Jaye Engelhardt

Dr. Yu-Ju Lin

Network Penetration, and Ethical Hacking CSCI 432 552

April 21, 2023

Security Engineering Ethical Concerns

In today's digital age, it is imperative to maintain a high level of security. It is evident that cyber security threats are on the rise, and individuals and organizations need to be prepared to deal with them. In the field of security engineering, the practice of designing and implementing security measures in order to ensure that information systems are protected from attack, damage, or unauthorized access is known as security engineering. It will be our intention in this paper to discuss ethical issues relating to security engineering. Also in this session, we will discuss red lines that a security engineer should not cross and steps that can be taken in order to become a responsible security engineer.

Security engineers must deal with several ethical issues when it comes to privacy. It is vital that security engineers respect the privacy and data of their users. As a result, they need to ensure that the data of their users is not accessed without their permission or shared without their consent. As a security engineer, you need to adhere to the least privilege principle. As a result, users should have access to the data and systems they need to do their jobs and should not be given access to anything else. It is important to grant access in accordance with a need-to-know basis. The integrity of systems is another major ethical issue in security engineering.

In order to ensure the integrity of data, security engineers must ensure that it is not modified or corrupted in any way. Secure protocols should be used by security engineers to ensure complete integrity of data, and data should be encrypted wherever possible. As well as overseeing secure systems, they must ensure that they are not vulnerable to attacks. To ensure that the data in transit and at rest is protected from unauthorized access, security engineers should use encryption and other security measures.

The issue of accountability is one of the most important ethical considerations in security engineering. They must be able to demonstrate that they have taken appropriate steps to protect the systems they are responsible for. They should keep detailed logs of security incidents and report on them if necessary. Transparency is also an essential ethical issue in security engineering. Security engineers must be transparent about their security measures, and the risks associated with them. They should communicate clearly with stakeholders about their efforts to protect data and systems. This helps to ensure that all parties involved understand the risks that come with the security measures, as well as the benefits. It also helps to build trust between the security engineer and the stakeholders, as they can be sure that the security engineer is taking the necessary steps to protect their data and systems. Transparency also helps to ensure that the security engineer's accountability is clear and that the stakeholders can hold them to their promises.

There are some red lines that a security engineer should not cross including. Security engineers must always act ethically and responsibly. There are certain red lines that they should not cross.

First, security engineers should not invade user private information without permission. They should only access data when it is necessary for their job and only with the user's explicit permission. Second, security engineers should not introduce malicious software or code into systems or networks. They should always test software thoroughly before deploying it and ensure it does not contain malicious code. Third, security engineers should not access locked or secure systems without authorization. They should only interact with systems they have been authorized to utilize. Fourth, security engineers should not violate security protocols or procedures. They should follow established protocols and procedures for accessing data and systems. Finally, security engineers should not share privileged information with unauthorized parties. They should only share information with authorized parties on a need-to-know basis.

There are several steps involved in becoming a responsible security engineer in the industry. It is essential for security engineers to keep abreast of the latest security trends, technologies, and best practices. For them to remain current with developments in the field, they should attend training and certification programs. Secondly, security engineers should follow security protocols, policies, and procedures. It is important that they are familiar with the organization's security policies and ensure that they are always followed. By applying the necessary security controls, security engineers should ensure data integrity and network security. Data should be protected during transit and at rest by means of encryption and other security measures. In addition, security engineers should establish a security culture within the organization. They should communicate the importance of security to all stakeholders and encourage everyone to take responsibility for security.

Finally, security engineers should maintain a high level of security awareness and training for personnel. They should conduct regular security training sessions for employees and ensure that everyone is aware of the latest security threats and how to protect against them.

Security engineering is an essential field that protects information systems from cyber threats. Security engineers must consider ethical issues such as privacy, integrity, accountability, and transparency. They should always act responsibly and avoid crossing red lines. By doing so, security engineers can help protect organizations and individuals against cyber threats and ensure information systems safety and security.

Works Cited

"ACM Code of Ethics and Professional Conduct." *ACM Ethics - The Official Site of the Association for Computing Machinery's Committee on Professional Ethics*, ACM Code 2018 Task Force, 22 June 2018, https://ethics.acm.org/.

Belding, Greg. "How to Become a Security Engineer: Training, Certifications and Resources." *How to Become a Security Engineer: Training, Certifications and Resources*, INFOSEC, 23 Dec. 2022, https://resources.infosecinstitute.com/career/how-to-become-a-security-engineer/.

Miller, Keith, and Simon Rogerson. "Software Engineering Code - ACM Ethics." *ACM Ethics - The Official Site of the Association for Computing Machinery's Committee on Professional Ethics*, Simon Rogerson, 8 June 2022, https://ethics.acm.org/code-of-ethics/software-engineering-code/.