Richard Schall
CS-405-H4327: Secure Coding 21EW4
Southern New Hampshire University
April 08, 2021

6-1 Journal: Don't Leave Security to the End

Explain what the following statement means as a best practice in secure coding: "Don't leave security to the end."

"Don't leave security to the end," means that security should be a part of the software development life cycle from the very beginning be it waterfall or an iterative approach. It is a good idea to have a well-developed security strategy. The strategy should include best practices that every software developer should partake in as they go about their daily work. An example of this is could be the way strings are handled or making sure the application is developed with the least user rights as possible, in other words try to develop as an administrator. These are only a couple of examples. The main idea is that security is considered from the beginning and is part of the project every step of the way instead of waiting until the end when the software is fully developed and then try to address security. Doing this could lead to security risks that cannot be addressed or expensive to address at a minimum.

Describe the steps you can take to prevent the threats.

The first step you can take to avoid threats is to look at historical risk and how those can manifest into future attacks. (Seacord, 2013) This could include analyzing past security breaches in the industry you work in.

Another step to improve security is to develop a coding standard that could be based of CERT/CC. The standard should contain compliant practices that apply to the project you are working on. It is important that the developers agree and understand the standard.

Another step is to develop a security policy. The policy should dictate who has access to what computer systems. The policy should employ the theory of least privilege, where a user is only given access to just the resources needed to complete their tasks.

Another step could be security testing by specialized third party. A network of computers and/or software application could be analyzed by a third party contractor that specializes in security threats.

Another step could be testing code for errors and vulnerabilities through a tool like Cppcheck. All code developed should be free of errors and warnings.

Provide one example that you can include in your Project Two presentation of how you plan to ensure that security is addressed intrinsically and not left until an issue is discovered—for instance, the use of unit testing.

One key to the presentation for me will be the use of the coding standard. If every developer on a team learns and understands the coding standard in place, known vulnerabilities can be avoided. An example of this is how to avoid buffer overrun when taking input from a user. If every developer understands the correct method to avoid this from happening, those risks will not make it into the code from the very beginning of the project. That is the hope anyway, that is why it is also important to conduct code reviews and allow the team to identify code that could be problematic that the developer missed.

References

Seacord, R. C. (2013). Secure coding in C and C¦. Boston, MA: Addison-Wesley.