Module Seven Project Two

Daryl Miller

Southern New Hampshire University

CS-405-T2675 Secure Coding 21EW2

December 9, 2021

Presentation Link: [**https://youtu.be/Uf0Vjaif-3g**](https://youtu.be/Uf0Vjaif-3g)

**Content**

[Project Two Script 3](#_Toc89948180)

# Project Two Script

| **Slide Number** | **Narrative** |
| --- | --- |
| **1** | Hello, my name is Daryl Miller and I am a software developer here at Green Pace and this presentation is our security policy and implementation guide. |
| **2** | This slide is the overview of what I will be covering in this security policy. In this presentation, I will cover Defense in Depth (DiD), Threats Matrix, the 10 security principals and coding standards, encryption strategy, Triple-A Framework, various unit tests, automation, risk and benefits to this policy, and finally the recommendations for maintaining this policy going forward |
| **3** | Defense in Depth is a redundant cyber security strategy that employs a layered approach to ensure maximum protection. Green Pace will adhere to the DiD image on the right as the basis for our cyber security. We will also adhere to 10 security principals and standards, encryption standards and Triple-A standards as set forth by Green Pace’s senior leadership |
| **4** | This slide is the overview of our Threats Matrix here at Green Pace. We employ 10 coding standards, which are stratified based on severity. Of the 10 standards, we have five that are considered high, two considered medium and three that are considered low. For example, the highest severity are those that are most likely to occur, have a medium to high remediation cost and are denoted in red on slide 6. In contrast the lowest severity standards are unlikely to occur, have a medium remediation cost and denoted in green on slide 6 |
| **5** | Slide five is a table representing the 10 core security principals here at Green Pace. Each principal is listed in the left column and then has its corresponding security standards in the right column. As evident from the table, many security standards are applicable to more than one security principal. For example, security standard 005, which is Memory Protection, applies to five out of the 10 core security principals. While the standards are stratified by severity, the core security principals are a comprehensive list with no one being more important than the other |
| **6** | Slide six is an overview of the 10 coding standards here at Green Pace. The table lists all the standards and provides relevant information about each such as, the standard number, standard name, the rule, severity, likelihood of occurrence, the cost associated with remediation, the priority and finally the level associated with each. Again, those denoted in red have the highest severity and are generally of most concern. |
| **7** | Slide seven is the encryption policy here at Green Pace. We utilize three encryption types, which are Encryption in Rest, Encryption at Flight, and Encryption in Use. Encryption in rest is fully encrypted data on a disk. This will prevent unauthorized access should the disk be accessed by someone other than those who have access. Encryption at flight is fully encrypting data as its being sent from one location to another. This is useful for drives that may store data in an unencrypted form and will then encrypt the data as its being transferred. Finally, encryption in use is the policy of fully encrypting and decrypting data based on user privileges. This is useful when apply the standard of least privilege so someone cannot access the memory to get the decryption key and decrypt the data. |
| **8** | Slide eight is the Triple-A policies here at Green Pace. The Triple-A Policies are broken down into three functions: Authentication, Authorization and Accounting. Authentication is used to validate a user against a set username and password in a data base. This will be the basis of grating a user access to our system. Next is authorization, which governs what each user has access to based on their credentials. Green Pace employs a system of least privilege so a user will not be given more access to the system than he or she needs to complete their tasks. Finally, accounting is the process by which all user’s actions are logged and monitored. This is useful for keeping track of who does what and potentially thwart things such as insider threats. |
| **9** | Slide nine is the Unit Tests overview which shows that all unit tests designed for Green Pace were successful in their different objectives. Each test will be designed using the “TEST\_F (parameter 1, parameter 2) {“ guidelines and will be a pass or fail test. If the test fails, it will be a fatal failure and the function will be aborted. Subsequent slides will go through the different unit tests in more detail. |
| **10** | Slide 10 is an Adding Value unit test. This test will ensure that a given quantity of entries can be added to the vector. |
| **11** | Slide 11 is the verifying max size and capacity unit tests. The verify max size tests will verify that a max collection size is greater than or equal to a given number. In this case, 0, 1, 5, and 10 were used as ASSERT\_TRUE tests. The verify capacity tests used the same numbers but checked the capacity rather than the max\_size |
| **12** | Slide 12 is the resizing tests. There are three displayed in the screen shot to the right. The first two are an increasing and decreasing collection size tests. The third is a resizing the collection size to zero. |
| **13** | Slide 13 is the erase beginning to end unit test. This unit test will verify whether the erase happened from beginning to end and assert true if the collection has been erased and set to zero |
| **14** | Slide 14 is the automation summary that is employed at Green Pace. This model should be used early in the Software Development Life Cycle. As evident in the image, the automation should begin in pre-production and flow all the way through production |
| **15** | Slide 15 is the Tools that can be used in automation and DevSecOps. DevSecOps is the process of automating the integration of security at every phase of the SDLC, from initial design through integration, testing, deployment, and software delivery. Many of the companies below develop DevSecOps tools that Green Pace should consider when developing and maintaining automation testing. |
| **16** | Slide 16 is the risks and benefits associated with automation and why it can be costly to neglect these benefits. These risks are straight forward in that it can be extremely costly to identify and correct bugs throughout the SDLC. Furthermore, depending on the scope of the bug, it can cost numerous man hours and damage a company’s reputation. Therefore, identifying and eliminating bugs as early as possible is the best way to avoid these problems further in the SDLC. According to IBM, it costs 6 times more to identify and fix a bug in implementation than it does in planning. That number jumps to 15 times more in QA. A good example of this would be when Samsung released their Note 7, it cost and estimated $17 billion dollars to fix its battery management system after the device was already in production |
| **17** | Slide 17 is the recommendations I have going forward. Gaps should be continually identified and documented early as possible. Continue to monitor for emerging threats and have a plan ready to mitigate these threats. This comprehensive presentation should serve as the standard to which Green Pace should move going forward. |
| **18** | In conclusion, this presentation has set forth the coding standards and principals that should serve as a minimum guideline going forward. It has also laid out the Defense in Depth strategy, as well as, the automation tools and encryption policies. Finally, continue to monitor the industry as applicable and implement new standards and policies as needed to maintain a safe environment for Green Pace in the future. Again, my name is Daryl Miller and I want to thank you for the opportunity to present you with Green Pace’s security policy. |
| **19** | Slide 19 is a comprehensive list of the references used throughout this presentation. |