

Abstract

The purpose of this thesis is to explore some of the ways in which a particular technological artifact may or may not be said to be "value-laden." Specifically, I intend to examine the software features and documentation for several different computer network scanning programs. I shall argue that at least three different (and frequently conflicting) value systems are active within the computer security software community, and that particular features of scanning software serve some of those values (but not others.) I shall then hone in on one particular piece of software, and demonstrate that the attempt of the software developer to negotiate between these conflicting value systems results in a piece of software in which a tension (and possible identity crisis) is evident. As such, I shall conclude that the particular artifact at hand is not value-neutral; nor can it be said to possess or serve any *one* value. Rather, the software may lend itself toward the articulation and exhibition of frequently conflicting and inconsistent value systems, sometimes simultaneously. This is not, however, testament to its neutrality: different pieces of software are more easily asserted toward certain goals than others. Attempts at simplifying this "value-laden-ness" to any single value system (or to assert value-neutrality) shall be demonstrated to fail – or at least not to do adequate justice to the complexity of the artifact.

The Technology

The technology that I propose to examine is computer network scanning software. This software is used by individuals to probe a computer (or network of computers) for security vulnerabilities. The software connects to the designated target host(s), and returns to the user a detailed list of services running on the target(s), the versions of those services, and possible means of exploiting those services in order to gain access to the target system(s). For instance, I may point the network scanner at a particular web site, and the software will tell me that the site is a Microsoft Windows 2000 server running an unpatched version of Microsoft's Internet Information Server version 5.0, which is vulnerable to a particular type of hacking attack. In one sense, the software has a single purpose – to collect security information and to return that information to the user. In another sense, it has at least a dual purpose. The same piece of software that serves hackers in collecting information vital to breaking into computer systems is also used by system administrators to inform them about possible vulnerabilities in the systems which they are responsible to protect. The same tool is used to provide the same information about the same target, but by different users with different intentions for the use of that information.

The historical development and software capabilities of individual network scanning programs reflect this dual purpose. Development of such tools has proceeded roughly equally within "black hat"¹ hacker groups and "white hat" security firms. Still more

¹ Within the security software community, "black hat hackers" typically refers to individuals who experiment with network and software security with malicious intent. "White hat hackers", on the

interestingly, the two often borrow technology and information from one another, and individuals frequently switch sides or attempt to remain somewhere in the middle. Today's hackers are often tomorrow's security consultants, and they routinely take their technology with them when they make the switch. Even the names of the software packages reflect the tension. The SAINT™ software package is a registered trademark (and for-purchase product) of the SAINT Corporation (“SAINT™ Introduction” 2003), and is built upon an older software package called SATAN (possibly the first comprehensive network scanning tool), which was open source code developed by hackers and released to the world at large (“What SATAN Is” 1985). The basic functionality between SATAN and SAINT™ has remained the same; the interface, feature set, and rhetoric have changed. Like the individuals who make the switch from being criminals to being consultants, the software code itself can be made to “switch sides” without any corresponding change in technical purpose or functional design.

The Competing Value Systems

1) **Dominant Morality (V1)** – By "dominant morality", I mean both our intuitive sense of right and wrong, and "traditional" philosophical moral theories. It may seem rash to conflate the two, but I do so intentionally and with what I propose are good reasons. The emphasis in both "common" morality and moral philosophy is usually on categorizing human actions in terms of moral and immoral behavior.

other hand, are those who look for vulnerabilities with the intent of repairing them (sometimes for profit, sometimes not). As with the hacker/cracker distinction (discussed later), the “white/black hat” distinction is more often used by the “white hats” to distinguish themselves from their law-breaking counterparts than the other way around.

Here, we determine the value of actions with regard to being "right" or "wrong". For instance, most of the published literature on computer ethics takes a normative approach to the moral issues in human uses of computer technology. Volumes such as those produced by Johnson (1994), Forrester and Morrison (1994), Hester (2001), Parker (1979), and Spinello (2001) have overwhelmingly focused on human moral responsibility and its relation to the uses of computers and computer network technology.

The approach to values and technology in V1 is what I shall label "external": the philosopher looking from the outside in; starting from a foundation containing a moral value system, and then applying that value system to a set of technologies. Most moral philosophers do not talk about the technology itself having value(s), but rather about the values involved in what human beings *do* with the technology. This seems to coincide well with most people's everyday intuitions about technology and values.

- 2) **The "Hacker Ethic" (V2)** – The so-called "Hacker Ethic" (articulated most prominently by authors such as Pekka Himanen and Manuel Castellas in *The Hacker Ethic* (2001) and *Rise of the Network Society* (2000), respectively) is "ethics" in a different sense than that which is typically used by moral philosophers. Like the "Protestant work ethic", it is perhaps better described as a value system. The "hacker ethic" values activity not exclusively (nor even primarily) with regard to a morality of right and wrong, but rather with regard to

"the spirit of informationalism" (Castellas 2000). In the "hacker ethic", the free spread and sharing of information is perhaps the key value, followed closely by the value of elegant technical problem-solving. (One of the rallying cries of V2 is that "information wants to be free.") The hacker who subscribes to V2 sees great value in solving interesting problems, and may consider the moral consequences of solving such problems to be of secondary importance to creating beauty – defined loosely as technical elegance in problem-solving. This ethic is not entirely without a sense of social responsibility, but it is a diffuse responsibility to the network community, and not to governing structures or dominant moralities. Freedom and personal autonomy are highly valued by V2; technologies that are decentralized and protect anonymity and personal privacy are favored over those that serve a central authority (i.e., open-source development is preferable to proprietary corporate development, encryption technologies should be developed and distributed without government interference, etc.) The political analog is somewhere between Libertarianism and self-organizing anarchism.

I shall label the approach to values and technology in V2 as partly "internal" and partly "external". By this I mean that the "hacker ethic" grounds at least part of its value system within the elegance of the technology itself, independent of what people may choose to *do* with the technology. An effectively-written computer virus may be seen as an evil product by the dominant morality, but the subscriber to the "hacker ethic" is just as likely to admire the program as a technical feat. While V2 may be quite willing to admit people shouldn't release viruses into the

wild because of their moral consequences (the external component of value shared by V1), the admiration of the cleverness of the technology itself is nonetheless present (the internal component). The subscriber to the hacker ethic would be much less prone than the moral philosopher to suggest that we shouldn't *write* viruses, because doing so may be a fascinating and educational technical exercise, regardless of its possible negative moral consequences.

3) **The "Cracker Ethic" (V3)** – While more properly called an alternative "hacker ethic", I shall call this the "cracker ethic" for the sake of distinction.² The cracker ethic contains an amalgam of the "Yippie" and punk-rock disdain for (and open rebellion to) authority, the anarchist-activist opposition to authority precisely *because* it is authority, and an extreme form of the hacker ethic (V2) that completely discards V1, considering it a tool of the exploitive ruling majority.³ The emphasis on the value of technical elegance and competence from V2 is maintained; the skilled hacker who develops her own tools gains considerably

² The hacker/cracker distinction and terminology is not of my own creation, and itself has a rich and fascinating history. Those who call themselves "hackers" by nature of the fact that they engage in solving interesting technical problems but not in illegal activity typically refer to the criminal, system-compromising, underground hacking participants as "crackers". The "cracker" label is intended to associate those who break into computers with "safe crackers" and other unsavory criminal elements, and to distance the self-labeled "hackers" from those elements. The "crackers", in an interesting rhetorical move, typically refuse the distinction, claiming that what they do is no different from what the "hackers" do when they create software, experiment with hardware, and otherwise pursue "purer" intellectual pursuits within the technical realm. As such, it is rare to find "crackers" willing to label themselves as such. See, for example, the interview with the hacker group called Cult of the Dead Cow published on the Linux/UNIX enthusiast website Slashdot ("Bizarre Answers" 1999).

³ This is not to say that all crackers engage in illegal activity for idealistic political goals, although many do. In fact, the majority of crackers (pejoratively labeled "script kiddies" by the wider hacking world for their uncomprehending use of pre-packaged, scripted hacking tools) participate in system cracking as little more than a form of electronic vandalism. Nonetheless, even this vandalism is done with a clear disdain for authority and its prescriptive morality.

more community status than the hacker who simply employs those tools or achieves success through brute-force attacks. Because of the illegal nature of most V3 activity, published citations are rare, except on the Web itself, where sources and rants on ethics are plentiful. (See, for example, "The Hacker Manifesto" (Mentor), "A Hacker Manifesto [version 4.0]" (Wark), others.)

I shall label the relationship between values and technology in V3 as primarily "internal": most of the participants in V3 are almost entirely obsessed with the technology itself, with little concern for "appropriate" or "inappropriate" use. V3 seldom bothers to look "outward" from the technology at all, except in search of targets. The value of a technology lies entirely in the elegance of its method and in its technical abilities to overcome other (opposing) technologies, and the value of individuals (and the corresponding respect accorded to them) lies in their abilities to create and manipulate those technologies and technological systems. There are those in the cracker community who participate in "political" hacking, which does seem to engage in some values other than the immediately technological; however, I would contend that those individuals are the minority, and that most would be participating in non-political hacking, were their political causes to be satiated.

The Project Proposal

While ethics V1, V2, and V3 have certain areas of overlap (at least in that they all serve as value systems of some sort), they are in tension or direct conflict with one

another in many aspects. This tension manifests itself quite prominently in computer security software; particularly, much of the software used to scan computer networks for security flaws displays a fascinating identity crisis. The rhetoric presented in the documentation of most network scanning software describes the software as a network auditing tool for system administrators, in order that they may better secure their own networks. In fact, many system administrators use the software for exactly that purpose. However, there are also features within much of the software that seems irrelevant or even counter to its stated purpose. For instance, scanners such as Nmap (“Quality Security Tools” 2003), in addition to having the capability to probe a computer or network, also have the capability to mask the source address of the machine performing the scanning. Other scanners provide the capability to tunnel through network firewalls, or otherwise circumvent standard security measures. While these features may be justifiable under the rationale that "more information is better", they also clearly serve the interests of illegal system crackers.

I propose to conduct a close examination of such software, as to explore the ways in which V1, V2, and V3 play often-conflicting roles during the design and development processes. The idea is not to determine how such software "should" look from any normative stance. Rather, the idea is to determine why a particular piece of software *does* look the way that it does, and what value systems contributed to its design and function. This should require not only an understanding and explication of the value systems involved (which sociology and computer ethics have already accomplished adequately), but also an understanding of the technology itself, and of what its

technical aspects can tell us about its design ethics and assumptions (which has been lacking in the philosophy of computer ethics thus far.)

In approaching the topic, I will borrow heavily from the methodologies of social historians of technology: in particular, the approaches of authors such as Winner (1986), Bijker and Pinch (1987), and Mitchum (1994). I will provide a survey of both the historical development of such software and the rhetoric surrounding it, in order to ascertain why current software looks the way it does. My approach will also be partly technical: I intend to focus on one or two particular programs, and to scrutinize their features and documentation in detail. Finally, my approach shall be partly philosophical: I will examine human values as commuted from a developer to a user by way of a technological artifact, and will explore the ways in which those values conflict or find harmony within the artifact itself, through an analysis of the software's features and the value system(s) which those features seem to serve.

I will conclude my thesis with a discussion of the question of the "value neutrality" of artifacts, using network scanning devices as my case study. I intend to demonstrate that this particular class of artifacts cannot be said to be value neutral; neither can they be said to "contain" or serve any single value system. Instead, they are often an expression of a conflict of values. In so demonstrating, I intend to invoke and vindicate Melvin Kranzberg's First Law: "Technology is neither good nor bad, nor is it neutral" (Kranzberg 1986).

Outline

I. Introduction and Overview of Project

- A. Thesis
- B. Literature Review

II. Explication of Competing Ethics

- A. Traditional Ethics
- B. Hacker Ethic
- C. Cracker Ethic

III. A Brief History of Scanning Software

- A. History of the Technologies
- B. History of the Rhetoric

IV. Are Values "Contained" in the Technology?

- A. Software Anatomy and Feature Dissection
- B. Relation of Features to Value Systems

V. Conclusion

Bibliography

- “@stake Research Labs Overview.” @stake, Inc. <<http://www.atstake.com/research>>.
- Barbour, Ian. *Ethics in an Age of Technology*. San Francisco: HarperCollins, 1993.
- Berleur, Jacque, and Klaus Brunnstein. *Ethics of Computing: Codes, Spaces for Discussion and Law*. London: Chapman and Hall, 1996.
- Bijker, Wiebe, Thomas Hughes, and Trevor Pinch, eds. *The Social Construction of Technological Systems*. Cambridge: The MIT Press, 1987.
- “Bizarre Answers from Cult of the Dead Cow.” *Slashdot* 22 Oct. 1999
<<http://interviews.slashdot.org/article.pl?sid=99/10/22/1157259&mode=thread>>
- Bowyer, Kevin, ed. *Ethics and Computing: Living Responsibly in a Computerized World*. Los Alamitos: IEEE Press, 1996.
- Bowyer, Kevin, ed. *Ethics and Computing: Living Responsibly in a Computerized World*. 2nd ed. New York: IEEE Press, 2001.
- Bynum, Terrell, Walter Manner, and John Fodor, eds. *Computing Security*. New Haven: Research Center on Computing and Security, 1992.
- Castellas, Manuel. *Rise of the Network Society*. Oxford: Blackwell Publishers, 2000.
- Denning, Dorothy, and Herbert Lin, eds. *Rights and Responsibilities of Participants in Networked Communities*. Washington: National Academy Press, 1994.
- Edgar, Stacey. *Morality and Machines: Perspectives on Computer Ethics*. Sudbury: Jones and Bartlett Publishers, 1997.
- Feenberg, Andrew. *Questioning Technology*. New York: Routledge, 1999.
- Forester, Tom, and Perry Morrison. *Computer Ethics: Cautionary Tales and Ethical Dilemmas in Computing*. Cambridge: The MIT Press, 1990.
- Forester, Tom, and Perry Morrison. *Computer Ethics: Cautionary Tales and Ethical Dilemmas in Computing*. 2nd ed. Cambridge: The MIT Press, 1994.
- “The Hacker's Ethics.” *The Cyberpunk Project*.
<<http://project.cyberpunk.ru/idb/hacker%5Fethics.html>>.
- Hester, D. Micah, and Paul Ford, eds. *Computers and Ethics in the Cyberage*. Upper

- Saddle River: Prentice-Hall, 2001.
- Himanen, Pekka. *The Hacker Ethic and the Spirit of the Information Age*. New York: Random House, 2001.
- Johnson, Deborah. *Computer Ethics*. 2nd ed. Englewood Cliffs: Prentice-Hall, 1994.
- Kaempf, Michel. "Re: Ethics." *Archives de lorraine*. 27 Nov 2000
<<http://www.via.ecp.fr/via/ml/lorraine/200012/msg00004.html>>.
- Kranzberg, Melvin. "Kranzberg's Laws." *Technology and Culture* 27 (1986): 544-560.
- MacKenzie, Donald, and Judy Wajcman, eds. *The Social Shaping of Technology*. 2nd ed. Buckingham: Open University Press, 1999.
- Mentor, The. "The Hacker Manifesto."
<<http://www.via.ecp.fr/via/ml/lorraine/200012/msg00004.html>>
- Mitcham, Carl. *Thinking Through Technology*. Chicago: University of Chicago Press, 1994.
- McClure, Stuart, Joel Scambray, and George Kurtz. *Hacking Exposed: Network Security Secrets and Solutions*. Berkeley: McGraw-Hill, 1999.
- "Nessus." 2003. <<http://www.nessus.org/>>
- Parker, Donn. *Ethical Conflicts In Computer Science and Technology*. Arlington: AFIPS Press, 1979.
- Pitt, Joseph. *Thinking About Technology: Foundations on the Philosophy of Technology*. New York: Seven Bridges Press, 2000.
- "Quality Security Tools." *Insecure.org*. <<http://www.insecure.org/tools.html>> 2003.
- "SAINT Introduction." *SAINT Corporation*. <<http://www.saintcorporation.com/cgi-bin/doc.pl?document=intro#what-is-saint>> 2003.
- Sassower, Raphael. *Technoscientific Angst: Ethics & Responsibility*. Minneapolis: University of Minnesota Press, 1997.
- Spinello, Richard, and Herman Tavani, eds. *Readings in Cyberethics*. Sudbury: Jones and Bartlett, 2001.
- Teich, Albert, and Mark Frankel, eds. *The Use and Abuse of Computer Networks: Ethical, Legal, and Technological Aspects*. Washington: American Association

for the Advancement of Science, 1994.

Thomas, Douglas. *Hacker Culture*. Minneapolis: University of Minnesota Press, 2002.

Vidstrom, Arne. "Ethics and My Tools." *NTSecurity.nu*.
<<http://ntsecurity.nu/toolbox/ethics2.php>>.

Wark, McKenzie. "A Hacker Manifesto [version 4.0]."
<http://subsol.c3.hu/subsol_2/contributors0/warktext.html>

"What SATAN Is." <<http://www.fish.com/satan/>> 1985.

Winner, Langdon. *The Whale and the Reactor*. Chicago: University of Chicago Press, 1986.

"Worst Case Scenario." *Cult of the Dead Cow*.
<<http://www.cultdeadcow.com/tools/>>.