Patterns for Ethical Decisions in Information Systems Security

MARY TEDESCHI, College of Technology, CUNY

Patterns are supposed to describe reality, not invent a new one, according to Ralph Johnson. Patterns in information security ethics may help to create better internet security. The starting point of all achievement is desire. Weak desire brings weak results, just as a small fire makes a small amount of heat. The internet is not a pattern. The internet is not secure. Ethics and ethical decision making helps to improve cyber security. Based on teaching an introductory course in computer security several ethical patterns have emerged. Block chain and bit coin technology have patterns in them, such as ethical patterns and design patterns.

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. Ethical decision making in terms of computer usage and data processing contains patterns. By definition, an intruder can be a person with criminal intent, but not necessarily. An intruder is someone who is in a place or situation where they are not wanted. They are someone who enters a place without permission in order to commit a crime. If the "intruder" or hacker is a person who uses computers to gain unauthorized access to data is unskilled or skilled, this may or may not be any less dangerous on the internet. A script kiddie is an unskilled individual who uses scripts or programs developed by others to do something, such as, deface websites. We use the term intruder because they may not be a skilled hacker. A skilled computer programmer can be a "security hacker" to use bugs or exploits to break into computer systems. A situation may require ethical decision making during a computer operation or usage. An intruder in a computer system can be either passive (listener) or active. An active intruder may record the messages, replay them, inject its own messages or modify the traffic passed on the network. Normally the intruder does not know what the decryption key is and therefore cannot decrypt the message that was recorded while listening to the traffic passed on the network. People don't care about the current state of your security program; they care about the negative situation that has occurred. They want to focus on the crisis and the recovery. The trouble with adverse security events is that they strike unexpectedly. Sometimes, at what seems to be the worst possible time. The patterns in the paper are a small sample of the types of ethical decision making patterns that users and computer professionals may encounter. Gender should not play a role in making ethical decisions in computer security. Gender bias is a different topic and will be addressed in a separate paper.

Situational ethics states that decision making should be based on the circumstances, not upon fixed law. This paper will address a few situations. The culture of social media has a role in how people behave and react as well. Block chain and bit coin are new but the social effects of block chain can be powerful and lasting. Bitcoin aims at counteracting misuse of political power. We experience ethical decision making opportunities and may choose to do right, wrong or nothing. For example, being a teenage girl in 2018, age 13-19, it means coming of age online in a hyper sexualized culture that has normalized extreme behavior, from pornography to the casual exchange of nude photographs; undermining feminist empowerment. We have a culture in which teenagers are spending so much time on technology and social media that they are not developing basic communication skills. The cryptocurrency movement and teenage usage of social media are such that value can be used to motivate people to forego important ethical norms with little or no risk. Issues of block chain ethics and child pornography can be explained with patterns.

Bitcoin is supposed to replace currency. How we purchase and use electronic or "ewallet" to buy things, get paid in bit coin, and conduct transactions are supposed to be secure with forward trace. "Blockchain" is open source code. Companies are creating their own versions and have a record of everything.

The behavior and attitudes we have regarding internet usage matter, such as cavalier behavior. 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 are: if you worried 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, 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

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.

A breach 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, you can't change what 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 ACM. 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, access to, information, which includes 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.

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.

1.2 Privacy and Security Background Information

The purpose of this section is to provide background information. The Privacy Act of 1974 is a United States Federal Law, which establishes a Code of Fair Information Practice that governs the collection, maintenance, use, and dissemination of personally identifiable information. The privacy act is supposed to protect against unwarranted invasions of privacy. The HIPAA Privacy Rule establishes national standards to protect peoples' medical records and other personal health information and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically, such as over the internet. The two concepts privacy and security often overlap each other since they are so closely related. Privacy concerns on the Internet effect people regarding use and misuse of personal information. The security on the Internet and in computer networks is an important

issue for users who are concerned that data they have can be accessed and manipulated by unauthorized intruders, who have no right to the information.

There are other concerns, besides wire-tapping, dealing with security on the Internet, like hacking and computer viruses attacking computer networks. Privacy in the context of information security is the right of the individuals or groups to protect themselves and their information from unauthorized access, providing confidentiality. The main difference between the concepts security and privacy in computer systems is that the information is secure if the owner has control over it. The information is private if the subject of the information has control over it. Private information is not revealed without permission.

Privacy and ethics involve risk and risk analysis and we need to help improve computer security by ethical decision making. Patient confidentiality is very important. Protecting the private details of a patient is not just about moral respect, it is essential in maintaining trust between the doctor and the individual.

The Internet was Arpanet/NSF Backbone. You could not use the internet for any commercial purposes at all. It was for scientific purposes only in the early days.

1.3 Conditions

The three most important goals for the security are:

- Integrity, which means that the data is whole, complete and uncorrupted
- Confidentiality, which means that data is protected from disclosure or exposure to unauthorized individuals or systems
- Availability, timely access to resources and functionality of software

In addition to these are:

- Authentication, is the access control mechanism that requires the validation and verification of a supplicant's purported identity
- Authorization, access to highly sensitive information will be restricted to users with secret or top secret clearance
- Accountability, all failed logon attempts will be logged with timestamp and source IP address

2. ETHICAL DECISION MAKING PATTERNS

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

Email Attack Pattern

Email is a widely used communication mechanism that can be categorized into two basic types of web based service: open or closed. Open web based services provide email to anyone, either for free or a fee. Closed web based services are managed by organizations that provide email only to their members. Email is used by commercial and social websites because of its security and speed. Email is quicker than conventional mail. Email is an increasingly common tool to communicate. Often an attacker creates attacks containing malware designed to take advantage of the recipient. Imagine that the subject of a company email has been "See our managers' salaries and social security numbers" instead of "Funniest joke you'll see today". Do you open the email? What is the best course of action to take? Was this attack caused by an insider or an outsider? Will virus control software prepare for the next incident? Was this attack the result of a virus or a worm? Is it ethical to open the email? What about the subject of the email? Is email for old people? Is it primary? We have a feeling of control with email. Why?

Therefore:

We need to be able to decide if the message is spam. Spam is created by attackers who send unsolicited or bulk email. We also need to determine if the email is a virus. A virus is a major threat to email security. Do not open the email.

Send the email to the security team to respond. PII must be protected against disclosure using approved algorithms. If you open the email, do you act on it and how? The main reason an email is hacked is to access, the personal or sensitive, or confidential information that it might contain. It is very harmful for the user and could damage the profiles on certain websites, bank accounts, or personal life. Email hacking is still a very common problem as email is replacing letter mail for important correspondence, and the increase of email use has led to many high profile cases of email intercepted by other people for illegal purposes. Confidentiality, integrity and availability are the goals. Integrity is addressed by determining if the message is real and not spam. Confidentiality is addressed with cryptography. Availability is addressed by testing for viruses. An infected email could cripple a computer system and cause detriment to the availability.

Protect email with digital signatures or encrypt the contents. A digital signature is a type of electronic signature that encrypts documents with digital codes that are particularly difficult to duplicate.
Key generation: first, choice of algorithm parameters and the second phase computes the public and private keys for a single user.
Parameter generation: Choose an appropriate cryptographic hash function and decide on the key length.
Decide the number per user keys, perhaps, choose a secret key, and then create the public keys.

Trespass Pattern

A company was infected with a worm program that came from an employee's personal USB drive. To prevent this from happening again, all users in the company were now prohibited from using personal devices on corporate systems and networks. The CEO wants to allocate additional funds to the next training budget. Instead of just ramping up the antivirus software, we need to develop a formal information security program. Do we assume that employees will do it anyway, like people who drive and speed? Do we stop all employees from all USBs, headphones, etc.? An example, is when someone does something unethical to test the system. If a TSA screener inserted a knife into someone's bag on purpose to test the internal controls of the operation. They are not authorized.

Therefore:

Information security includes computer security, plus security of the networks. Someone plugged in another USB drive and infected two servers. The employee violated policy; did he commit ethical violations as well? How much security is enough? Is it safe? We need to think about the risks and consequences. An internal cyber threat is a real possibility. Dormant malware potentially can reveal system errors or steal intellectual property. There is a risk of contamination. People have lost USB devices or give them away at trade fairs. A seemingly harmless portable peripheral device can trigger a massive cyberattack. The fact that even the international space station with all its safety and security protocols, can be hacked. The worst case scenario were software capable of disrupting industrial processes can infiltrate and deteriorate production chains and lead to industrial accidents with considerable human and material damage.

Decontamination lock chambers equipped with antivirus terminals can be set up at various access points to the workplace. They can verify if USB flash drives have been infected after use. They do not prevent human errors, such as forgetting to analyze USB Sticks and limited effectiveness to anti-virus software. The user may also use only internal USB flash drives that are kept in a secure place. Even with education and awareness raising, people might still engage in incorrect practices. Driven by curiosity, people tend to connect USB sticks even though they are perfectly aware of the risks. A solution might be to use portable peripheral devices.

An infected computer can spread a virus to a clean USB thumb drive as well. USB drives can fry your computer but not from a USB cable, it does not hold data. Confidentiality, integrity and availability are the goals for the solution.

In the case of the TSA screener, are they authorized or not, is one question. The government conducts tests internally to check the employee response, in order to know if they are performing the correct procedures. In this pattern a person may be unethical or just irresponsible. There are side effects. You must check if it was accidental or if there was intent. Was the employee authorized to test the system.

Upgrade Technology Pattern

The system architecture team wants to upgrade the system. A contractor suggested improvements for implementing application and web servers. The consultant proposed two alternative designs, one was adequate and the other more elaborate. The issues were two categories, cost versus maintaining high security while keeping flexibility. Do you upgrade your phone? In the old days, you would buy a thing and install it. That was inconvenient and costly. Do your upgrades harm? Microsoft used to send upgrades on floppy disks. What if there was a software recall of the upgrade. You think you are saving money or the company does, and all the money would be gone, if a recall of the upgrade happened. When to upgrade your cell phone, as a rule of thumb, do you upgrade on an incremental upgrade or a large upgrade.

Therefore:

The network design consultant purposely under-designed the less expensive solution and produced a cost estimate for the higher end version that was over budget. Is it unethical to produce a report that steers the client toward a specific outcome? Also is it unethical to steer them into the less expensive option solely to reduce costs without regard to the project's security outcome? Our goal is to care about ethics before profits.

There are many arguments for and against upgrades to software systems, the best attributes are ability to integrate and connect to other applications that your business uses. Many organizations are upgrading systems and thinking about how to migrate to the cloud. To get the most out of the upgrade, they should consider automating manual and repetitive tasks. Lack of security has been a crisis for our technology dependent world. Historically, security has been considered a nice to have feature and something that can be added when needed later. We have learned the hard way that security must be designed into every technology and application, and it cannot be left out to reduce the cost.

With the Internet of Things (IoT) we have seen many examples. We do not want our household appliances hacked into just as much as our bank accounts. Never grab at the latest software because you think you should. Think about how you can fix a process versus install new technology. Find the real bottlenecks in your processes and fix them. Sometimes the fix will require new technology, sometimes not. Don't just "go cloud", for example. Focus on the barriers to growth and efficiency and relentlessly fix them with adequate solutions. Companies managing large amounts of data often keep it siloes within isolated and proprietary systems that can't communicate with each other. Website content, product inventory, client information, employee details, and digital assets can be managed in many ways. The solution may have a single database as a service, or maybe not. Less training, easy access and lower costs are important to the upgrade technology pattern. Confidentiality, integrity and availability are the goals.

Bad people can easily introduce malware/ransomware, virus on a machine, delete files, and steal information. We must use caution when upgrading.

Attack Protocol Pattern

An employee was terminated and he decided he was going to hack into the system. He performed a detailed fingerprinting of all Internet addresses. He launched a network port scanner from his Linux laptop and configured it to scan the entire IP address page for the extranet. With a single keystroke he unleashed the port scanner on the network. What can the former employee do to the company computers?

Therefore:

It seems obvious that he is breaking at least a few laws in his attempt at revenge. What if the company detected him and added his IP address to the list of banned sites, then they triggered a response to seek out his computer and delete key files on it to disable his operating system. Is the company ethical? Is this legal? What if the company was part of an industry consortium and all companies blocked a group of users for 10 minutes? The users would be blocked from perhaps hundreds of company networks. Would that be an ethical response?

Large amounts of data are transmitted and exchanged over a network. You do not want your File Transfer Protocol (FTP) server site to become a store-and forward site for files of questionable ethical content. Confidentiality, integrity and availability are the goals.

3. MODEL

3.1 Encryption method

Plain text is encrypted with the output becoming a cipher text.

Figure 1 Encryption method

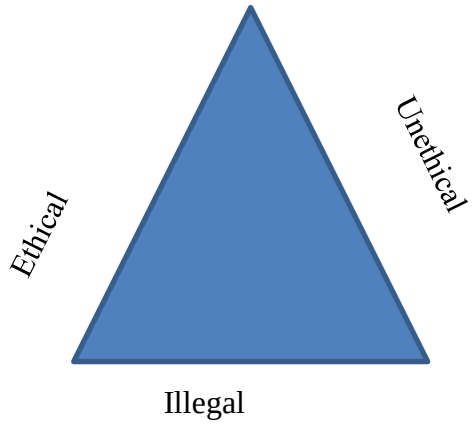
3.2 Decryption method

Cipher text is decrypted with the output becoming plain text.

Figure 2 Decryption method

3.3 CIA Triad

This is a visual pattern representation in figure 3. In this paper, patterns for ethical decisions can be viewed as a three



sided polygon .

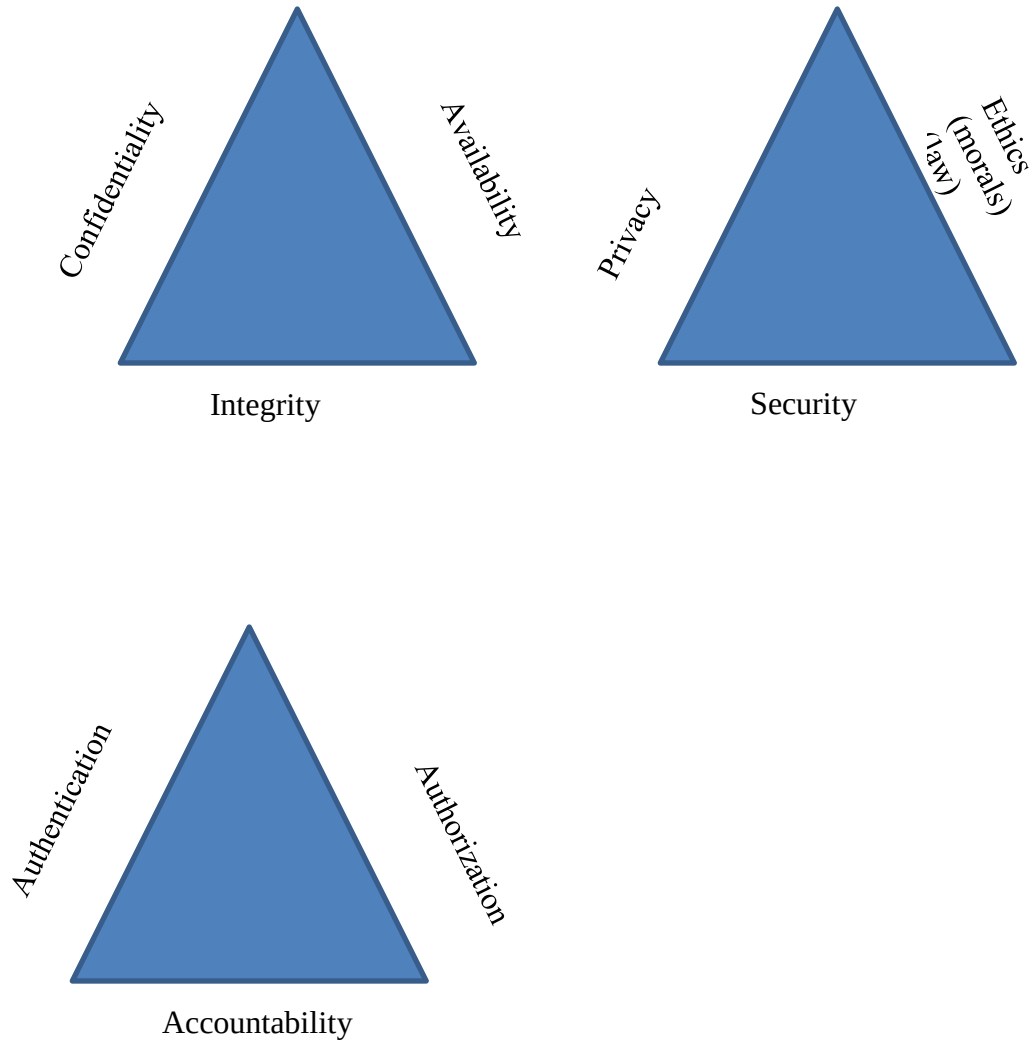


Figure 3 Three most important security pattern goals

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. "Block chain" is the technology that protects "bitcoin" and its users by keeping them safe from hackers. It is powered by a network of computers, which are often called "nodes". These nodes work together to verify every bitcoin transaction that takes place. In simple terms, when someone sends a bitcoin to someone, one node on the block chain network will verify the transaction using a mathematical equation. The transaction is then placed on the block chain network. Bitcoin is decentralized. Nodes all over the world operate the network. The network is not controlled by a main server, or a group of main servers. This is good for the security of bitcoin, as it makes it much harder for hackers to get access to the network. Bitcoin and ethics concerns will continue for the near future.

A 2015 study by LinkedIn found that "software engineering teams in tech have proportionally fewer women that non-tech industries; namely, healthcare, retail, government, education, and non-profits." This raises ethical concerns. Organizations like the National Center for Women and Information Technologies (NCWIT) correct the imbalance of gender diversity in technology and computing by empowering change leaders to report, retain and advance women.

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. Block chain 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.

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 becoming ubiquitous, i.e., they are everywhere. 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. These are part of a future work.

ACKNOWLEDGEMENTS

I would like to thank my shepherd, Michael John for his valuable comments in writing this paper and his enthusiasm in my topic. I would like to that our program chair Kyle Brown for detailed and constructive comments and my department chair Dr. Hong Li, for help and support with this paper. Thank you to Richard P. Gabriel for leading the peer review at PLoP 2018 and the feedback from all the session participants. Thank you to my students who inspire me every day to motivate them. Thank you to Dr. Aviva Wertkin, Robert Farkas and William B. Telafor for encouragement, praise and support.

REFERENCES

Fowler, M. 1997. Analysis Patterns: Reusable Object Models, Addison Wesley, Reading, MA.
Sales,Nncy Jo, 2016, American Girls Social Media and the Secret Lives of Teenagers, Alfred A Knopf, New York
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