中央研究院 資訊科學研究所

112年暑期實習生實習報告 (工作時間7/1~8/31)

|  |  |  |  |
| --- | --- | --- | --- |
| 姓名 : 白宗民 | 學校：台灣大學 | | 系所/主修: 電機工程學系 |
| 計畫主持人姓名 : 陳孟彰教授 | Email：b09602017@ntu.edu.tw | | |
| 實習內容簡要 | | 資安、機器學習 | |
| 這次經歷是否符合您的預期?  請說明。 | | 是，非常滿意且符合。 | |
| 總體評量 | | 回顧這段充滿學習和探索的旅程，我不禁感到由衷的滿足。從一開始對資訊安全領域毫無了解，到現在能夠自信地應對各種技術挑戰，雖然可能還是要花很多時間去查詢資料，但我的能力在這段過程中得到了顯著的提升。  首先，資訊安全領域的知識是我這段旅程的起點。從MITRE ATT&CK、TRAM到攻擊思維的理解，我打開了資安領域的大門。在技術層面，我掌握了眾多工具和框架，如Selenium、Docker、os、PyTorch、DGL等。這些工具在我解決問題和執行任務時提供了強大的支持。我能夠使用Selenium進行自動化處理，運用Docker來管理環境，並運用PyTorch和DGL來訓練自己的模型。這些技能的提升不僅讓我在學習上更加得心應手，也為我未來在技術領域的發展奠定了穩固的基礎。  此外，我在資料分析和處理方面也有了顯著的進步。從收集資料、分析數據、處理格式到進行資料前處理，我逐步建立了一個完整的流程。這些能力不僅對於機器學習專案有所助益，也在解決日常問題時提供了寶貴的支援。  最後，我還提升了每週產出output的能力，讓我在團隊合作中表現得更加出色。我能夠清晰地向團隊呈現我所完成的工作，這不僅鍛煉了我溝通的能力，也讓我更加自信地參與到團隊的討論和決策中。 | |
| 給自己的分數 | | 60 | |
| 【成果報告】-  **從自動化處理到機器學習：跨足資安領域的學習之旅**  我認為加入中研院暑期實習使我收穫良多，從一個完全陌生的領域出發，我開始了一段充滿挑戰和驚喜的學習之旅，並在過程中進一步拓展了我的技能和視野。我的主題聚焦在資訊安全以及機器學習，資安是我以前從未接觸過的領域。然而，我經過一系列的學習和實踐，成功地將自己的技能從一開始的網站自動化處理延伸到了機器學習，成就了這段不平凡的旅程。  一開始，我對於資訊安全的概念一無所知。然而，當我接觸到MITRE ATT&CK這兩個名詞時，我仿佛打開了通向一個新世界的大門。這些概念揭示了攻擊者的思維和策略，讓我對於資安領域的重要性有了更深刻的理解。這也是我開始自動化處理安全操作的起點，我使用Selenium工具，模擬如何獲得NLP訓練資料的行為，這也是之前在學校助教都會幫我們處理好的事情，有了這個經驗後，使我更貼近實際情境，並鍛煉了我的技能。  然而，我的探索並未止步於此。在加入euni學姊的專案後，我有機會參與訓練GNN模型，以及做了一大堆資料處理的事情，這在以往我是完全沒有接觸過的，尤其是將graph視覺化出來，在看到成果的那一瞬間真是非常滿足，也覺得自己成長了許多。而將機器學習引入了資訊安全的領域的這一階段讓我接觸到了GAT、GCN、Graphormer等模型，這些模型對於處理複雜的圖結構具有獨特的優勢。透過這些模型，我學習了更多以前可能有接觸過的名詞，但在這邊加入了更多得自己的思考，要思考這個layer可以為我們的任務帶來什麼，思考如何讓模型吃到我們的資料，思考如何讓訓練收練的更好，因此我得以更深入地分析資安問題，同時也為我未來在機器學習領域的探索打開了一扇大門。  我也想要特別感謝英仁學長以及國維學長，他們在這段學習過程中給予了我寶貴的協助和指導。他們的專業知識和耐心解答，讓我更深入地了解了機器學習以及資安這個領域。這種導師式的學習方式，不僅讓我學到了知識，更在解決問題的過程中培養了我的自信心，我想在之後的日子裡，這些知識也會陪伴我走過更加艱辛的道路。  當然還要感謝教授每個禮拜的會議都出席並且給於我們建議，給了我們一些在這個層級不會思考到的問題，老師在會議上的態度也讓人非常自在不會緊張，寄信問老師問題老師也都迅速回復，非常謝謝老師給了我這次機會來到實驗室學習，非常希望能夠繼續向老師學習！  通過從網站自動化處理到機器學習的學習之旅，我不僅增加了自己的技術實力，也培養了持續學習和解決問題的能力。這段旅程讓我更加自信地展望未來，我深信著自己在技術道路上將有更大的突破。  了解了MITRE ATT&CK、TRAM、GAT、GCN、Graphormer後，它們豐富了我的知識庫，讓我在未知領域中能夠穩步前行。同樣對於Selenium、NetworkX、OS、Pandas、NumPy、DGL、PyTorch等工具，我也可以在以後的任務中更加熟稔的使用它們，一切都是如此的有趣且實用。  總而言之，這段從自動化處理到機器學習的學習之旅不僅充實了我的技能，更讓我明白了持續學習和開拓的重要性。我將以更加堅韌的姿態，繼續前進，不斷挑戰自己，迎接更多的技術挑戰和成就。 | | | |

請寄至sat@iis.sinica.edu.tw，並副本給指導教授及所指導的研究助理/博後。