From Legacy to Compliant: Investigating the Role of ChatGPT in Aligning Cybersecurity Requirements to ISO Standards

Tyler Thomas Procko, Timothy Elvira, Omar Ochoa
Department of Electrical Engineering and Computer Science
Embry-Riddle Aeronautical University
Daytona Beach FL, USA
{prockot, elvirat}@my.erau.edu, ochoao@erau.edu

Abstract—**In software engineering, cybersecurity concerns are among the most overlooked and neglected during requirements elicitation, despite modern systems being always online and vulnerable to a number of cyber threats. The Software Engineering Body of Knowledge, derived from the insight of dozens of practitioners over decades, gives practical guidance to software engineers, but even this well-established document lacks guidance on the formation of correct cybersecurity requirements. The international family of standards, ISO/IEC 27000, defines guidance on the implementation of information security systems. Being a natural language guide on this specific topic, it may be used as the basis in few-shot prompting with large language models. With the reasoning capabilities of GPT-4, we posit that it is possible to 1) generate new cybersecurity requirements and 2) refactor old cybersecurity requirements that are compliant with a defined standard, e.g., ISO/IEC 27001, NIST, etc. To this end, we present an approach that utilizes GPT-4 through the OpenAI API in combination with parsed cybersecurity standard documents to elicit and refactor compliant cybersecurity requirements. These standards are general in nature; given the instructional prompting ability of GPT-4, it is possible that highly specific standards, for niche sub-domains in cybersecurity or otherwise, could be integrated with the proposed approach.**

Keywords—GPT, cybersecurity, software requirements, ISO 27000

I. Introduction and Background

The establishment of well-defined, correct requirements for software engineering applications is essential to the proper formation of software products. Requirements dealing with explicit functionality are typically given the most consideration during the requirements elicitation phase of the Software Development Life Cycle (SDLC), while other, less salient facets of software applications are neglected. One of the most consistently overlooked software requirement areas is that of cybersecurity. Explicit software functionality is given precedence, allowing cybersecurity concerns to fall to the wayside. This is ominous, as contemporary software applications integrate with a wider range of new systems and applications with every passing day. The Internet of Things (IoT) is a worldwide, interconnected cyberphysical system, where software applications and hardware devices interact over the Internet with one another. This vast interconnectedness highlights the issue underlying traditional software development: with cybersecurity concerns overlooked during requirements formation, software systems are vulnerable to cyberattacks from any number of assailants. Because of the distributed nature of the Internet, many cyberattacks can happen across continents and without recourse for affected systems.

The Software Engineering Body of Knowledge provides guidance for software practitioners operating in any facet of the SDLC; but considerations on cybersecurity requirements, are minimal [1]. The International Organization for Standardization / International Electrotechnical Commission (ISO/IEC), an independent, non-governmental organization, concerns itself with the development of technical standards in a variety of domains, including information security, of which cybersecurity concerns are a part. The ISO/IEC 27000 document family provides information security experts with well-established nomenclature, guidelines, techniques and insight. ISO/IEC standards ultimately resolve as semi-structured text documents, in the form of PDFs.

With the advent of the Transformer architecture in 2017 [2], Deep Learning (DL) natural language applications entered a zeitgeist of mainstream fascination and scientific proliferation. Perhaps the paragon of the Transformer-based DL models, the Generative Pre-trained from Transformers (GPT) Large Language Model (LLM), is currently in its fourth major version, titled GPT-4 [3, 4, 5]. GPT-4 is capable of complex tasks, given instruction in the form of natural language prompts [6]. GPT-4 is also capable of ingesting large quantities of data in its "memory", called context length or context window, allowing users to provide it with entire articles or book sections.

Because of the instructional-generative ability of GPT-4, and the natural language serialization of both ISO/IEC standards and software requirements, we propose that it is entirely feasible to automatically bring cybersecurity requirements into compliance with international standards. By prompting GPT-4 with example standard text, e.g., ISO/IEC 27001, and following up with prompts about particular, novel requirements, GPT-4 can engender ISO compliance. This proposal is directed to the party overseeing the Cybersecurity Grant of OpenAI, which was opened on June 1, 2023 [7]. In the following section, we propose an approach that leverages GPT-4 to automatically elevate software cybersecurity requirements into compliance with international standard documents.

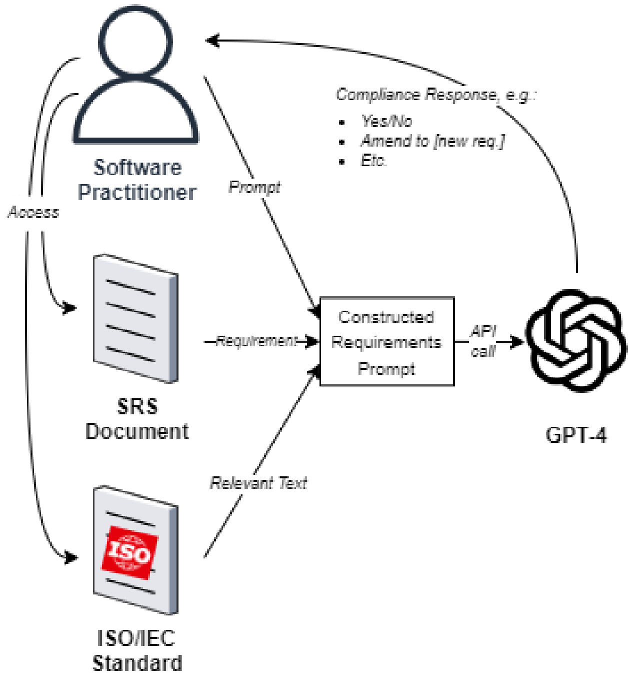

Fig. 1 The proposed GPT-enabled ISO cybersecurity requirement compliance approach.

II. Proposal

This section details the proposed approach. It should be noted that, where specific standard documents are mentioned, e.g., ISO/IEC 27001:2022, it is possible that alternative standard documents can be used, not just the one stated. This is on account of the ability of GPT-4 to respond to one- or few-shot prompts with new and unseen data. Some of these considered alternative documents are given in subsection B.

With this proposal, we aim to answer the following Research Questions, which may be refined and expanded upon as the research progresses:

<u>RQ1:</u> How can GPT-4 assist in improving cybersecurity specifications without including examples in the prompt?
<u>RQ2:</u> What process can guide GPT-4 in transforming extant cybersecurity specifications to be compliant with ISO/IEC standards?

A. *GPT-enabled ISO Cybersecurity Compliance Approach*

The proposed approach would allow for the semi-automated generation of ISO-compliant cybersecurity requirements by leveraging GPT-4 as a sort of digital cybersecurity consultant and software engineer. Three pieces are needed to effectively prompt GPT-4 for requirements:

1. The software practitioner
2. The Software Requirement Specification (SRS) document
3. The ISO/IEC standard(s)

In an interactive Web session with GPT-4, the model would be input with the ISO/IEC standard document(s), and thereafter prompted dynamically, as needed. In the semi-automated approach, with OpenAI's API, given an SRS and the relevant ISO/IEC standard document, the software practitioner would prompt GPT-4 with relevant section(s) from the ISO/IEC document(s), asking for a compliant requirement in response, striving to fit within the token length of GPT-4.

Conceptually, the proposed approach can be reduced to establishing appropriate prompts for GPT-4, as GPT-4 performs the heft of the work in creating cybersecurity requirements compliant with ISO/IEC. As such, it is of the greatest necessity to ensure appropriate prompts for GPT-4, by leveraging effective prompt engineering techniques.

There is a plethora of techniques in the novel discipline of prompt engineering that aim to improve the accuracy of LLM outputs. One that stands out in particular as applicable to the problem presented in this proposal is Chain-of-Thought prompting, which occurs when an LLM is instructed with an example chain of thought, or is asked to provide its chain of thought before asserting an answer to a query [8]. This method of prompting has led to impressive results in mathematical reasoning and is also applicable generally to any sphere of interest. An earlier paper presents the Secure and Usable Requirements Engineering (SURE) method for establishing good software security requirements [9]. SURE breaks down the formation of requirements into three steps, in a process called refinement:

1. Security Statement
2. Security Need(s)
3. Security Requirement(s)

Security statements are simple, general expressions of what the system should do; they require no expert knowledge about security practices. Security needs are derived from security statements, and security requirements from security needs. This stepwise approach is sensible and can be emulated by prompting GPT-4 to explain its breaking down of stated cybersecurity needs into requirements.

B. *Identified Standard Documents*

As proof of concept, and because there are so many standards available, we have identified and selected four ISO/IEC standard documents that are applicable to the definition of cybersecurity requirements. These standard documents are well-established and, in most cases, internationally recognized. Of primary interest is the ISO/IEC 27000 standard family, which defines best practices for information security management. Formed even before ISO/IEC, the National Institute of Standards and Technology (NIST) has the Framework for Improving Critical Infrastructure Cybersecurity, which contains useful techniques for organizations seeking improved cybersecurity. Similarly, the Information Assurance for Small and Medium-sized Enterprises (IASME) is a simple and affordable set of guidelines and certifications for regular companies seeking cybersecurity standardization [10]. IASME is an ISO 9001 (quality management) certified organization, so their document is well-established and useful. Table *I* presents the selected standard documents.

Table I. Identified standard documents of relevance.

Standard	Content
ISO/IEC TS 19608:2018	Guidance for developing security and privacy functional requirements based on ISO/IEC 15408
ISO/IEC 27001:2022	Information security management systems – Requirements
ISO/IEC 27032:2012	Information technology – Security techniques – Guidelines for cybersecurity
ISO/IEC 27701:2019	Security techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines
NIST Cybersecurity Framework version 1.1	Ensuring organizational cybersecurity
IASME Cyber Assurance Standard version 6.0	Ensuring organizational cybersecurity

There are other established ISO/IEC standard documents that may be relevant, but were not chosen for this work, as it is exploratory in nature. These include: 27002:2022, 27003:2017, 27013:2021, TS 27100:2020, TR 2710:2018 and TS 27110:2021. These documents could be considered in future work.

C. Approach

We propose to begin testing the ability of GPT-4 in generating ISO-compliant cybersecurity requirements by experimenting with the standard documents defined in Table I. To maintain a relatively controlled study, we propose to use an SRS for a real-world software system used as instruction material in a university course; this SRS includes cybersecurity requirements that can be evaluated and brought into compliance with ISO/IEC.

It is necessary to formulate an objective means of evaluating the cybersecurity requirements output by GPT-4 in the proposed approach. Aside from human expert evaluation, high quality requirements specifications should consider the 3 Cs of developing production level software requirements specification: consistency, completeness, and correctness [11]. There are guidelines in ensuring requirements adhere to 3 Cs of high-quality software requirements .

III. Request and Project Plan

To complete the research and implementation for this project, we propose an expected completion date of January 31, 2024. This allots a time of approximately eight months, from proposal submission to project finalization.

A. Project Timeline

Below is the proposed timeline for the project; this is a very forward-looking timeline that will be flexible as research progresses and findings change. Notwithstanding, the dissemination of a research article by the end of January 2024 is planned for, in order to justify the funding by OpenAI and to bring fresh and unique insight to the scientific community.

- July 2023 - Fine-grained survey of the research landscape, particularly on cybersecurity requirements and other cybersecurity standards/bodies of knowledge
- August 2023 - Parsing of selected standard documents, baseline cybersecurity knowledge evaluations of GPT-4 prompting
- September 2023 - Definition of "good" or baseline cybersecurity requirements, and preliminary tests with GPT-4 in generating requirements without provided standards (zero-shot prompting) to obtain performance baselines
- October 2023 - Formation of API interface and file system management; begin experimental prompts with standard documents
- November 2023 - Experimental prompting, data collection and results analysis
- December 2023 - Further experimental prompting, preliminary writeup
- January 2024 - Final writeup and submission to publication outlet
- February 2024 - Publication deliberation, feedback
- March 2024 - Final submission, travel and presentation

Given the proposed timeline, we look to publishing in the 8th International Conference on Innovation in Artificial Intelligence (ICIAI 2024), which is scheduled to occur in March of 2024 in Tokyo, Japan. There are a number of other reputable conferences with similar timeframes, but ICIAI is the preferred fit and has a desirable reputation and publication impact.

B. Request

First, we request a monetary amount of $714.08 USD to obtain access to the four selected ISO/IEC standard documents. Additionally, we request the remainder of the stated maximum allowance for the OpenAI Cybersecurity Grant: $10,000 worth of API credits (or equivalent) [7]. Given the price of the requested ISO/IEC standard document, this amounts to $9,285.92 in token credits. The token credits will be directly used in the project with GPT-4. The requested funding is the stated maximum increment, because of the price of GPT-4, in addition to the fact that the documents being parsed often exceed 50 pages in length, so API credits will be expended rapidly. If OpenAI's advancement allows it, *we would also like to access GPT-4's 32k context model*, to allow better ingestion of large standard documents. This would accelerate token use considerably. So saying, we request OpenAI’s stated maximum funding increment of $10,000 in equivalent value.

Table II. Breakdown of requested funding.

Request	Amount (USD)
ISO/IEC TS 19608:2018	$184.35 [12]
ISO/IEC 27001:2022	$137.71 [13]
ISO/IEC 27032:2012	$184.35 [14]
ISO/IEC 27701:2019	$207.67 [15]
OpenAI API token credits	$9,285.92 (equivalent)
Total Requested	$10,000 (equivalent)

Please note that the prices for the listed standard documents are estimated in USD from the original ISO/IEC Swiss Franc (CHF) prices.

IV. Conclusion

What has been proposed is the motivation and approach of a GPT-enabled system that is capable of automatically lifting software cybersecurity requirements into compliance with international standards, e.g., those in the ISO/IEC 27000 family.

Additionally, because of the generalized knowledge of GPT-4, and its ability to "learn" from examples in prompts, it is feasible that forays into other domains of interest can occur. ISO/IEC standards exist for software quality, e.g., ISO/IEC 25010:2011, Systems and Software Quality Requirements and Evaluation (SQuaRE). Such a standard could be used in the proposed approach for evaluating code quality, by adjusting the prompts to GPT. Any number of use cases and standard documents can be cited, but the approach for doing so, grounded on an empirically evaluated use case, ensuring cybersecurity requirement compliance with ISO/IEC 27000 standards, is the concrete starting point. The implementation and testing of the approach remain an open request to the OpenAI Cybersecurity Grant program, on which the research depends for sponsorship.

The authors all have experience in using OpenAI's GPT API to improve aspects of software engineering or machine learning. Two authors were early adopters of GPT, having experience with the nascent Davinci models. Additionally, all three authors are experienced in publication and dissemination in top journals and conferences and fully intend to publish an empirical report on the use of GPT in establishing cybersecurity requirement compliance with ISO/IEC standards.

We believe the fulfillment of this proposal will lend to improving 1) the dearth of consideration for cybersecurity requirements in the SDLC and 2) the credibility of GPT, and LLMs in general, because of the integration with high-grade, premier standards like those proliferated by the august ISO/IEC group. The association of GPT and the OpenAI organization with federated, international standards through empirical research is surely an aspect of interest.

V. References

[1] P. Bourque and R. E. Fairley, "Guide to the Software Engineering Body of Knowledge, Version 3.0," IEEE Computer Society, 2014. [Online]. Available: www.swebok.org.

[2] A. Vaswani, N. Shazeer, N. Parmar, J. Uszkoreit, L. Jones, A. N. Gomez, Ł. Kaiser and I. Polosukhin, "Attention Is All You Need," *Advances in Neural Information Processing Systems* , vol. 30, 2017.

[3] A. Radford, K. Narasimhan, T. Salimans and I. Sutskever, "Improving Language Understanding by Generative Pre-Training," 2018.

[4] A. Radford, J. Wu, R. Child, D. Luan, D. Amodei and I. Sutskever, "Language Models are Unsupervised Multitask Learners," *OpenAI Blog,* vol. 1, no. 8, p. 9, 2019.

[5] T. Brown, B. Mann, N. Ryder, M. Subbiah, J. D. D. P. Kaplan, A. Neelakantan, P. Shyam, G. Sastry, A. Askell, S. Agarwal, A. Herbert-Voss, G. Krueger, T. Henighan and R. Child, "Language Models are Few-Shot Learners," *Advances in neural information processing systems,* vol. 33, pp. 1877-1901, 2020.

[6] OpenAI, "GPT-4 Technical Report," vol. arXiv 2303.08774, 2023.

[7] B. Rotsted, G. Sastry, H. Nguyen, G. Bernadett-Shapiro and J. Parish, "OpenAI cybersecurity grant program," 1 June 2023. [Online]. Available: https://openai.com/blog/openai-cybersecurity-grant-program.

[8] J. Wei, X. Wang, D. Schuurmans, M. Bosma, E. Chi, Q. Le and D. Zhou, "Chain of thought prompting elicits reasoning in large language models," *arXiv preprint arXiv:2201.11903,* 2022.

[9] J. Romero-Mariona, H. Ziv, D. J. Richardson and D. Bystritsky, "Towards Usable Cyber Security Requirements," *Proceedings of the 5th Annual Workshop on Cyber Security and Information Intelligence Research Cyber Security and Information Intelligence Challenges and Strategies - CSIIRW '09,* 2009.

[10] "THE IASME CYBER ASSURANCE STANDARD V6.0," IASME Consortium Limited, 2022.

[11] M. Kamalrudin and S. Sidek, "A review on software requirements validation and consistency management," *International Journal of Software Engineering and its applications,* vol. 9, no. 10, pp. 39-58, 2015.

[12] "ISO/IEC TS 19608:2018," ISO, [Online]. Available: https://www.iso.org/standard/65459.html. [Accessed June 2023].

[13] "ISO/IEC 27001," ISO, [Online]. Available: https://www.iso.org/standard/27001. [Accessed June 2023].

[14] "ISO/IEC 27032:2012," ISO, [Online]. Available: https://www.iso.org/standard/44375.html. [Accessed June 2023].

[15] I. 27701:2019, ISO, [Online]. Available: https://www.iso.org/standard/71670.html. [Accessed June 2023].

Author Information

Tyler T. Procko – PI

Mr. Procko graduated ERAU in 2020 as a software engineer. He has over five years' experience in applied Ontology, Linked Data and Semantic Web work. Currently, he is pursuing his Ph.D. in Electrical Engineering and Computer Science under the auspices of the Department of Defense through the Science, Mathematics and Research for Transformation (SMART) scholarship program. Mr. Procko spends each summer participating in research at the Air Force Research Lab's Information Directorate in Rome, New York. His dissertation centers around the use of ontologies and NLP to enrich the research process, with a use case in the software development life cycle.

Timothy Elvira – Technical Lead

Mr. Elvira graduated from ERAU as a software engineer in 2020. He has over five years' experience in Deep learning applications. Currently, he is pursuing his PhD in Computer Science funded by the Department of Defense through the Science, Mathematics and Research for Transformation (SMART) scholarship program. Mr. Elvira spends each summer participating in research at the Air Force Research Lab's Information Directorate in Rome, New York. Mr. Elvira's dissertation direction aims at integrating traditional software engineering practices into the ML workflow to better facilitate the engineering, validation, and verification of ML models.

Omar Ochoa – Advisor and Consultant

Faculty Advisor, Dr. Ochoa is an Associate Professor of Software Engineering and Computer Science at ERAU. He has over 10 years of experience working in industry: the Army Research Laboratory, IBM, and Hewlett Packard Enterprise. Currently, Dr. Ochoa is PI on NSF #2221602 "Expanding the Nation's STEM Talent Pool by Accelerating Graduate Degree Completion in Computer, Software, and Cybersecurity Engineering" and Co-PI on NSF #1920780 "Using Scrum to Develop an Agile Department", Co-PI on NSF #2146462 "CyberCorps Scholarship for Service: High-skilled Workforce Development for the Aviation and Aerospace Cybersecurity Domains", Co-PI on FAA funded project titled "Cybersecurity Training Curriculum Development", PI in Navy funded SBIR Phase II titled "ACTER – Air Traffic Cloud-based TrainER" and PI in AFWERX funded SBIR Phase II titled "Simulation Based Predictive Analytics for Enhanced Autonomy and Artificial Intelligence Collaboration"