

國立台灣科技大學 114學年 第2學期 課程大綱

Spring 2026 NTUST Course Outline

授課教師：黃意婷

Instructor: Yi-Ting Huang

課程名稱：資訊安全與人工智慧分析

Course Title : Cybersecurity and AI-based Analytics

2026/6/22

<p>課程代號： EE5515701 Course Code 學分數： 3 Credits</p>	<p>必選修：選修/半學年 Required/Elective: Elective/Half Yr. 先修課程： Prerequisites</p>
<p>節次教室： W2(EE-B03) W3(EE-B03) W4(EE-B03) Time/Location</p>	
<p>專業核心能力： Core Professional Competencies</p> <ul style="list-style-type: none"> <input type="checkbox"/> 資料蒐集、研讀、整理、策劃、設計、系統整合及執行專題研究之能力 <input type="checkbox"/> 創新思考及獨立解決問題之能力 	
<p>課程網址： Course Website</p>	
<p>課程宗旨： Course Objectives</p> <p>此課程為進行人工智慧在資訊安全相關研究與專題的課程，給予學生對於現今人工智慧的在資訊安全上的攻擊、防禦等主題有深度的了解。課程涵蓋三個部分，第一部分會介紹惡意程式相關議題，包含動靜態分析、利用RNN、CNN等類神經網路的方法以偵測與分類惡意程式；在第二部分介紹紅隊演練模擬入侵攻擊，透過側錄系統事件行為、發展入侵檢測系統；第三部分介紹典型深度學習Embedding的演算法與Attention機制，作為防禦惡意威脅與資訊安全相關工具開發。</p> <p>透過這堂課的學習，同學能夠了解資訊安全在防禦、偵測、辨識等的研究議題，以及進一步的實作類神經網路模型在資訊安全相關研究上的任務。</p>	
<p>課程大綱： Outline of Lectures</p> <p>Part A: 電腦安全概念 惡意程式靜態與動態分析 深度學習基礎介紹 卷積神經網路於靜態分析 遞歸神經網路於動態分析和惡意郵件偵測</p> <p>Part B: 紅隊演練 系統安全稽核日誌 入侵檢測系統 攻擊偵測系統</p> <p>Part C: 詞嵌入與圖嵌入 編碼器-解碼器與注意力機制 Transformer & BERT</p>	
<p>授課方式： Method of Instruction</p> <p>講授 Lecture：% 分組討論 Group discussion：% 案例研討 Case study：% 操做練習 Practical exercises：% 講授 Lecture：%</p>	
<p>教科書： Textbooks</p>	

參考書目：
References

修課須知：
Notice

評量方式：
Grading

備註說明：
Notes