Nick Alexander
February 11, 2015

Paper 2 – Code of Ethics

In the majority of all industries, there is a set of guidelines or standards to which professionals are expected to adhere. The computer science domain is of no exception; in fact, computer science may, arguably, need to be held to a higher standard with regards to information security and assurance. The most critical and private information is stored in databases connected to the Internet: data such as health records, bank information, and government secrets. This paper aims to discuss two major vulnerabilities/exploits with regards to how computer science code of ethics was neglected.

Before the exploits are discussed, the code of ethics must be summarized. While private organizations may provide their own code of ethics related to computer science and information security, the most renown is that of the Association of Computing Machinery (ACM). Being the most prominent group of professional computer scientists, the ACM is held in high regard and has a very explicit code of ethics. Major points include: contribute to society and human well-being; give proper credit; respect privacy of others; honor confidentiality; strive to achieve the highest quality work; maintain competence; accept and provide professional review; evaluate systems and analyze risks; honor contracts and agreements; and improve public understanding of computing[1].

The next major code of ethics is one provided by the Association of Information Technology Professionals (AITP). The highlight points from this document are much the same from the ACM. Points include: protect the privacy of all information; insure the my products are used in a socially responsible manner; support and respect all laws; never misrepresent or withhold information relevant to a situation of public concern; never use entrusted information for personal gain[2].

Although not every computer scientist and information technologist is a member of neither ACM nor AITP, I find that the code of ethics is general enough that all computer professionals should be expected to uphold the standards. The major flaw in a code of ethics is the enforcement is purely personal. There are no governing bodies that will impose a punishment for those that break these codes; instead, the highest consequence is to have membership from the ACM or AITP terminated or to be publically ridiculed. To this effect, it is the responsibility of every computing professional to hold their peers to these standards to ensure the most safe and effective systems.

Now that two major codes of ethics have been outlined, the first vulnerability to be analyzed is the OpenSSL Heartbleed vulnerability. OpenSSL is an open-source library that implements web security protocols such as SSL and TLS; it is so widely used that it has become the de facto standard for secure server connections. Being so popular and open-source, one would expect it to be relatively bug-free; however, this is far from the case. In early 2014, the Google Security team found a long-standing bug, terrifyingly named

Heartbleed, in the OpenSSL library. The basis of the bug was the ability to illegally access memory locations through improper validation of user input when using the C memcpy function[3]. Personally, I find such a simple, incompetent mistake to breach the code of ethics of the ACM. When using the C language, it is a *cardinal sin* to not validate user input! Any C programmer, let alone accomplished software engineer, should have avoided such a rookie mistake especially in the critical SSL library. Moreover, the bug laid dormant for years before being discovered by a team of security experts performing an audit on the project. Why are these types of audits not high priority in the, for the third time, most widely used SSL library – it's nonsensical.

When questioned about why the bug was not found sooner, the president of the OpenSSL software group, Steve Marquess, stated that there simply was not enough funding for large audits of the library[4]. From the chorus, the most widely used SSL package could not be properly maintained and the excuse comes down to money. The ACM code calls for professionals to strive to further society. Using money as an excuse for a huge fault is far from furthering society. Though there are more points to be expressed, they will be withheld for the sake of brevity.

The next major exploit to be discussed is the hacking of the Montana Department of Public Health and Human Services (MDPHHS) server. In the summer of 2014, the Montana government found that a server containing public health records had been compromised although it was not clear if records had been accessed[5]. In direct violation of the AITP code of ethics, MDPHHS did not disclose how the hackers gained access to the server[6]. The code specifically states that critical information regarding a situation of public concern should never be obscured. If the public is unaware of the exploits used, there is no guarantee that said exploits will ever actually be fixed. More importantly, the department did not disable the server until a week after suspicious activity was detected on the network[6]. The department knowingly allowed more information to be compromised before actions were taken – another direct violation of the code of ethics from the AITP.

More importantly, the citizens impacted by the MDPHHS hack were wildly left in the dark. The final statement from officials, as aforementioned, simply stated that there was unauthorized access to records; there was never finality to the idea that records had been stolen or altered. Despite that concept, the information officer for the department informed the public that a post to an unidentified website exhibited evidence that a breach had occurred[5]. At the end of the day, the public has absolutely no idea what has happened to their entrusted information, which breaks a handful of AITP ethical guidelines alone.

In conclusion, people will always make mistakes. In neither of the discussed exploits did a person purposefully cause havoc. Regardless, the lack of preparedness and haste to which situations are dealt with are a major factor in terms of public scrutiny and ethicality. With the heartbleed bug, it took years to find the exploit in one of the most popular public codebases on Earth. It is impossible to know what kinds of data may have been accessed in the meantime. With the Montana data breach, the government was simply not prepared

enough to fend off an attack – a gross miscalculation for a government entity. Moreover, said government purposefully veiled the situation from the public and only gave misleading and vague details. Both of these exploits could have been handled in a better way, perhaps even prevented, in accordance to properly laid codes of ethics.

On the idea that changing times calls for new standards, it is not something that should be ignored. Today, we live in world that is absolutely controlled by computers – without them all societal operations would cease. Homes, automobiles, airplanes, etc. are being automated with computers and there are faces behind this software and information – trusted faces. The guidelines laid by both the ACM and AITP are extremely general, though not really vague, and provide a sort of timelessness. There may come a day where a new standard may be reworded or an amendment made, but I think both guidelines could exist in their current form without necessarily needing a change.

References

1. ACM (1992) *ACM Code of Ethics*. Retrieved from http://www.acm.org/about/code-of-ethics (Accessed: 11 February 2015).
2. AITP (n.d.) *AITP Code of Ethics*. AITP. Retrieved from http://c.ymcdn.com/sites/www.aitp.org/resource/resmgr/forms/code_of_ethics.pdf. (Accessed: 11 February 2015).
3. Wheeler, D. (2014) *How to Prevent the next Heartbleed*. Wheeler. Retrieved from http://www.dwheeler.com/essays/heartbleed.html. (Accessed: 11 February 2015).
4. Smith, G. (2014) 'How The Internet's Worst Nightmare Could Have Been Avoided', *Huffington Post*, 10 April.
5. Schuman, E. (2014) 'Montana health data breach a textbook example of what not to do', *Healthcare IT News*, 1 July.
6. Thompson, J. (2014) 'Montana Breach Affects Up To 1.3 Million As Health Care Data Gets Hacked', *WallStreet OTC*, 25 June.