2021 LG Security Specialist Project Grading Guidelines:

Recall that the project will be executed in two main phases designed to emphasize different aspects of software security design, implementation, evaluation, and management:

- **Phase 1: Secure Development** Design and implement required enhancements to the system; Emphasis will be on following good secure software development practices. Conduct a security evaluation on the team project; Produce a security assessment of the system in the form of a report.
- **Phase 2: Security Analysis of Classmate System** Teams will swap project artifacts and conduct a security evaluation of their classmate's system. Teams will need to produce a plan to describe how they will evaluate the security of an unknown system.

Each LG team is responsible for providing the following artifacts at the conclusion of the project:

- A document describing team organization and project plans (i.e. Team Charter).
- A report summarizing security design and and properties of the internal system including a list of found vulnerabilities.
- A report summarizing security properties of an unknown (classmate) system including a list of found vulnerabilities.
- A final presentation summarizing the project.

The purpose of this document is to provide guidance and templates for providing feedback to the teams. You will provide feedback on the project plan, requirements artifacts, design artifacts, presentation, and product demonstration. You should use the templates provided in this document to provide general feedback on these artifacts, but if you want, you may provide electronic and/or handwritten feedback on the specific artifacts as well. However, you should also base your feedback and grading on your interactions with the team as well. In general, we will use the following as grades:

4 points (A) = Excellent. Above and beyond what was required. Exceptional quality.
3 points (B) = Good. All elements met with high quality.
2 points (C) = Average. All elements just satisfied with acceptable quality.
1 points (D) = Poor. Not all elements satisfied, and/or less than acceptable quality.
0 points (E) = Failed to meet minimal standards.

Use the point values if you want to average individual element scores for an overall grade on an artifact (see the templates below).

Team Charter:

Considerations for grading the team's performance with the final analysis report include artifacts generated as well as their processes and overall project execution: Specific elements include:

- The team should describe the team organization and team roles in some capacity. How did they distribute work?
- The team should describe the security goals that they've identified for their project. This should include
  - A list of requirements with an emphasis on security-focused requirements
  - A prioritized list of threats the team believes must be mitigated
- The team should provide design documentation for their project
- The team should have some form of schedule providing key milestones grounded in reality. Notably, they should describe how they will focus effort. This should be aligned with stated quality goals for the project.

Security Analysis Plan:

Each team had to select different security analysis approaches to use on the project. They should justify the choices that they made. At a minimum, this includes:

- A description of each analysis technique selected including implementation details. If the team used a tool to implement the technique, then that tool should be discussed.
- A clearly articulated rationale for selecting the technique and/or tool. Given the strengths and weaknesses of a given tool or technique, why did they decide to use it? For example, if the team states they are going to perform security reviews, then they must describe the artifacts that will be subject to review, the timing, the frequency, etc.
- Some assessment of how well the technique worked. This should be based on hard data including, but not limited to vulnerabilities found using the technique.
- The teams should make a compelling argument that the techniques selected were appropriate.
- Breadth of technique selection. Did they recognize that different techniques are needed for different security properties?
- Any infrastructure or setup needed to make a technique work, such as creating mock classes or simulators.

The team will also need to provide a plan for analysis for how they evaluated the other team's project. This plan will be similar to the security analysis plan described above but it will take into account the priorities and requirements of the other team's project.

At a minimum make sure that each team has a process in place to answer questions about their system for the assessing team.

Vulnerability List Considerations:

Teams must submit a list of found security-relevant defects. The list should be well structured and include actionable information, such as:

- A description of the vulnerability.
- The analysis technique that uncovered the vulnerability.
- The specific test, technique step, or scenario that uncovered the vulnerability. This will depend on the technique selected.
- The location of the vulnerability in the project. This may be a component or source file.
- The perceived impact of the vulnerability.

Other pertinent information may be submitted. Again, there will be two lists submitted: one for the team's project and one for their assessment of another team. The structure of the lists should be the same.

Presentation Grading Considerations:

The content of the final presentation will include the following elements:

- Introduction to the team members and team organization.
- A description of plans, schedule, and schedule performance.
- A sense of prioritized security goals. What did the team think were the most important/critical security requirements and why? Were there any elements of the system the required prioritized, special, or otherwise different evaluation? Be sure to provide explicit definitions for terms used.
- The team's threat model used for identifying and prioritizing threats.
- A description of each analysis technique selected including some details, such as implementation requirements, setup, challenges, and needed supporting artifacts.
- A clearly articulated rationale for selecting a quality analysis tool or technique. Given the tool/technique strengths and weaknesses in the context of this project, why did the team decide to use it?
- Some assessment of how well the tool/technique worked. This should be based on hard data including, but not limited to defects found using the tool/technique, some notion of efficiency (i.e. in the case of testing, how many redundant tests were created), code coverage metrics, overall effort, etc.
- The results of your analysis in terms of the defects found. This list should include actionable information about each defect.
- Any other major decisions or clever analysis strategy that the team believes is worth mentioning.
- Reflection on what the team has done. What worked well? What did not work well? What would the team do differently if given the opportunity to do this project again?

Templates

In the following sections, there are templates to help in the grading of the key artifacts that the team has produced. These templates will be provided to each team so that when the students leave CMU, they can use all the teams' artifacts and the evaluation as examples when they establish their own project based courses. The idea is to promote consistency in evaluation and in feedback format. The following templates are provided:

- Security Analysis Report Grading Template
- Classmate Analysis Report Template
- Vulnerability List Grading Template
- Presentation Grading Template

TEAM NAME: ____

MENTOR: ____

Analysis Report Grading Template:

Grading Aspect	**Grade (A-E)**
1. Basic Processes	
Did the team utilize basic disciplined processes for security analysis. Specifically, how well did the team: ● Organize and select roles & responsibilities? ● Devise/evolve a strategy and document it? ● Create a strategic schedule with key security requirements? ● Try to estimate the size of the task and use this information to Create the strategic plan and schedule? ● Did the team provide a clear sense of security goals for this project? ● Did the team attempt to prioritize the security requirements for this project? ● How did the team focus effort? Were there aspects of the system that the team did not focus on? Did they explain a rationale for these decisions?	
Comments:	
2. Threat Model	
Does the threat model include the following: ● A clear description of the threat modeling technique used ● Descriptions of the tools and processes used to support the modeling procedure ● Identification of security objectives and assets for the system. ● A notional design for the system based on the assets of the system. ● List of threats facing the system. ● Ranking of threats in terms of priority.	

3. Analysis of other Team Project	
The team must provide a plan for how they plan to assess another team's project. This plan must include the following: ● Organize and select roles & responsibilities? ● Establish rules-of-engagement to describe the processes and procedures for their assessment. ● What procedures did the team use to identify targets for assessment? ● What tools and techniques did the team use to conduct their assessment? ● How did the team focus effort? Were there aspects of the system that the team did not focus on? Did they explain a rationale for these decisions?	
4. Organization and Quality	
How well did the team organize the report and are the artifacts of a reasonable quality given the project scope? What assumptions did they make about the project? How did the team handle the ambiguity of the project description? Are these assumptions clearly documented?	
Comments:	
5. Usage of Security Analysis Techniques	
Consider the following ● Did the team provide a clear, concise explanation of each analysis technique *used* (not what could have been used)? ● Did the team provide a rationale for why they selected a given technique? ● Did the team use the technique properly (in your assessment given the information they provided)? ● Were the tools and techniques selected appropriate for the task to which they were applied? (an example of a bad match is testing for concurrency issues)	

● How did the team measure the effectiveness of the tool/technique? Did the team collect data on tool effectiveness? Does the data presented help them assist in evaluation? ● How did the team distribute effort required for a given technique? ● How did the team implement each technique? Did they require additional infrastructure to support quality analysis (think configuration management, simulators/mocks, etc.)? Look for specifics in terms of tools used, appropriateness, and effort.	
6. Reflection	
Consider the following: ● How did the team approach analysis of their own project versus analysis of the other team’s project? ● Did the team identify strengths and weaknesses of the analysis techniques used? What challenges did they encounter and how did they overcome them? ● Did the team identify what went well? What could have gone better? ● Did the team recognize mistakes made and discuss how they would avoid them in the future? ● Did the team analyze their data? Effort? Defects found? Code coverage? Other? *Does their analysis support their conclusions?*	
Comments:	

Presentation Grading Template:

Grading Aspect	Grade (A-E)
1. Content and Organization	
Did the talk sufficiently cover the required topics? Was the talk focused and to the point? Were the presentation materials well designed and readable?	
2. Delivery	
Was the presentation completed within on time? Was the presentation clearly rehearsed? How smooth were transitions between parts of the talk? How well did the team handle questions: poise, tact, answers	
Comments:	

Vulnerability List Template:

Grading Aspect	Grade (A-E)
1. Organization	
The team will submit a list of vulnerabilities found in their project. When grading this document, please consider the following: ● Did the team include a list of vulnerabilities found? This list must include: ○ A description of the vulnerability. ○ The analysis technique that uncovered the vulnerability. ○ The specific test, technique step, or scenario that uncovered the vulnerability. This will depend on the technique selected. o The location of the vulnerability in the project. This may be a component or source file. ○ The perceived impact of the vulnerability. ● Did the team include actionable information for the vulnerability logged? This may vary but should include something similar to the following: ○ Description of activity and/or tool used to uncover the detect the issue ○ Containing artifact	

○ Trigger, evidence, proof-of-concept ○ Description of the problem ○ Impact, risk rating, and/or severity ○ Date found ○ Team member that found the issue ○ Related security issues The key is that they provide structured and actionable information on each defect.	
Comments:	

Vulnerability List Grading Template:

This report will cover the peer assessment of the project.

Grading Aspect	**Grade (A-E)**
1. Organization	
Did the team include basic information and sections: ● Executive summary and overall results. ● Narrative/process used, such as ○ Target discovery and reconnaissance o Attack tools and techniques o Effort allocations o Team organization o Rules-of-engagement	
2. Vulnerability Details	
For each issue the report must include ● Description of activity and/or tool used to uncover the issue ● Containing artifact ● Trigger, evidence, proof-of-concept ● Description of the problem	

● Impact, risk rating, and/or severity	
3. Conclusions	
● Did the team provide an overall security assessment? ● Did the team provide a list of recommendations for the team?	
Comments:	

Other Comments:

General Comments and Observations:
Summary of Strengths:
Summary of Weakness: