Pedagogical Framework for Ethical Development

Melissa Dark
Purdue University, USA

Richard Epstein
West Chester University, USA

Linda Morales
Texas A&M University, USA

Terry Countermine
East Tennessee State University, USA

Qing Yuan
East Tennessee State University, USA

Muhammed Ali
Tuskegee University, USA

Matt Rose
Purdue Univeresity, USA

Nathan Harter
Purdue University, USA

INTRODUCTION

The Internet has had an enormous impact on society. The benefits are numerous and so is the potential for misuse and abuse. Hacking, spam, denial-of-service attacks, identity theft, digital rights infringement, and other abuses are now commonplace. Malice and criminal intent motivate some of these attacks, yet for others the motivation is not so clear.

An attacker may feel a need to prove a particular cleverness or technological skill. An attacker may view a particular vulnerability as a challenge that cannot be resisted. An attacker may desire revenge against a corporation or private individual, or may view the downloading and sharing of copyrighted software, movies, and music to be a personal "right." An attacker may be motivated by a dare from fellow hackers. Other motivations undoubtedly exist.

The ubiquity and openness of the Internet require self-governance; however, we see that the ethical maturity of Internet users is often put to the test. Curricula struggle to integrate ethics education in meaningful ways. Relevant professional associations have recognized the need to integrate ethics into computer science and information technology curricula (ACM, 2001; ACM/CS-IEEE, 2001, 2004; IEEE-CS/ACM Joint Task Force, n.d.) and have developed codes of ethics for computing and engineering professionals (ACM, 2001; IEEE, 2001; IEEE-CS/ACM Joint Task Force, n.d.). The problem has certainly been recognized in the information security community, where ethical judgments are needed on a regular basis. Information security programs are rapidly growing. Are these academic programs equipped to nurture the ethical development of information security students?

The teaching of ethics is fundamentally different from the teaching of science and technology. Pedagogical approaches need to be purposefully selected to facilitate the creation of educational opportunities that allow students to examine their personal ethical beliefs. This needs to be done against the broader explicit context of right and wrong engendered by the existing technical, professional, legal, and cultural environment. The goal of this article is to present a pedagogical framework for such ethical development in information security.

SUBJECT AREA FRAMEWORK

We have developed a pedagogical framework to help those who teach information security ethics to conceive their course structure and delivery in a manner that allows students to explore their personal moral beliefs and development. The discussion that follows assumes that information security ethics are arranged by topic, for example privacy, digital rights, and intellectual property. The framework examines information security ethics from four dimensions: the ethical dimension, the security dimension, the solutions dimension, and the personal moral development dimension. The four dimensions are not rigid compartments nor are they on a continuum. Instead, the four dimensions are loosely bounded areas that describe existing attempts to address ethical issues in information security. There are technical solutions that attempt to enforce ethical

Copyright © 2008, IGI Global, distributing in print or electronic forms without written permission of IGI Global is prohibited.

issues, just are there are legal solutions, cultural norms and expectations, and professional codes of conduct and expectations. Sometimes these solutions overlap or interact with one another. We think it is important that students examine the nature of the solution, contemplate that solutions can be differing in nature, and also analyze the sufficiency of such solutions. A discussion of how this framework can be used to teach topics in information security ethics is found in Dark et al. (2006).

The Four Dimensions

The Ethical Dimension

The ethical dimension explores the ethical ramifications of a given information security topic from a variety of perspectives. It entertains questions, such as: What are the implications of this topic for individuals, particular groups of individuals, and society at large? What ethical dilemmas arise in discussion of this topic? How do evolving technologies impact the way that individuals, groups, and society perceive the ethical issues surrounding this topic?

As students learn to analyze ethical problems and develop their personal ethics, they first must learn to examine topics from a variety of perspectives that sometimes conflict with each other. When asked to defend their views about what is right or wrong, many students are unable to successfully articulate the underlying reasons for their beliefs or present rational arguments for them (Haidt, 2001). They may justify their actions with superficial rationalizations such as "what is good for you may not be good for me" or "everybody else is doing it so it must be okay" (Pritchard, 1999). Furthermore, existing and emerging security technologies add layers of complexity to issues, leading students to assume that, because they are dealing with an evolving technology, the underlying ethical norms have also changed. We want students to examine their current state of thinking, question intuitions, address existing norms, and discover the inadequacy of intuitionist rationalization.

To foster a deeper, systematic understanding of ethical problems, the authors propose using three normative ethical approaches as tools for examining the underlying ethical issues for any given information security topic. Normative ethical theories abound (for a more detailed exploration of ethics, readers are referred to Kant, 1964; Johnson, 2001; Popkin & Stroll, 1993; Spinello, 2003). In this article, we include a brief description of three broad ethical approaches that are helpful in exposing ethical issues: virtue ethics, utilitarianism, and deontological ethics. Virtue ethics, an agent-centered approach, emphasizes the *motivation* for an action more than the action itself. Virtue ethics emphasizes an individual's character: if an individual is virtuous, then his or her actions are thought to be ethical. Utilitarianism, a consequence-centered approach, emphasizes the ultimate outcome of an action whose worth is based on the net total of "good" that it produces, regardless of the motive. People are advised to maximize happiness for the whole and not just their own happiness. Finally, deontological ethics examine an agent's motives. They claim that, in order to act in an ethical manner, a person must take action for the sake of fulfilling an obligation. A person must do his or her duty. According to Kant (1964), learning what is one's duty begins with the *categorical imperative,* to treat others as you would have them treat you. Students have heard versions of these theories before. They have been urged to cultivate virtue, as in "don't be stingy." They have been taught to anticipate how their actions will affect other people, to seek "the greatest good for the greatest number." And they have encountered some variation on the Golden Rule. They will have been acquainted with advice to develop virtue, maximize happiness, and perform their duties.

Applying these three ethical approaches to a topic in information security allows students and instructors to investigate how the topic manifests itself to individuals and their belief systems, groups and their shared cultural values, and society at large with its social codes. Use of the ethical approaches also allows the underlying ethical dilemmas to be untangled from the confusion of detail that sometimes accompanies new technology. These classic approaches to understanding right and wrong are beneficial for examining the impact that emerging technologies have on various populations because they help to separate technological features from their ethical implications, thereby preparing students to examine security issues.

The Security Dimension

The security dimension for a specific information security topic includes ways in which the topic manifests to information security professionals and others

4 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/chapter/pedagogical-framework-ethicaldevelopment/13518

Related Content

Security Issues for Cloud Computing
Kevin Hamlen, Murat Kantarcioglu, Latifur Khanand Bhavani Thuraisingham (2010). *International Journal of Information Security and Privacy (pp. 36-48).*
www.irma-international.org/article/security-issues-cloud-computing/46102

An Image Steganalysis Algorithm Based on Multi-Resolution Feature Fusion
Zhiqiang Wuand Shuhui Wan (2024). *International Journal of Information Security and Privacy (pp. 1-19).*
www.irma-international.org/article/an-image-steganalysis-algorithm-based-on-multi-resolution-feature-fusion/359893

The Role of Privacy Risk in IT Acceptance: An Empirical Study
Joseph A. Cazier, E. Vance Wilsonand B. Dawn Medlin (2007). *International Journal of Information Security and Privacy (pp. 61-73).*
www.irma-international.org/article/role-privacy-risk-acceptance/2461

A Novel OpenFlow-Based DDoS Flooding Attack Detection and Response Mechanism in Software-Defined Networking
Rui Wang, Zhiyong Zhang, Lei Juand Zhiping Jia (2015). *International Journal of Information Security and Privacy (pp. 21-40).*
www.irma-international.org/article/a-novel-openflow-based-ddos-flooding-attack-detection-and-response-mechanism-in-software-defined-networking/148301

Metamorphic Malware Detection Using Minimal Opcode Statistical Patterns
Mahmood Fazlaliand Peyman Khodamoradi (2018). *Security and Privacy Management, Techniques, and Protocols (pp. 337-359).*
www.irma-international.org/chapter/metamorphic-malware-detection-using-minimal-opcode-statistical-patterns/202054