The Information Assurance Ethics Dilemma

Kevin Krause and Dr. Mario A. Garcia
Texas A&M University
Corpus Christi, Texas, USA

Abstract

Information assurance focus is on one of the three major tenants: confidentiality, integrity, and availability. Undertakings in each have indeed improved the overall security of current information systems. This research seeks to promote Information Assurance ethical awareness. A brief discussion on ethics and moral development along with related works of Plato, Aristotle, Kant and Mill will follow a report on the current conditions and challenges to our profession. Ethical case studies were developed by examining a limited collection of infamous actions implemented in the name of information assurance. By understanding the past, the goal is to produce a literary tool kit that can lead to ethically sound decisions in the development of future security systems.

1. Introduction

As rational beings, humankind has always had the uncanny ability to process and store information from the surroundings. With acquired knowledge, humans have created tools to manage their environment. Rotblat [1] calls this process the power of "original thinking" and that the acquisition this power has greatly accelerated the process "natural evolution."According to Kurzweil [2], each "epoch" progresses more rapidly because it is built on advancements introduced in the previous. Oortmerssen [3] suggests that Darwin's evolutionary theory of the survival of the fittest is augmented by progressive development. None the less, Brattain [4] states that, "*the scientists and technologists*," of humans proper societal role. According to Bynum [5], Donn Parker of SRI International in Menlo Park, California alleged "*it seemed that when people entered the computer center they left their ethics at the door*." For Watson [6], however, it boils down to a matter of trust between computer professionals and the communities in which they serve. "*The general public often does not understand technology, they put their trust in those who provide it*," Watson maintains. Rapalus [7] reported "most hack attempts are perpetrated by juveniles on joy-rides in cyberspace."Accordingly, the 2002 CSI/FBI Computer Crime and Security Survey [7] reported 74% of all computer crimes were conducted through an Internet connection. The number of Internet crimes had doubled from 1996 levels. Although the survey only had 25 respondents who could quantify their financial losses, their cumulative loses reached a staggering $459,755,245.00. To Power [8], the survey confirmed that threats from computer crimes and information security breaches continue to be "unabated and that the financial toll is mounting."

Lenarcic [9] emphasizes software complexity is far beyond the cognitive bounds of any one individual and that a single simple error can "peculate" through an entire system with devastating results. Brooks and Vutsinas [10] claim attacks on the information infrastructure are attractive because of low cost, high profile, large effect, ease of implementation, and difficulty to trace. Moreover, Endicott-Popovsky [11] noted the perceived anonymity on the Internet fuels one's willingness to break the law. Leiwo and Heikkuri [12] suggest misuse of technology can be modeled and defer to the four component MOMM model proposed by Carroll [13]. The MOMM components are Motive, Opportunity, Means, and Method and each one is readily enabled in cyberspace. Finally, Schumacher and Welch [14], citing the rapidly evolving treats and complexity of networks, have suggested that there will never be a

"silver bullet" technical solution. Threat models, according to Brown and Laurie [15], have to assume a powerful adversary, one with access to all communications links and insecure data and systems.

As Schumacher and Welch [14] report, Defense Advanced Research Projects Agency (DARPA) research has demonstrated that defenses are much more effective when they include planning from the attacker's point of view. Likewise, Schumacher and Welch as well as others such as Brooks and Vutsinas [10] include references from the 4th century B.C. book, *Art of War* by Sun Tzu, in their discussions about information assurance. Fundamentally, Tzu taught that in confrontation; one must know their enemy.

2. The Information Assurance Education Dilemma

By applying Tzu's advice, many effective information assurance curriculums now include attack tools and methodologies. While recognizing the mastery of such materials could be open to misunderstanding, Brooks and Vutsinas [10] argue that to do otherwise would be useless. Endicott-Popovsky [11] maintains that many students who find this discipline to be exciting and interesting must also learn the serious side of this subject along and have a thorough understanding of the serious consequences for misguided behavior. Schumacher and Welch [14] concur by calling for ethical considerations when teaching this potentially dangerous knowledge. Leiwo and Heikkuri [12] have acknowledged that ethics should be an important facet of comprehensive information assurance education. As a result, Zlatarova [16] suggests students sometimes graduate with little or no knowledge of the ethical precepts required to cope with many of the everyday cyberspace tribulations. Lenarcic [9] attributes this to the fact that many IT curricula found at the university level are awash in excessively procedural subjects that often pander to the era's commercial fashions. Dudley-Sponaugle and Lidtke [17] insist the reluctance to teach ethics either as a standalone course or as a module within another course is because most computer science faculty have had little or no ethical background or training. According to Watson [6], ethical dilemmas seldom have black or white solutions; often the solutions are shades of gray without a single right or wrong answer leaving engineers to search for their best personal solution. Finally, Payne [18] contends that a common mistake among those without specific training in ethics to assume that ethics is somehow intuitive.

3. Ethics Defined

Leiwo and Heikkuri [12] maintain the purpose of ethics is twofold. First, it is to find criteria to distinguish between good and bad. And secondly, ethics aims to promote good desires and discourage bad ones. Yet, according to Lenarcic [9] ethics is not to be confused with dogmatic morality or legalistic absolutes. So, just what does it mean to be ethical? Many great minds have tackled this old question. The nineteenth century philosopher John Stuart Mill belabored this fact in his paper *Utilitarianism* (reprinted by Burtt [19]). Mill wrote: "*After more than two thousand years the same discussions continue, philosophers are still ranged under the same contending banners, and neither thinkers nor mankind at large seem nearer to being unanimous on the subject, than when the youth Socrates listened to the old Protagoras*."

Popkin and Stroll [20] explain that in classical ethics attempts are made to answer one or both of two basic questions: "*What is the good life for people?*" and "*How should people act?*" Clearly, the answers to these questions are open to interpretation and, as a result, two main ethical camps have emerged. They are the objectivists and the relativists. According to Weckert and Adeney [21], objectivists believe moral truths hold the "good" independently of one's likes or dislikes, whereas relativism can be viewed as either "cultural" or "moral" relativism. Cultural relativism, as they explain means "*moral values are relative to the particular culture of the society that accepts them*" and that moral relativism is "where moral judgments seek neither approval nor disapproval from one's culture or society, but rather, it comes from oneself" [21]. Regardless of one's ethical position, people have to make a choice when faced with an ethical dilemma. There are three modes to ethical analysis: **Normative ethics** - development and justification of rules; **Ethics of virtue** - questions of personal character; and **Social ethics** - how society supports or is affected.

Leiwo and Heikkuri [12] maintain that there two basic approaches to ethical analysis. Accordingly, the deontological approach where rules pertaining to what should or should not be done are predefined and followed, and the consequential approach where merit is based on the outcome instead of the action. According to Leiwo and Heikkuri [12], information security specialists tend to the deontological. Deontological ethics states that there are

things that should be done and things that should not be done. Virtue is seen as an end of ethical activities. Finally, Watson [6] provides the following list that should be taken by engineers to prepare for ethical dilemmas. The list which can be applied to computer science and the sub disciplines of information assurance and security include: **Understand** the basics of engineering ethics; **Review** personal values associated with engineering ethics; **Develop** awareness of ethical concerns; **Learn** to identify early signs of ethical situations; and **Apply** engineering principles to determine appropriate solutions.

4. Four Philosophers

Dudley-Sponaugle and Lidtke [17] have indicated that there is neither an agreed upon group of ethical theories are consistently used nor can all theories be presented in teaching computer ethics. Accordingly, the focus of this discussion is limited to the views of Plato, Aristotle, Kant, and Mill as presented by Popkin and Stroll [20].

For Plato, (c. 427 BC – c. 347 BC), finding "the good" was an intellectual quest. Plato believed the good was like mathematical principles which exist independently from mankind. That is, no matter how hard we try to prove otherwise; the absolute principles of 2 + 2 will always produce 4. Like math, Plato was convinced the good only provided the one and only right answer. Plato firmly believed that once someone discovered and truly understood the nature of the good, that person would never again commit an evil act. Thus to benefit society, Plato urged for all young people to study the good, especially the youth of the ruling classes.

Aristotle, (384 BC – 322 BC), was one of Plato's more notorious students. However, Aristotle had problems accepting the absoluteness of the good. Through his studies, he made two observations about what is the good life for mankind: 1.) the good life consisted of the things which made us happy and 2.) no two people ever achieved happiness in exactly the same way. From this, Aristotle deduced that right action for any given situation had to be as unique as the person committing the act. To accommodate his intellectual position, Aristotle proposed the "Golden Mean" which states that the right action for one to choose was actually one of the many possible right actions falling in between extreme actions and that the action chosen would be the one best suited for the individual making the choice. He also advocated the youth to develop virtuous habits early so that they may be better prepared to exercise the Golden Mean later in life.

Jumping ahead 2,000 years, we find Immanuel Kant, (1724 – 1804). Certainly, there were several other ethical theories proposed between the time of Aristotle and Kant; however, Kant sensed a societal need for a strict and well defined moral guidance. Since Kant believed in the free will of all individuals, he also believed that people had the freedom to determine their own actions and they were individually responsible for the actions they chose. Thus, he said it was people's duty or obligation to always conduct ourselves in the right way despite any desire to do otherwise. To help people make the right decisions, Kant introduced "the categorical imperative." The categorical imperative had two parts. First, it mandated people to choose an action that could become a universal law. Accordingly, certain activities such as lying and stealing would never be committed because a universal law based on these activities could never be established. A second feature of the categorical imperative stipulates that one should never impede another's free will as a means to an end.

Shortly after Kant, the "greatest good" principle was developed by John Stuart Mill, (1806 – 1873) and others. In his *Utilitarianism* (reprinted by Burtt), Mill declared Kant's work as "a landmark in the history of philosophical speculation." However, Mill and the utilitarian movement sought to separate one's action from one's underling motives by determining the virtue of any action from the consequences. They believed the best action was the one which would provide the greatest good for the greatest amount of people. Therefore, an immoral action could be justly committed if it provided more good than taking an alternate moral action [19].

Leiwo and Heikkuri [12] report that hackers have used Plato to justify their motives. Accordingly, hackers tend to see themselves as searchers of something more than knowledge akin to the following Plato passage reprinted by Russell [22]: "*A philosopher is a lover of wisdom. But this is not the same thing as a lover of knowledge, in the sense in which an inquisitive man may be said to love knowledge; vulgar curiosity does not make a philosopher*."

5. Use Cases

According to Zlatarova [16], "discussing case studies by analyzing and judging appropriate real and imaginary situation is very helpful because of the strong impression and influence left by the concrete example of human behavior and associated consequences offered in the considered case." Lenarcic [9] likens case studies to "the ancient art of storytelling in the guise of parables reminiscent of Aesop and his progeny."

The goal of using cases, Herreid [23] claims, is to teach process rather than content in order to develop higher-order learning skills. By providing a limited ethics theory background, the study of ethical cases appeal to the students own experiences, a central tenet of the "constructivist" teaching approach. According to Huitt [24], advocates of a constructivist approach suggest that educators should create a curriculum that can expand and develop the students' already existing knowledge and experiences with new learning. Certainly university level students should possess some preconceived notions of right and wrong. None the less, Endicott-Popovsky [11], after reviewing the 2002 CSI/FBI report, note that teens are committing the majority of computer crimes and speculates that many information assurance students are more than likely to have had previously indulged in questionable computer activities. Cases come in many forms and not all cases are created equally [25].

Mindful that a good case can be based on either real or imaginary facts, the following example case is based on a factual "Napster" case presented by Spinello [26] in the book *Case Studies in Information Technology Ethics*. The case entitled "The day that the music died" is split into three main parts. Part one sets the scene and introduces the fictional characters Ann, Bob, David, and Mallory who are college students with a vested interest. Part two tells the Napster story and part three presents the recording industry's point of view and reviews their lawsuit against Napster. Each part is followed by a series of questions whose themes range from case facts to ethical considerations with the intent to force critical thinking. Finally, end notes supply the final outcome, references from Spinello's original work, and ethical map.

6. Conclusion

The above observations provide evidence that in computer society, information is greased. It moves like lightning and will have application and reapplications that are impossible to imagine when initially entered in to computer field. Ethical policies for the use and distribution of information must take into account the social nature of information, even as they recognize the legitimate claims of the producers which give basis for considering the interest of the rest of society, in addition to those of the developers. Dispute occurs in every human endeavor and yet progress is made. Computer ethics is no different in this regard. If we naively regard the issues of computer ethics as routine or, even worse, as unsolvable, then we are in greatest danger of being harmed by computer technology. Because the computer revolution now engulfs the entire world, it is crucial that the issues of computer ethics be addressed on a global level.

7. References

[1] J. Rotblat, "Science and Humanity in the Twenty-First Century" (September 1999). Available from http://nobelprize.virtual.museum/nobel_prizes/peace/articles/rotblat/index.html (Visited Oct. 25, 2006)

[2] R. Kurzweil, "Kurzweil's Law" (Jan. 3003). Available from http://www.kurzweilai.net/meme/frame.html?m=10 (Visited Oct. 25, 2006)

[3] G. Oortmerssen, "The future – everybody and everything connected." Progress in Informatics, No. 3, 2006, 1-3.

[4] W. Brattain, Abstracts of remarks by panelists at 1968 Region 6 Conference: Impact of technology on mankind. *IEEE Region 6 Conference* (25-27 May 1977). Available from http://ieeexplore.ieee.org/iel4/5782/15429/00721085.pdf?arnumber=721085 (Visited Oct. 25, 2006)

[5] T. Bynum, " Computer ethics: basic concepts and historical overview." *The Stanford Encyclopedia of Philosophy (Winter 2001 Edition).* Available from http://plato.stanford.edu/archives/win2001/entries/ethics-computer/. (Visited October 16, 2006)

[6] J. Watson, "Ethics for engineers falls in an unstructured gray zone." *IEEE Potentials* (July/August 2006), pp. 14 – 16.

[7] Computer Security Institute. Cyber crime bleeds U.S. corporations, survey shows; financial losses from attacks climb for third year in a row (April 7, 2002). Available from http://www.gocsi.com/press/20020407.jhtml;jsessionid=NMCNMMSSPFDMEQSNDLOSKHSCJUNN2JVN?_requestid=292700. (Visited September 23, 2007.

[8] R. Power, 2002 CSI/FBI computer crime and security survey. *CSI Computer Security* (Spring 2002), pp. 1 – 22.

[9] J. Lenarcic, "The dinosaur and the butterfly: a tale of computer ethics." *IEEE Security and Privacy* (September/October 2003), pp. 61 - 63.

[10] R. Brooks, and C. Vutsinas, "Kafka in the academy: a note on ethics in IA education." *IEEE Security and Privacy*, (July/August 2006), pp. 50 – 53.

[11] B. Endicott-Popovsky, "Ethics and teaching information assurance." *IEEE Security and Privacy* (July/August 2003), pp. 65 – 67.

[12] J. Leiwo, and S. Heikkuri, "An analysis of ethics as foundation of information security is distributed systems." *System Sciences, 1998., Proceedings of the Thirty-First Hawaii International Conference on*, (Jan. 6 – 9, 1998), pp. 213 – 222.

[13] J.M. Carroll, "A portrait of the computer criminal." In *IFIP TC11 11th International Conference of Information Systems Security*, 1995.

[14] J. Schumacher, and D. Welch, "Educating leaders in information assurance." *IEEE Transactions on Education* (May 2002), pp.194 - 201.

[15] I. Brown, and B. Laurie, "Security against compelled disclosure." *Computer Security Applications, 2000. ACSAC'00. 16th Annual Conference*, (Dec. 11– 5, 2000), pp. 2 – 10.

[16] F. Zlatarova, "Incorporating ethics in computing courses and extra class activities." *34th ASEE/IEEE Frontiers in Education Conference* (October 20 – 23, 2004), pp. S1E/6–S1E/9 vol. 3.

[17] A. Dudley-Sponaugle, and D. Lidtke, "Preparing to teach ethics in a computer science curriculum." *Technology and Society, 2002. (ISTAS"02). 2002 International Symposium on* (June 6 - 8, 2002), pp. 121- 125

[18] D. Payne, "Engineering ethics and business ethics: commonalities for a comprehensive code of ethics." *IEEE Region 5, 2003 Annual Technical Conference* (April 11, 2003), pp. 81 - 87.

[19] E. Burtt, "*The English Philosophers from Bacon to Mill.*" Random House, Inc., New York, NY, 1967.

[20] R.H. Popkin, and A. Stroll, "*Philosophy Made Simple*." Second Edition, Doubleday, New York, NY, 1993.

[21] J. Weckert, and D. Adeney, "*Computer and Information Ethics*." Greenwood Press, Westport, CT, 1997.

[22] B. Russell, "*History of Western Philosophy.*" George Allen & Unwin Ltd., 2nd Edition, 1961.

[23] C. Herreid, "What makes a good case? Some basic rules of good storytelling help teachers generate student excitement in the classroom." *Journal of College Science Teaching*, (Dec.1997/Jan.1998), pp. 163 – 165. Available from http://ublib.buffalo.edu/libraries/projects/cases/teaching/good-case.html. (Visited July 30, 2006).

[24] W. Huitt, "Constructivism. *Educational Psychology Interactive*." Valdosta, GA: Valdosta State University. Retrieved March 9, 2006 from http://chiron.valdosta.edu/whuitt/col/cogsys/construct.html

[25] C. Herreid, "Case studies in science: a novel method of science education." *Journal of College Science Teaching*, (Feb.1994), pp. 221 – 229. Available from http://ublib.buffalo.edu/libraries/projects/cases/teaching/good-case.html. (Visited July 30, 2006).

[26] R. Spinello, "*Case Studies in Information Technology Ethics*." Second Edition. Person Education, Inc., Upper Saddle River, New Jersey, 2003.