Project 1: Prompt Engineering Applications

Generative AI in Cybersecurity
Date: Jan. 24, 2024

1. Introduction

The integration of artificial intelligence (AI) in cybersecurity presents a novel area of exploration, with both potential benefits and challenges. In this assignment, students are tasked with employing prompt engineering to generate a cybersecurity document. This task aims to provide a practical understanding of how AI tools can be utilized in creating cybersecurity documentation, while also recognizing the limitations and need for human oversight in this process.

The objective of this assignment is to work in a team of three or four students to use prompt engineering to produce a cybersecurity document. This could be a policy guideline, a threat assessment report, a security protocol, or any other relevant form of documentation. Students will be required to formulate effective prompts to guide the AI in generating initial document drafts. Subsequent stages will involve critically evaluating and refining the AI-generated content to ensure its relevance, accuracy, and applicability.

This exercise is designed to offer a balanced perspective on the use of AI in cybersecurity. You will experience firsthand the process of integrating AI into cybersecurity practices, while also encouraging critical thinking about the capabilities and limitations of AI tools in this field. The assignment is not only about producing a cybersecurity document but also about *understanding the role and impact of AI in cybersecurity*.

As we proceed with this assignment, you are encouraged to approach the task with both curiosity and a critical mindset, exploring the potential of AI in cybersecurity while remaining mindful of the ethical and practical considerations involved.

Generative AI Use: Throughout the assignment, there are suggestions on how to make more use of Gen AI. While you don't need to follow all of them, please try as many as you reasonably can. Feel free to try something, review the output, and selectively follow or not follow any of it.

Alternatives: As written, this assignment is oriented towards producing and analyzing a (primarily text) document using generative AI tools. If your team has other ideas, such as developing a GPT / prompt template for creating spear-phishing emails, please reach out to the instructors. The key criteria for this assignment is that the workflows you develop are primarily oriented towards producing and/or analyzing textual content.

2. Understanding the Assignment Context

This section focuses on establishing a solid foundation for your prompt engineering project in cybersecurity. Utilizing generative AI throughout this process can enhance your understanding and efficiency in creating the cybersecurity document.

2.1 Selecting the Type of Cybersecurity Document

- **Choose a Specific Document Type**
  - Decide on the type of cybersecurity document to create (e.g., policy guideline, threat assessment report, security protocol).
  - *Generative AI Use*: Leverage AI to generate examples or templates of different document types for inspiration and understanding of format and content.
- **Clearly Define the Purpose of your Document**
  - *Generative AI Use*: Utilize AI to simulate potential scenarios or use cases where the document might be applied, helping to clarify its purpose.

2.2 Identifying the Audience

- **Determine the Target Audience**
  - Clearly define who will read your document (e.g., security analysis, IT administrators, business executives, etc.).
  - *Generative AI Use*: Use AI to analyze similar existing documents and their audiences for insights into language, tone, and complexity.
- **Tailor Your Approach**
  - Adapt to the needs, expectations, and expertise of your audience.
  - *Generative AI Use*: Apply AI to create audience profiles or personas to better tailor the document's approach.

2.3 Understanding Key Cybersecurity Concepts

- **Research Relevant Topics**
  - Research topics related to your document type, including threats, best practices, and technologies.
  - *Generative AI Use*: Employ AI for quick and comprehensive gathering of recent articles, reports, and expert opinions on relevant cybersecurity topics.
- **Stay Current**
  - Ensure your understanding is current with the latest cybersecurity developments.
  - *Generative AI Use*: Use AI to provide summaries of the latest research, news, and trends in cybersecurity.

2.4 Setting Objectives for the Document

- **Define Clear Objectives**
    - Establish the goals of your document. What are the key pieces of information that your reader should step away with?
    - *Generative AI Use*: Utilize AI to brainstorm and refine objectives based on potential impacts and outcomes.
- **Align Objectives with Audience Needs**
    - Ensure the document's objectives meet your expected audience's needs using the information you defined in 2.2.
    - *Generative AI Use*: Apply AI to analyze feedback or responses to similar documents, aiding in aligning objectives with audience requirements.

3. Preparation Phase

In this phase, you will prepare for the actual creation of the cybersecurity document. Generative AI can play a significant role in assisting with the research and gathering of information, as well as in the selection of the right tools for prompt engineering.

3.1 Research and Information Gathering

- **Gather Relevant Information**
    - *Generative AI Use*: Utilize AI to conduct comprehensive and efficient research, aggregating information from various sources, including academic papers, industry reports, and online databases.
- **Analyze Cybersecurity Trends and Best Practices**
    - *Generative AI Use*: Employ AI for data analysis and trend identification, summarizing complex cybersecurity datasets and highlighting key insights.

3.2 Selecting AI Tools and Platforms

- **Identify Appropriate AI Tools**
    - *Generative AI Use*: Use AI to compare and evaluate different AI tools and platforms, providing recommendations based on features, ease of use, and suitability for the task.
- **Familiarize with Tool Capabilities**
    - *Generative AI Use*: Leverage AI to access tutorials, guides, and user reviews to quickly get up to speed with the chosen tools.

3.3 Developing a Conceptual Framework

- **Outline the Document Structure**
    - *Generative AI Use*: Apply AI to generate sample outlines or frameworks based on the document type, aiding in structuring the content effectively.

- **Identify Key Themes and Topics**
    - *Generative AI Use*: Use AI to analyze similar documents and extract common themes and topics, providing a starting point for content development.

3.4 Establishing a Timeline for Project Organization

- **Create a Project Timeline**
    - Identify the tasks that will need to be completed to develop your document, and assign roles to individuals within your team..
    - *Generative AI Use*: Utilize AI to generate a project timeline, taking into account the complexity of the task and any deadlines.
- **Allocate Time for Review and Revision**
    - Consider how long each component is expected to take. Take note of when and why you over-run time estimates when developing your document.
    - *Generative AI Use*: Employ AI to estimate the time needed for each phase of the project, ensuring a balanced and realistic schedule.

4. Content Generation and Refinement

This part of the assignment encompasses both the creation of the initial draft using prompt engineering and the subsequent refinement of the AI-generated content to produce a coherent and accurate cybersecurity document.

4.1 Crafting Prompts and Generating Content

- **Develop Effective Prompts & Templates**
    - Create clear, specific prompts aligned with your document's objectives and iteratively refine them based on AI feedback.
    - *Generative AI Use*: Leverage AI to generate examples of effective prompts and to analyze their effectiveness, suggesting refinements for better content alignment.
- **Generate Initial Draft with AI**
    - Use the selected AI tool with your prompts to produce the initial content, focusing on relevance and coherence.
    - *Generative AI Use*: Employ the AI tool to explore different content options and to provide initial evaluations of the generated content.

4.2 Reviewing and Refining the Content

- **Critical Assessment of AI-Generated Content**
    - Evaluate the AI-generated content for accuracy, relevance, and completeness.

    - *Generative AI Use*: Utilize AI to highlight areas in the content that align well with the objectives, as well as those requiring adjustments.
- **Incorporate Human Expertise**
    - Refine the content by integrating your cybersecurity knowledge, ensuring the document meets professional standards.
    - *Generative AI Use*: Apply AI to assist in organizing and structuring the content, while you focus on adding depth, accuracy, and context.

4.3 Finalizing the Document

- **Enhance and Polish the Content**
    - Ensure that the document is coherent, logically structured, and professionally presented.
    - *Generative AI Use*: Use AI to suggest improvements in language, flow, and presentation, with limited manual editing.
- **Create a Cohesive and Comprehensive Document**
    - Ensure that the final document effectively communicates objectives identified in 2.4. Keep the document as concise as possible – try to avoid redundancies in information and text.
    - *Generative AI Use*: Leverage AI for a final review, checking for consistency, clarity, and overall quality.

5. Critical Analysis, Reflection, and Self-Assessment

This part of the assignment emphasizes a comprehensive review of the AI-generated cybersecurity document, personal reflection on the process, and a self-assessment of individual contributions and learnings, with generative AI aiding each step. You should engage in individual reflection for a written reflection statement, but also discuss your thoughts as a team to prepare for the presentation.

5.1 Analyzing the Effectiveness of the AI-Generated Document

- **Evaluate Content Accuracy, Quality, and Relevance**
    - How appropriate is the generated information?
    - *Generative AI Use*: Utilize AI tools for content analysis, providing rubrics on readability, quality, and relevance to support your evaluation.
- **Identify Strengths and Weaknesses**
    - What are the benefits of using generative AI in your workflow? What were the drawbacks?
    - *Generative AI Use*: Work with the AI tools to list potential strengths and weaknesses that you can compare your experience with.

5.2 Reflecting on the Process and Team Collaboration

- **Reflect on the Prompt Engineering Process**
    - *Generative AI Use*: Use AI to retrospectively analyze prompt performance, offering insights for reflection.
- **Assess Team Dynamics and Individual Contributions**
    - *Generative AI Use*: Employ AI to analyze team communication patterns and individual contributions, aiding in a more objective self-assessment. Be sure that any messages are not saved by the AI. Alternatively, have the AI offer suggestions about positive and negative team experiences that could have occurred, and compare them with your experiences.

5.3 Ethical, Practical, and Personal Considerations

- **Ethical and Practical Implications**
    - *Generative AI Use*: Work with the AI tools to list potential ethical and practical implications of your project, and reflect on these options.
- **Personal Insights and Growth**
    - *Generative AI Use*: Leverage AI as a reflective tool, generating prompts for introspection and aiding in articulating personal insights and learning experiences.

6. Presentation, Submission, and Individual Reflection

This part of the assignment involves the final steps of submitting your team's cybersecurity document, submitting the individual reflection report, and delivering a class presentation.

6.1 Submitting the Cybersecurity Document

- Submit the document to the “**Project 1: Document**” assignment on MyCourses
    - **Deadline**: **Monday, Feb. 5, 5:00 pm**

6.2 Class Presentation

- **Prepare a Team Presentation:** Collaboratively create a presentation that summarizes the key aspects of your cybersecurity document and the process of creating it.
    - *Presentation Content*: Include an overview of the document, the prompt engineering process, the role of AI, and key findings or insights.
        - Presentations should be 10-12 minutes, not including time for Q&A
    - *Assign Roles and Responsibilities*: Determine each team member's role in the presentation to ensure a cohesive and well-organized delivery.

    - *Generative AI Use*: Use generative AI tools to assist in developing the presentation. AI can help with creating outlines, generating visual aids, suggesting talking points, and even providing feedback on practice runs.
- **Deliver the Presentation:** Present your team's work to the class, demonstrating clear communication, teamwork, and an understanding of the assignment's objectives.
    - Presentations will be on Feb. 6 and Feb. 8 in class
    - *Engage the Audience*: Aim to engage your classmates and instructor, inviting questions and discussion about your project.
    - *Generative AI Use*: Consider using AI tools during the presentation for real-time assistance, such as providing additional data, answering complex questions, or adapting the presentation based on audience reactions.
    - Submission: Submit the team's slides to the "**Project 1: Slides**" assignment on MyCourses
        - **Deadline:** **Thursday, Feb. 8 at 5 pm**, but just submit them once delivered

6.3 Individual Reflection Report

- **Personal Analysis:** Write an individual reflection report that analyzes experiences with generative AI, your personal contribution to the team project, and your learning from the process. Part 7 includes some suggested
    - *Reflection on the Use of Generative AI:* Consider the role and impact of generative AI in the project. Reflect on how AI assisted in the process, its effectiveness, and any challenges encountered in integrating AI with team efforts.
    - *Reflect on Team Dynamics*: Discuss how you collaborated with your team members, including any challenges and how they were overcome.
    - *Evaluate Your Contribution*: Assess your own contributions to the project, reflecting on your strengths and areas for improvement.
    - *Generative AI Use*: Utilize generative AI tools to help structure and articulate your reflections. AI can provide prompts for self-analysis, help organize thoughts, and even suggest language for effectively communicating your experiences and learnings.
- **Submission:** Submit your individual reflection report to the "**Project 1: Reflection Report**" assignment on MyCourses.
    - **Deadline:** **Friday, Feb. 9, 5:00 pm**