**Ethics of Secure Coding**

CS 210 – Fall 2020

Colton Willits

Ethics are an important part of secure coding and secure coding is an important part of ethical computing. Without programming many different aspects of our technological world would not exist. Since programming is everywhere, criminals must adapt to exploiting this technology. Many often look for errors in coding done by developers to gain access and exploit a system. This is where secure coding comes in. Secure coding practices allow for vulnerabilities to be avoided during the development process. By implementing these practices, each and every developer can create a more ethical environment for their users.

Secure coding is the practice of writing software that’s protected from vulnerabilities (Bellairs). In today’s age, software vulnerabilities are a constant risk using secure coding allows for a developer or company to mitigate vulnerabilities that could affect their users or systems. This can result in the following. Denial of Service, where users are not able to access the system. Stolen data, such as credit card information or other PII of user that can be stored on a system. Complete loss of service, where the servers could even be affected. Damage to the systems where user data is corrupted or lost. In the event of an exploitation in healthcare systems or safety systems, there is also a potential in loss of life. These results can be the cause of Buffer Overflow, such as Heartbleed, or a code injection flaw, such as shell shock (Bellairs). These types of attacks are possible due to not using secure coding practices.

According to the ACM Code of Ethics, computing professionals should recognize that all people are stakeholders, honesty is essential in trust, computing should be used to make a positive impact, computing is a service to society, supports the public good, and should support ethical conduct of all computing professionals (ACM). However, there are computing professionals who do not wish to follow by this Code of Ethics. This is why measures such as secure coding are effective. They allow computing professionals to protect all stakeholders and create trust. By using the ACM Code of Ethics computing professionals are able to follow guidelines to create goals in their secure coding. It allows them to focus on certain priorities without having to worry about extraneous circumstances. Computing professionals create these goals and implement secure coding measures to gain the trust of their customers and be a service to society.

Computing professionals are able to protect their systems using a variety of different methods. However, for secure coding there are three common practices that professionals follow. The first is to not leave security until the end. In many cases, certain applications must be structurally changed completely to avoid vulnerabilities. Leaving it for last would only create more issues for the developer and the end user. The second is to look at different motives for attack. You must look at what types of information that your system will contain, and understand it’s worth to other individuals and criminals. Doing this allows professionals to understand what a criminal would look for when trying to exploit a system. Creating this mindset allows professionals to find flaws that could allow this information to be stolen or exploited by a criminal. Finally, computing professionals must understand that systems are constantly under attack. With each update or progress in work, professionals must understand that ethics are important to keep updated with as well. If you just fix and issue but never correct other ones you are putting other’s at risk of stolen data and compromising your code of ethics.

Secure coding and ethics are important to everyday development of computing systems. Without it, the actions of others cannot be held accountable, and user data and trust can be lost in a matter of minutes, through different attacks or by accident. By following a guideline of ethics with secure coding you can protect your systems and your users without compromising your ethical integrity by in computing.

**References:**

Bellairs, Richard. “What Is Secure Coding?” *Perforce Software*, [www.perforce.com/blog/sca/what-secure-coding](http://www.perforce.com/blog/sca/what-secure-coding).

Gotterbarn, D., Brinkman, B., Flick, C., Kirkpatrick, M. S., Miller, K., Vazansky, K., Wolf, M. J. (2018) ACM Code of Ethics and Professional Conduct

**Documentation Statement: I confirm that this is my own work, and received no help on this assignment.**