Patterns for Ethical Decisions in Information Systems Security

MARY TEDESCHI, College of Technology, CUNY

According to Ralph Johnson, “Patterns are supposed to describe reality, not invent new ones”. Identifying patterns in information security ethics has the potential to create better Internet security.  The Internet is not an ethically secure place and has no known ethical security patterns associated with it.  Ethical decision making helps improve cyber security.  Patterns are primarily about solutions, but understanding the problem is vital. In this paper, we demonstrate how we created several ethical patterns based on teaching an introductory course in computer security.

Categories and Subject Descriptors

General Terms: Ethics, Security

Additional Key Words and Phrases: Privacy **ACM Reference Format:**

Tedeschi, M Patterns for Ethical Decisions in Information Systems Security. HILLSIDE Proc. of Conf. on Pattern Lang. of Prog. 25 (October 2018), 10 pages.

1. INTRODUCTION

All computers can be hacked. Computers connected to the Internet are the most vulnerable. Computers are connected together for the purpose of communicating data electronically. Any technology that aids in gathering information about people or organizations without their knowledge, such as spyware, may be considered unethical. Ethical decision making helps people make difficult decisions when faced with an ethical dilemma, a situation in which there is no obvious clear right or wrong answer. This course covered the use of scenarios in computer ethics studies. Ethical decision making in terms of computer usage and data processing contains patterns. The students were asked in class to anonymously and carefully review each scenario and respond using a Likert scale. They were asked to respond if the actions of the person were very ethical/ethical/neither ethical nor unethical/unethical/very unethical. The opinions of partially-trained students is not a strong enough basis to assert an ethical claim. The collective responses generated the source of the resulting pattern. The tool, Likert scale, may be an ethical ratings pattern to raise awareness to students learning about ethical decision making in information security.

Situational ethics states that decision making should be based on the circumstances, not upon fixed law. This paper will address two situations. The behavior and attitudes we have regarding Internet usage matter, and can be mapped on a behavior continuum ranging from constrained to cavalier. We need a clear understanding of ethics and ethical behavior in situations matter. Having a sense of what is correct and acceptable Internet usage and behavior in your mind will determine the solution. Some of the questionable ideas include: if you worry about security on the Internet; if you trust using your phone; if you use email; if you use or trust spam filters; if you use social media; if you interact with your friends and colleagues on the Internet, and if you believe you are part of a collective mind. Ethics is a set of moral principles that govern the behavior of a group or individual. Computer ethics is a set of moral principles that guide or regulate the use of computers. Common issues include privacy concerns and how computers effect society.

1.1 Ethical Decision Making

Each society forms a set of rules that establishes the boundaries of generally acceptable behavior. Many times the rules are expressed in statements about what people should or shouldn’t do. These rules fit together to form the “moral code” by which that society lives. The term morality refers to social conventions about right and wrong that are so widely shared that they are the basis for an established common consensus. The intent is to use the example of a security incident to demonstrate opportunities for ethical decision making. Security incidents must be looked at as opportunities that deserve mature and measured responses. If a system was attacked or hacked or otherwise swindled, we must figure out what exactly happened and go beyond that. Determining what happened is a very important step in the process. For example, many incidents happen and yet the decision was made not to determine what happened. Perhaps the reason is cost, but also because of the desire to bury the problem. Either way would be an ethical lapse. The aim of this paper is to give guidance in these types of situations.

If a breach occurs it is important to determine how it happened. It might be a known weakness, such as a password or SQL error, or it could be something obscure that requires in-depth analysis. The details will be learned. The next step is to determine the impact to the system. Perhaps it was an external server or web application – or maybe a lost laptop or internal data base. A check of information that might have been effected is required. Was it nothing? It could be intellectual property or customer information. A granular level of detail is needed to figure this out. The next step is to determine who was involved in order to help with long-term response efforts and security program corrections. When an incident or breach occurs, it is fact; you can’t change what already happened. Ethics can be described in terms of the field of the computer and information professional, the field of philosophical ethics, and the field of sociological/descriptive ethics, i.e., the “digital divide” issue. Computer and information professionals do have a code of ethics, for example, members of the Association for Computing Machinery (ACM). The Institute of Electrical and Electronics Engineers (IEEE) has a Code of Ethics, as well. Ethics in computers can connote ethical issues associated with computing machines. It can also connote a cluster of ethical concerns affecting the free flow of, and access to, information, including censorship and freedom.

The field of ethics, or moral philosophy, involves systematizing, defending, and recommending concepts of right and wrong behavior. Philosophers today usually divide ethical theories into three general subject areas: metaethics, normative ethics, and applied ethics. Normative ethics is the study of how people ought to behave. This is also called virtue ethics approach. It does not define an exact formula for ethical decision making. Virtue ethics suggests that, when faced with a complex ethical dilemma, people do either what they are most comfortable doing or what they think a person they admire would do. Descriptive ethics is the study of how people do behave and how they think they should behave.

Descriptive ethics is a form of empirical research into the attitudes of individuals or a group of people. Because descriptive ethics involves empirical investigation, it is a field that is usually investigated by those working in the fields of evolutionary biology, psychology, sociology, or anthropology. This paper reflects the research of classes taught and attitudes of classroom discussion.

2. ETHICAL DECISION MAKING PATTERNS

This is not a comprehensive study, but a few examples as a vehicle for a discussion concerning ethical decisions.

# Name: Signed Email Pattern

**Problem:**

You need to read your email, but anyone can be the sender. Receiving an email from an unknown source may be tempting to open. Should we open the email?

**Context:**

You get a flood of emails. It is time consuming to read all at once. It could be your work email or your personal email, and they are different environments. Not everything is work related. Sometimes we expect an email and sometimes we don’t. What do you do?

**Forces:**

You cannot force the sender to use a digital signature. You may not have the latest virus scanning software. A “risky” email was not caught by the junk or spam filter. Do we read the subject to determine whether or not to open the email? Does having a subject make a difference to us?

**Solution:**

Try to only open from known senders. Install a policy to allow your employees to only open signed emails. Avoid using email when a simple text or telephone conversation is more appropriate. Use email cautiously.

**Consequences:**

Could cause system worm or virus introduction. Could get fired if you open sensitive work email and get caught.

**Examples:**

If the subject stated “Funniest Joke”

Do you open?

If the subject stated “Managers Salaries”

Do you open?

Does it make a difference?

Either could be a virus.

Is it ethical to open either?

It depends on the context: Work or Home?

Funniest Joke to home email – you might consider opening it; if it is to your work email it is not a good use of work time.

Managers’ salaries to home email – how did it get to your home email? Should not open; to your work email – who sent it? Should not open it.

Today’s workers are subject to the monitoring of their e-mail and Internet access while at work, as employers and employees struggle to balance the need of the employer to manage important company assets and employees’ work time versus the employees’ desire for privacy and self-direction.

**Name: Working Between Stitches Pattern**

**Problem:**

A student found a loophole in his university’s computer system that allowed him access to other student records.

**Context:**

The student told the system administrator about the loophole, but continued to access student records until the problem was corrected two weeks later.

**Forces:**

While you can’t fully protect yourself from hacking, you can help prevent it from happening.  The student’s action for searching for the loophole was? The student’s action in continuing to access others’ records for two weeks was?

The system administrator’s failure to correct the problem sooner was?

**Solution:**

As soon as an update becomes available for anything from your phone apps to your entire operating system, you should apply it if possible.  Instead of looking for a loophole in the school encourage the student to compete in hacking contests.  Students are developing valuable skills.

**Consequences**

The update patch could cause a new virus.  If you sell exploits and vulnerabilities even though it may not be illegal it could be a crime. They can give information for free to the companies whose system they are testing, or to the government. If a person acts with integrity, that person acts in ways that are consistent with his or her own code of principles. Integrity is one of the cornerstones of ethical behavior. One approach to acting with integrity is to extend to all persons the same respect and consideration that you yourself desire. Unfortunately, it is difficult to act in a consistent manner. One opportunity for inconsistent ethical behavior arises when you find yourself in a situation in which there is a conflict between your standards.

**Examples**

**Earlier this year** a group of high school students are accused of hacking their school’s computer system to change grades. Police arrested four teenage boys last week at Dickinson High School in Jersey City. They range in age from 15 to 17. The teens are charged with illegally accessing data to change the grades of as many as 10 students. Officials say they used software that tracks teacher’s keystrokes. The school says the students were disciplined, but did not say how.

If you witnessed a friend copy someone else’s answers while taking an exam, you might be caught in a conflict between loyalty to your friend and the value of telling the truth. Sometimes, the rules do not seem to cover new situations, and you must determine how to apply the existing rules or develop new ones. You may strongly support personal privacy, but in a time e=when employers are tracking employee email and Internet usage, what rules do you think are acceptable to govern appropriate use of company resources?

Suppose, that you believe it is important for your career to do as your employer requests, and you also believe you should be fairly compensated for work that you do. Now, imagine that, due to budget constraints, your employer insists that you do not report some hours of overtime that you have worked on a project. The situation creates a conflict between your moral standards. You can do as your employer requests, or you can insist on being fairly compensated, but you cannot do both. In this situation, you may be forced to act in a manner inconsistent with one of your principles and act with an apparent lack of integrity.

Students around the world have been caught downloading material from the Internet and plagiarizing content for their term papers.

1. MODEL

In the course, the students were given situations and asked to rate them (1-5)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Very ethical | Ethical | Neither | Unethical | Very unethical |

The findings were that most of the students chose neither ethical nor unethical for the majority of the situations. To raise awareness of ethical behavior we can create an ethical ratings pattern. Another form of inconsistency emerges if we apply our moral standards differently to different people or to different situations. To be consistent and act with integrity, we must apply the same moral standards to one person or one situation that we apply to another. You might consider it morally acceptable to tell a friend a “Little white lie” to spare the person some pain or embarrassment, but would you consider lying to a work colleague or customer about a business issue to avoid unpleasantness? Good ethics are not always good business.

4. DISCUSSION

The discussions about computer and network security have been many since they relate to the difference between democracy and the state where “Big Brother is Watching You”, George Orwell’s 1984.

The evaluation criteria for ethical security patterns should contain the following items: Class of service; configuration management; alternate routing; fault management; efficiency; cost; openness; accounting; transition effort; availability, and constant response time. Class of service as it relates to network technology and ethical decision making. Configuration management as it related to responsibilities and resources. Alternate routing is the ability to use another transmission line if the regular line is busy. Fault management involves making sure that new digital services are of excellent quality. Openness or open source software, such as Dragonchain developed in 2016 at Disney in Seattle. Blockchain standardization and secure distribution of data is starting to become mainstream. Application areas, such as identity, which include privacy and security and confidentiality factors, i.e., HIPAA are important to maintain confidentiality, integrity and availability.

The evaluation criteria for ethical security patterns should contain the following items:

* Class of service: relative to network technology and ethical decision making
* Configuration management: relative to responsibilities and resources
* Alternate routing: the ability to use another transmission line if the regular line is busy
* Fault management: ensuring that new digital services are of excellent quality
* Efficiency:
* Cost:
* Openness: open-source software, such as Dragonchain developed in 2016 at Disney in Seattle
* Accounting:
* Transition effort:
* Availability:
* Constant response time:

5. CONCLUSION

The students in the course are given situations and then asked to respond to whether or not the situation is ethical, very ethical, neither ethical nor unethical, unethical, very unethical. This study will continue with improved findings for future work.

Today computers are effectively ubiquitous. We have RFID chips in our passports. Computing devices will become more and more indistinguishable from many other kinds of noncompeting devices. Computers are smaller and smaller in size. Computer security on the Internet has a major impact on our moral, legal and social systems. Ethical concerns having to do with whether or not someone should participate in developing a certain kind of computer system did not exist before the advent of computing technology. Ethical decision-making existed before computer technology systems existed. Before “digital” privacy concerns the issue of piracy itself existed as a moral concern. We need to continue to distinguish between unique technological features and unique ethical issues of computer security.

Additional attack patterns exist in web applications, privilege misuse, cyber espionage, crimeware or malware, point of sale attacks. The patterns in the paper are a small sample of the types of ethical decision making patterns that users and computer professionals may encounter. Patterns provide a way to organize and name those ordinary solutions to make it easier for people to use them [1]. Taking a patterns-based approach can help both business and technical teams to agree on the primary objective of the solution.

ACKNOWLEDGEMENTS

I would like to thank my shepherd, David Kane for his valuable comments in writing this paper and his enthusiasm in my topic. I would like to thank Christian Kohls for EuroPlop sessions and the opportunity to improve this paper. Thanks to Christopher Preschern for helping me prepare for EuroPlop 2019. Thanks to Hong Li, my department chair for authorizing my efforts and Ashwin Satyanarayana for constructive feedback and encouraging me to try. Thanks to Diana Merenda for helpful editing comments. Thanks to Michael Blandino for the production of this paper. I would also like to thank William Telafor who helps me every step of the way.

REFERENCES

Bergstra, Jan A. (2013). *Bitcoin and Beyond: Exclusively Informational Money.*Informatics Institute, University of Amsterdam. <http://arxiv.org/pdf/1304.4758.pdf>

Fowler, M. 1997. Analysis Patterns: Reusable Object Models, Addison Wesley, Reading, MA.

Schneier, B. 1996. Applied Cryptography, John Wiley & Sons, Inc. New York, NY.

Whitman, M.E. and Mattord, H.J. 2016, Principles of Information Security, Cengage Learning, Boston, MA. Bitcoin.org <https://www.martinfowler.com/articles/writingPatterns.html><https://www.justice.gov/opcl/privacy-act-1974>

[*https://techterms.com/definition/computerethics*](https://techterms.com/definition/computerethics)

<https://tools.ietf.org/html/rfc1087>

<https://tools.ietf.org/html/draft-fastenrath-ethics-search-protocol-00>

<https://www.bitcoincash.org/>

<https://hillside.net/plop/plop2001/accepted_submissions/PLoP2001/ebfernandezandrpan0/PLoP2001_ebfernandezandrpan0_1.pdf>

<https://www.idi.ntnu.no/emner/tdt4237/2007/yoder.pdf>

<https://hillside.net/plop/2011/papers/A-39-Hafiz.pdf>

https://newyork.cbslocal.com/2019/02/28/nj-students-accused-of-hacking-schools-computers-to-change-grades/