against a society that they disagree with or as a simple means of electronic experimentation and self-expression (i.e., ignoring the resultant damage inflicted upon others).

Much of the discussion in this paper has presented an intentionally bleak view, focusing on worst-case scenarios and outcomes in many cases. As such, it may be considered by some to be exaggerating and overstating the problems. However, the authors do not believe this to be the case and many of the sources referenced provide sufficient evidence of the points raised. Furthermore, a negative view is a necessary response to the Hacker Manifesto, which presents its perspective in a manner oblivious to many of the wider issues.

References

Anonymous. 19xx, *The Terrorist's Handbook*. Available on Internet / WWW.

Audit Commission. 1998. *Ghost in the Machine – An Analysis of IT Fraud and Abuse*. Audit Commission Publications, UK. February 1998. ISBN 1-86240-056-3.

DOD. 1985. *Trusted Computer System Evaluation Criteria*. DOD standard 5200.28-STD, December, 1985.

Freedman, D.H. and Mann, C.C. 1997. At Large : The strange case of the World's biggest Internet invasion. Simon & Schuster, New York. ISBN 0-684-82464-7.

Hill, D. 1998. "Stop card thieves taking off", *The Sunday Times*, Money, 19 July 1998: 3.

HMSO. 1990. *Computer Misuse Act 1990*. Her Majesty's Stationary Office, UK. ISBN 0-10-541890-0.

Levy, S. 1984. *Hackers : Heroes of the computer revolution*. Anchor Press / Doubleday.

Mizrach, S. 1997. "Is there a Hacker Ethic for 90s Hackers?". http://www.infowar.com/hacker/hackzf.html-ssi.

MGM. 1997. *Hackers*. Homepage at http://mgmua.com/hackers/

Partridge, C. 1997, "Credit card fraud hits the Internet", *The Times*, Interface Supplement, 26 November 1997.

Ratnasingham, P. 1998. "The importance of trust in electronic commerce", *Internet Research* 8, no. 4: 313-321.

SECURE Computing. 1998. “US Justice Hires Hackers”, *SECURE Computing*, September 1998: 16.

SETCo. (1997), “SET Secure Electronic Transaction Specification - Book 1: Business Description”, Version 1.0. 31 May 1997. http://www.setco.org/set_specifications.html

Sterling, B. 1992. *The Hacker Crackdown*. Penguin Books Limited, London. ISBN 0-14-017734-5.

Stoll, C. 1989. *The Cuckoo’s Egg*. Pan Books Limited, London. ISBN 0-330-31742-3.

Ungoed-Thomas, J. 1998. “The schoolboy spy”, *The Sunday Times*, News Review, 29 March 1998: 1-2.