Contribution ID: **18** Type: **Poster Presentation**

Open source software security application intelligence acquisition based on Large Language Model

With the rapid development of information technology, an increasing number of open-source software is widely used across various domains, significantly reducing development costs and enhancing production efficiency. However, as the number of open-source software continues to grow, the software supply chain becomes more complex, and the associated risks are also increasing. Therefore, obtaining timely intelligence related to the secure application of open-source software is critically important. However, the predominant method for most individuals to obtain security intelligence for open-source software is primarily through the use of scanning tools or querying relevant websites and platforms. This approach requires them to invest a significant amount of time and incur higher costs. To address this issue, this paper proposes an intelligent method for obtaining security intelligence for open-source software based on a large language model. Users only need to interact with our application in a conversational manner, posing questions related to security intelligence for open-source software, and our application can provide accurate answers.

The core design concept of our application involves integrating the Chain of Thought (CoT) technology with a large language model-based Agent, endowed with reasoning and tools usage capabilities. As is well known, large language models obtained through massive-scale unsupervised deep learning are a black box, where the reasoning decision chain is not transparent, making the model results less trustworthy. However, Chain of Thought technology breaks down a logical reasoning problem into multiple steps, proceeding step by step. This generates results with a clearer logical chain, providing a degree of interpretability, allowing us to understand how the answers are derived. In our application, the large language model, through Chain of Thought technology, decomposes logical reasoning problems into multiple steps, progressively resolved by the Agent. At each step, our Agent can automatically invoke API tools, providing parameters in accordance with the API input to obtain answers to the posed questions, subsequently confirming the final resolution through observation. By using our application, software developers and businesses can easily obtain security intelligence for open-source software, stay informed about the security status of the software, assess and manage security risks in the software supply chain, and then take appropriate security measures.

Primary author: YUAN, Xinyang (Computing Center, Institute of High Energy Physics, Chinese Academy of Sciences, Beijing 100049, P.R.China; School of Nuclear Science and Technology, University of Chinese Academy of Sciences, Beijing 100049, P.R.China)

Co-authors: WANG, Jiarong (Institute of High Energy Physics); ZHAO, Haozhi (Institute of Automation, Chinese Academy of Sciences); SUN, Qianran (Computing Center, Institute of High Energy Physics, Chinese Academy of Sciences, Beijing 100049, P.R.China; School of Nuclear Science and Technology, University of Chinese Academy of Sciences, Beijing 100049, P.R.China); LIU, Yu (Zhengzhou University); YAN, Tian (IHEP); QI, Fazhi (Institute of High Energy Physics,CAS)

Presenter: YUAN, Xinyang (Computing Center, Institute of High Energy Physics, Chinese Academy of Sciences, Beijing 100049, P.R.China; School of Nuclear Science and Technology, University of Chinese Academy of Sciences, Beijing 100049, P.R.China)

Track Classification: Track 10: Artificial Intelligence (AI)