

Rubric

Follow the **GS Final Project Guidelines** document for a more detailed description of the content.

IMPORTANT NOTES:

- **Remember, writing counts! Unclear and confusing writing can affect your grade in the other sections if your message is unclear or too vague** (e.g., “security for X is important” is a vague statement without a deeper explanation).
- **Generated text and plagiarism from already published work will result in point deductions.**
- **Reviews/Survey papers are not allowed.**

Good quality document (10 points total):

- Proper layout including content, figures, references, and page limit.
- Easy to follow
- Correct grammar/spelling
- Clarity and conciseness

Section 0: Abstract

Appropriately summarizes and contextualizes the paper **(10 points total)**:

- Introduction to and context of the review (5 pt)
- Overall summary of the review with relevant information (5 pt)

Points will be deducted for missing, unclear, or irrelevant information.

Section 1: Introduction

Introduction of the paper **(15 points total)**:

- Clear and coherent introduction to the topic of the review with context for the subtopic (How does this subtopic fit into security?) (5 pt)
- Brief overview of the categorization and criteria used for the review (5 pt)
- Brief overview of the information and potential future directions extracted from synthesizing the reviewed papers (5)

Points will be deducted for missing, unclear, or irrelevant information.

Section 2: Background

Provide relevant background information **(10 points total)**:

- Explanation of background information which would be necessary for a computer security researcher who doesn't specialize in the topic to understand the review (5)
- Correct background resources and information (5)

Points will be deducted for use of unreliable sources, lack of relevant information, and using related work rather than background information.

Section 3: Categorization and Criteria

Selecting reasonable papers and categorizing them into a meaningful taxonomy (**20 points total**):

- Selection of **at least 10 papers** from reliable sources, reasonably recent (last 5 years), and **not SoK or review (survey) papers** (5 points)
- Creates multiple distinct, meaningful categories for these papers with reasonable distributions of papers in each category (i.e., do **NOT** make one category of papers with 9 papers and another with 1, 10 categories based on the author of each paper, “fuzzy” categories with heavy overlap, etc.) (5 points)
- The papers placed in each category clearly belong in the category based on its criteria (5 points)
- The chosen criteria for category placement reveals some information about the state of research on the topic and ties into the analysis (5 points)

Points will be deducted for unclear categorization criteria and meaningless categories.

Section 4: Analysis

Extracting meaning from your taxonomy (**20 points total**):

- The analysis relates to the categorization of papers and provides meaningful takeaways rather than basic observations about or summaries of information in the set (i.e., the analysis should **NOT** just be a summary of the papers or a generic observation like “X% of the papers focus on this subtopic”, but it can be, for example, “ X% of papers focus on this subtopic, but they neglect to consider factor Y even though this factor is meaningful for reason Z”) (10 points)
- The analysis is accurate for the set of reviewed papers and does not rely on heavily cherry-picking the set (e.g., do **NOT** pick 10 papers on side-channel analysis relating to acoustic and power side channels and make the claim that there is no research on EM side channels). Note that we do not expect you to know the entire body of research on the topic, but there should not be an excessive number of papers that contradict your takeaway claim (10 points)

Points will be deducted for takeaways and analyses that are generic, inaccurate, or do not relate to the categorization or not related to cyber-physical system security.

Section 5: New Research Directions

Identifying new research directions based on the analysis (**15 points total**):

- The new research directions relate to the analysis (5 points)
- The new research directions answer meaningful research questions (i.e., no “test more models of the devices tested in the papers”) and are feasible (5 points)
- At least one research direction is identified and described in detail (5 points)

Points will be deducted if there are no concrete research directions and if they are unrelated to the analysis or security, do not feasibly answer meaningful questions, or are not described in detail.