台灣資安菁英人才培育

蕭旭君[1]、黃俊穎[2]、鄭欣明[3]、黃世昆[2]、劉彥君[3]、吳宗成[4]
[1]國立台灣大學資訊工程學系、[2]國立交通大學資訊工程學系、
[3]國立臺灣科技大學資訊工程學系、[4]國立臺灣科技大學資訊管理學系
hchsiao@csie.ntu.edu.tw、chuang@cs.nctu.edu.tw、smcheng@csie.ntust.edu.tw、
skhuang@cs.nctu.edu.tw、lyc0421@gmail.com、tcwu@cs.ntust.edu.tw

摘要

隨著資訊安全的攻擊和防禦技術迅速發展與高度專業化，在高等教育中，特別是在業界所需的實務攻防技能方面，個別教師要跟上腳步，是非常具有挑戰性的。我們相信聯合具有不同技能的網路安全專業人員，讓學員透過協作式教學和學習的方式，可以克服這個挑戰，培養具實務能力的資安人才。

本論文介紹我們在台灣資安實務教育的協作教學和學習經驗。在過去四年裡，我們設計並實施了兩個實驗性的資安課程：一個是為期一週的暑期學校課程，旨在培養已有先備資安知識的學生，另一個則是跨校的大學正式課程，旨在有系統地指導學生修習基本的攻擊和防守技能。兩門課程都使用 Capture The Flag (CTF)作為測驗和評分的通用模式。我們強調設計決策，且探討了遇到的挑戰、經驗教訓以及可能的改進方向。

關鍵詞：AIS3、資安搶旗、EDU-CTF、資安實務教育

Advanced Security Education in Taiwan

Hsu-Chun Hsiao[1*], Chun-Ying Huang[2], Shin-Ming Cheng[3], Shih-Kun Huang[2],
Yen-Chun Liu[3], and Tsung-Cheng Wu.[3]
[1]National Taiwan University, [2]National Chiao Tung University,
[3]National Taiwan University of Science and Technology
hchsiao@csie.ntu.edu.tw、chuang@cs.nctu.edu.tw、smcheng@csie.ntust.edu.tw、
skhuang@cs.nctu.edu.tw、lyc0421@gmail.com、tcwu@cs.ntust.edu.tw

Abstract

As cyberattack and security technologies evolve rapidly and are highly specialized, it is challenging for individual instructors in higher education to keep up with the advancement, especially in practical offensive and defensive skills that are desired by the industries. We believe this challenge can be overcome through collaborative teaching and learning in which cybersecurity professionals with diverse skill sets can join force to cultivate talents.

This paper reports our experiences in collaborative teaching and learning for practical cyber

security education in Taiwan. Over the past four years, we designed and implemented two experimental security curricula: One is a week-long summer school program that aims to advance students who have prior knowledge in security, and the other is a cross-university semester course designed to guide students to systematically develop fundamental offensive and defensive skills. Both courses use Capture The Flag (CTF) as a common platform for assignments and evaluation. We highlight the design decisions and discuss the challenges encountered, lessons learned, and possible directions for improvements.

Keywords: AIS3、Capture the Flag、EDU-CTF、Practical security education

壹、前言

資訊安全始終是一個重要但容易被忽視的問題，人們通常對資安議題採取觀望的態度。然而，最近發生的資安事件再次喚醒了人們對電腦與系統安全的意識。近年來在台灣發生了兩起嚴重的安全事件，分別是 ATM 盜領和針對金融行業的 DDoS 攻擊。同時也有許多個人或企業用戶遭受了勒索軟體的威脅和 APT 攻擊，進而導致財務損失和機密資訊洩露。因此，人們開始意識到資安教育的投資對於防止個人、政府組織和行業被駭至關重要。

雖然對資安教育的需求不斷增長，但目前並沒有一個最有效且可靠的方法去教學資安概念和技能。在大學中，現有的資訊安全課程都側重於理論知識而不是現實世界的實務演練。然而，這些基本概念並不足以來應對企業組織面臨的實際挑戰。我們認為資安教育不該只是紙上談兵般的攻防，學生必須透過將資安觀念應用在解決實際發生的問題才能融會貫通他們所學到的知識。因此，由學術研究者和教育工作者帶頭去探索資安教學的新方法是必要的。

在本論文中，我們採用協作式教學和學習來激發學生學習資安技能的熱情。首先，我們說明對台灣資安威脅和教學的看法，然後介紹我們教授資安實務的嘗試。通過協作教學和學習，我們設計的課程整合了學術界、產業界和資安社群所提供的資源。

本文的章節安排如下。在第貳節中，我們提出了對台灣當前資安威脅和實務的觀察，並簡單概述了我們的課程設計原則和課程地圖，並介紹兩種不同類型的課程。第參節和第肆節分別介紹了我們的短期課程（AIS3）和長期課程（EDUCTF）。最後，在第伍節做了總結。

貳、背景

2.1 台灣的網路安全觀察

資訊安全意識不足。儘管在生活上嚴重依賴網路，人們依舊缺乏足夠的網路安全意識。根據 APWG 2016 年第四季度關於網路釣魚的趨勢報告，台灣有 38.98%的機器被惡意程式感染，排名世界第三[1]。除了一般的用戶外，企業的安全防護措施也非常不足，導致了嚴重的財務損失，也讓自身的聲譽下降。根據 FireEye 的報告統計，有六成的台灣企業在 2015 下半年遭受 APT 攻擊[2]。

重要卻脆弱的基礎建設。與世界上其他國家一樣，如銀行和政府的服務這樣至關重要的基礎建設，是台灣被攻擊的主要目標。2016 年 7 月，第一銀行的 41 台 ATM 機器被駭客入侵，偷走了 250 萬美元現金。犯罪團夥透過第一銀行在倫敦分支的錄音服務器滲透到銀行內網，控制設備管理系統向 ATM 發送惡意程式。透過這支惡意程式，讓駭客能遠端控制 ATM，拿走大量現金且刪掉 logs 不留下痕跡。在 2017 年 2 月，台灣有 13 家證券商受到 DDoS 威脅：攻擊者要求他們支付比特幣，否則將遭受 DDoS 攻擊。儘管 DDoS 攻擊峰值只有 2-3 Gbps，但他們仍然成功讓受害者網站在 20-60 分鐘內無法使用，通過上述的兩起事件，我們可以明顯觀察出這些重要的服務有多麼脆弱。

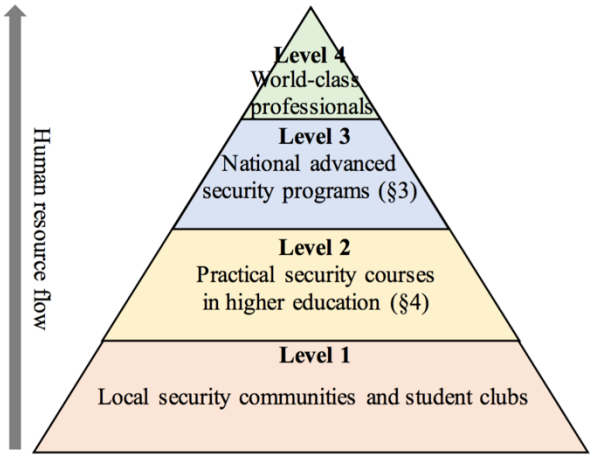
應變機制。這些嚴重的網路攻擊促成了一些政府作為，在 2016 年 8 月，政府為此成立了網路安全部門，並在隔年投入了超過一倍的預算來支持台灣的資安發展。其中一個關鍵的作為是促進各級安全教育：一般民眾、高中生、大學生、研究生以及專業發展。本文重點介紹大學環境中的進階安全教育，如第 2.2 節所述。

2.2 資安教育中的人力資源流動

圖一說明了我們對於台灣資安教育的人力資源流動的看法。我們認為人力的分級大致可分為四個階層。從下到上分別是：第一級：在地的資安社群和學生社團、第二級：高等教育中的資安實務課程、第三級：國家級的進階資安專案、第四級：世界級的專業人員。

儘管擁有這些充滿活力的在地社群（如 HITCON Community），但台灣依然擁有太少的世界級資訊安全專業人才，這種現象可能歸因於資安課程不足，這需要持續地系統性培養人才。

為了拉近在地社群與世界級專業人員之間的差距，我們設計並實施了兩個互補的資安實務課程：AIS3 課程（§3）和 EDUCTF 大學跨校課程（§4）。在下面兩節中，我們將詳細描述設計決策，以及從學員篩選、課程安排和教學團隊規劃所學到的經驗。



圖一：台灣資安教育的人力資源流動

參、AIS3 課程

3.1 歷史

新型態資安暑期課程（AIS3）是我們第一個嘗試拉近資訊安全理論與現實世界之間差距的專案。我們相信，像 Capture-The-Flag（CTF）這樣的實務駭客技能和遊戲化競賽將成為吸引學生學習資安技能的絕佳賣點，因此，我們在設計 AIS3 課程時考慮了三個基本原則。首先，每門課程皆必須包含講座和實際練習環節，並且課程邀請的講者皆來自學術機構、公司企業和資安社群；其次，我們希望跟資安公司合作，在課程中進行真實案例的研究；第三，我們為參加的學員舉辦了 CTF 競賽。

AIS3 課程首次於 2015 年舉行，這是台灣首個對所有大學生開放的資安課程。我們的第一次嘗試是成功的，有約 300 名學生報名，但是由於空間和人力資源有限，我們的教室只能容納 100 名學生，而每個學員必須攜帶自己的筆記型電腦，以便他們能夠在課堂上實際操作。經過兩週的課程培訓後，我們在課程的最後一天為所有正課學員舉辦了一場 CTF 比賽，讓他們能實際運用課程所學的知識。

為了讓更多的學生能參與，我們在 2016 年擴大了 AIS3 的課程規模，嘗試在北中南三區各找一所大學來舉辦，而非僅只在台北。三個教學點教授的是同樣的課程。這節省了大多數學生的交通和住宿費用，也因為這種多點授課的安排，我們將課程長度縮短為一週。2016 年我們依然有相同數量的學生來報名，最後有總共 170 名學生正式參與課程，在最後一天也安排了 CTF 比賽，讓在不同地區上課的學員都能一起參加。AIS3 課程的詳細資訊將在本節的其他部分介紹。

3.2 學員篩選 – Pre-Exam

由於報名的學生數量遠遠大於實際能提供的座位，於是我們使用了幾種機制來篩選報名的同學，除了根據推薦信和過去的 CTF 競賽經驗進行選擇外，我們還舉辦了 AIS3 Pre-exam 作為最關鍵的機制。Pre-exam 實際上是一個簡單的 CTF 比賽，報名的學生被要求必須先參加考試，來展現他們對 CTF 競賽和資安技能的了解。我們將 15 個問題分為五類：Misc、Crypto、Reverse、Pwn 和 Web，每個類別都有三個不同難度的題目，並且其所能獲得的分數分別為一到三分。報名的學生有 48 小時的時間來解題，並將獲得的 flag 上傳到 Pre-exam 的 CTF 平台上。

我們的經驗說明 Pre-exam 是對報名的學生進行篩選最有效的方式，因此我們計劃從 2017 年開始將 Pre-exam 作為選擇正式學員的唯一機制。雖然 AIS3 課程對所有對資安實務技能感興趣的學生開放，但 Pre-exam 的一個關鍵要素就是區分所有報名學生的程度，雖然有一些對資安技能掌握較多的學生，但也有一部分有熱忱的同學只是 CTF 的新手。在 2015 和 2016 年，我們注意到有少部分學生只解得出如“Hello World”般類似程度的問題，而無法解出其他的題目，Hello World 問題會在題目描述時就告訴參賽者正確的 flag，只要上傳這個 flag 即可獲得分數。為了區分出初學者的技能水平，我們打算提供更簡單的題目。因此在 2017 年後，我們增加了更多的題目，以提升學生程度的鑑別度。當 AIS3 課程向所有學生張開雙手時，讓不同程度的學生一起上課仍然是一個非常有挑戰的問題，我們仍在努力尋找能夠選出在報名人海中擁有潛力的學生的最佳方法。

3.3 課程安排

課程安排是 AIS3 的另一個挑戰。在前兩年，我們邀請了中央研究院和國立交通大學等學術機構的教授;也邀請了下列公司（按該企業的首字英文字母排序）：宏碁 Acer、戴夫寇爾 DEVCORE、大猩猩科技 Gorilla、Horangi、ICST、LINE、日本樂天 Lotte、聯發科技 MediaTek、NTT、趨勢科技 Trend Micro 和 Verint 台灣分公司;除此之外，我們也邀請了來自不同社群的講者，包括 HITCON（台灣）、PPP（美國）和 SECCON（日本）。得到這些社群的支持也是一個很好的宣傳，實際上，由於這些來自社群的著名講者，更吸引了學生來參加 AIS3 課程，這些在社群裡受景仰的講者往往有很多 CTF 競賽經歷，這對有計劃參加國際 CTF 比賽的學生大有裨益。在這裡，我們想對那些支持我們的組織、企業和社群說聲感謝。

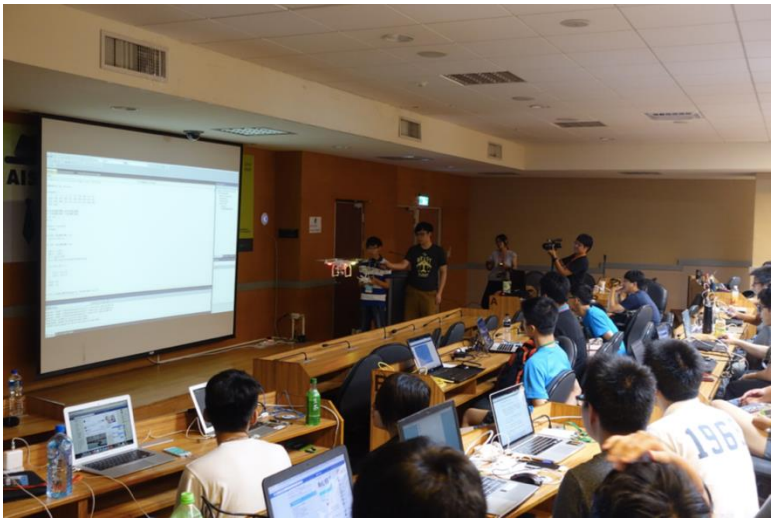
AIS3 的課程安排盡可能著重於資安實務技能的所有方面。過去我們的課程包含了以下的主題。

- APT analysis
- Automatic exploit generation

- Binary exploiting and Pwning
- CTF introduction
- Forensics
- Malware analysis
- Mobile application security
- Radio hacking
- Reverse engineering (on various platforms)
- SOC operation
- Web application security
- IoT security

儘管許多來參加的學生希望能提高他們的 CTF 實力，但這並不是 AIS3 課程的唯一目標。我們同時希望學生能學習一些常用來解決現實生活問題的技術。如圖二所示，上課的學員正在學習如何使用物聯網開發工具來設計不同的物聯網應用，特別的是，他們學會了如何將 LinkIt ONE 用作 HDK（由聯發科技贊助）來實作出一個簡單的遠端控制裝置。在對本身資源受限的物聯網設備有基本了解後，學員可以更輕鬆地開發出攻擊或防禦軟體。此外，我們還邀請趨勢科技的講者給予大家一場關於「無人機劫持」的演講，該演講類似於他之前在 DEFCON 24 上發表的成果，圖三為講者在課堂上向學員展示的照片，利用一個軟體定義的無線電來實際攻破 GPS 訊號器。除此之外，來自產業界的講者也可以讓學員了解資安公司和部門實際面臨到的問題，同時，企業也可以從這些學員中招募有潛力的員工，我們相信這將為學生和企業創造雙贏局面。

圖二：使用物聯網開發工具的過程。電子設備包含麵包板、電阻器、LED、晶體管、可變電阻器、光敏電阻器、溫度和濕度感測器、蜂鳴器、馬達和 HDK LinkIt ONE



圖三：使用軟體定義無線電來入侵 GPS

3.4 協助教學

為了確保課程順利進行，我們招募了一些助教來協助課程當下的教學，其中一項助教的重要工作是檢查學生是否能夠按照講者提供的說明進行操作，此外，助教還必須協助回答學員們在課堂上或課後所提出的疑問。助教的另一項重要工作是維護課程共同筆記的內容，由於 AIS3 課程的時間安排非常緊湊（我們在一週內就安排了數十個課程），多數的學員們都希望能利用這樣的共同學習筆記，以便在課後複習時能喚醒他們的記憶。在過去四年裡，我們使用 Hackpad 服務作為來建立共同的課程筆記，而使用 Hackpad 這個點子實際上是由學生和助教發起的，現在，共同筆記已經成為 AIS3 課程的傳統之一，我們相信這也是一個好方法讓學員能隨時參考這些存放在共筆中的課程資料。

3.5 評分：期末考試

雖然 AIS3 課程只有四年的歷史，但我們的傳統是對參與課程的學生進行 Pre-exam 和期末考試。相較於 Pre-exam，期末考試也是 CTF 比賽，且固定在課程的最後一天舉辦。如圖四所示，所有正課學員都必須參加期末考試，以證明他們是否有從課程中學到新的知識。

在過去舉辦過的期末考試中，我們在不對外開放的環境中設計了 15 個 CTF 題目，只有正課學員才能參加。因為這個期末考試只有一天約八小時的時間，所以我們要求每個學員必須尋找一名夥伴一起組隊合作解題。而隨著歷年學員人數的成長，我們組隊人數亦從二人一隊增加為四人一隊。我們在 Pre-exam 中已經使用了相似的規則和解題環境，但期末考的題目比 Pre-exam 要困難很多，有一個有趣的事情是我們向課程的講者發

出邀請，他們可以提供期末考試的題目。如果講者想要的話也可以在最後一天的比賽到現場，看看他們提供的問題有沒有順利地被學員解出。

圖四：AIS3 Final CTF 解題型競賽

3.6 國際合作

過去幾年我們一直試圖與國際建立合作關係，除了這種基於一次性課程的合作外，我們還嘗試與亞洲各國建立更緊密的長期關係，例如韓國的 Best of the Best（BoB），日本情報通信研究機構（NICT）和同樣來自日本的 SECCON 團隊。我們相信這些來自不同文化歸屬的學生之間的競爭，也會激勵更多同學共襄盛舉。

肆、EDUCTF 跨校課程

4.1 歷史

4.1.1 跨校課程聯合期末考試

在開始跨校課程之前，我們從 2000 年春季開始，開設了一門課叫「程式安全」。該課程對程式相關的安全議題有所貢獻，與傳統的資訊安全課程的觀點不同。

表一是五種類型的資訊安全課程細分，我們計算了各種資訊安全教科書中針對不同觀念的傳授的頁數百分比，包括資料安全，網路安全，系統安全，軟體安全和程式安全 [4, 6, 5, 3, 7, 8]。「資料」的課程涵蓋加密、公鑰和密鑰管理協議等相關內容，「網路」將重點放在常用的網際網路協議上，「系統」則是對存取控制和系統範圍的保護做說明，如

病毒防禦、防火牆和入侵檢測系統等，「軟體」是對相關軟體的使用和開發，而「程式」如字面上的意思，是針對程式相關的安全問題。

表一：資訊安全課程

課程內容	資料	網路	系統	軟體	程式
資料安全	80%	15%	4.9%	0.1%	0%
網路安全	56%	30%	1.3%	1%	0%
系統安全	10%	20%	60%	5%	5%
軟體安全	10%	10%	20%	30%	30%
程式安全	10%	10%	10%	10%	60%

由於程式安全可以透過 CTF 和 wargame 類型的比賽得到最好的練習和實踐，所以我們會長期運用這樣的活動來加強學生的能力。透過這些課程的訓練，有四名學生因此加入了 HITCON 戰隊，並贏得了 DEFCON 23 CTF 的第二名。這些學生為由台灣大學和交通大學聯合開設的資安課程籌劃了期末考試，用比賽的動畫加上攻防 CTF 來測驗修課同學的程度，如圖五所示。

圖五：跨校課程期末考試的戰場－攻防 CTF (2015)

4.1.2 課程協作

受到聯合課程期末考試成功的啟發，我們試圖探索在多所大學間共同教授資訊安全實務課程的可能性。

作為一個實驗性的嘗試，在 2015 年秋季，我們共同設計了一個跨校的學期課程，在國立台灣大學和國立台灣科技大學開課，教導資訊安全實務技術。分別有 53 名和 21 名學生登記上課。2016 年秋季時，該課程提供給三所大學的同學修習：國立台灣大學、

國立台灣科技大學和國立交通大學。分別有 49 名、11 名和 24 名學生登記上課。

本課程主要是開設給研究生，側重於攻防實務技術，包括網路入侵、二進位利用、密碼學、逆向工程、數位鑑識和訊息隱藏。為了能完全理解課程教授的內容和在攻防 CTF 獲得好成績，學生不僅需要在課堂時練習，也必須繳交作業和參與期末考試。

由於這樣的跨校資安學期型課程並沒有先例可以遵循，因此我們需要在開設這門新課程時做出許多決定。以下是在設計時主要考量的重點：

1. 學生篩選（§4.2）：由於台灣大多數開設的資安課程都比較偏理論概念而非現實問題的實作，如果學生修課前期望的是傳統的教學方式和內容，那他們可能會不知所措，所以我們該怎麼做才能吸引到合適的學生，並且能讓學生先探索課程相關的重點再決定是否要修課？

2. 虛擬化教室（§4.3.1）：由於修課學生來自不同的學校、都位於不同的教室，我們需要建立一個空間，可以無時差的授課，而學生也可以遠端提問。所以什麼才是最適合我們需求，並且花費較少、機動性佳的解決方案？

3. 教學團隊（§4.4）：如開頭所述，促成我們開設此課程的一個主要原因是加入了擁有不同技能強項的資訊安全專家，因此我們擁有一支由多個組織成員所組成的大型教學團隊，更不用說每所大學都有自己的行政作業需要履行配合如期末成績繳交的截止日期可能不同等。我們如何才能在如此龐大的團隊中有效合作？此外，我們應該如何盡可能地分享我們的資源，同時能夠保持足夠的自主權？

4. 評估學習成果（§4.5）：先前的努力顯示出，CTF 形式的題目是激勵學生學習和運用資安實務技能的有效途徑。但是除了能否成功解題外，我們還希望根據學生解題的不同思路來衡量學生的學習成果，事實證明這是非常不平凡的方法。

在本節的其餘部分，我們將描述我們當時的設計決策以及回顧過去的反思。

4.2 學生篩選

作為一個包含實驗部分的新課程，我們希望確保吸引到的是合適的學生，所以我們讓同學在決定是否修課之前先探索並了解課程風格和期望。尤其是，儘管近年來，在台灣學生間的 CTF 比賽越來越受歡迎，但他們之中的許多人卻只知道 CTF 的名字，而不清楚其內容。

我們構思的解決方法是規定一個作業 0x00——是一些入門級 CTF 的題組，並提供他們明確的提示，讓學生能了解他們即將面臨的題目的風格。例如，在作業 0x00 中，我們要求學生使用 SQL Injection 發現隱藏在資料庫中的標記，對應到網頁安全的基礎；解密一些經過經典加密法的 flag，對應到基本的密碼學；從被限制的檔案中，利用緩衝區溢出的漏洞取回 flag，對應到基礎的二進位利用。作業 0x00 會在學期的第一週之前發

佈，我們鼓勵學生先完成作業 0x00，再決定是否要修習本課程。

我們需要做出的另一個決定是，是否允許審核以及是否應該有任何審核篩選的程序。具體來說，由於我們的課程網站上提供了所有學習資源，因此誰應該有權訪問課程網站是我們必須重視的一大問題。從一方面來說，本著教學和分享的精神，如果我們完全無限制的允許訪問將是一件好事；但從另一方面來說，由於網路安全規則在本質上是敏感的，因此授權給未知用戶的訪問權限可能是不合適的。

我們最後的決定是實施較寬鬆的存取控制規則，課程網站可以透過有參與跨校課程的大學的 IP 位址來存取。學期結束時，我們統計出在 2015 年和 2016 年分別有 337 個和 438 個不同的使用者 ID 註冊了課程網站。

4.3 課程安排

4.3.1 虛擬化教室

由於實作和課堂練習是學習體驗中不可或缺的一部分，因此我們的課程地點在大學的電腦教室內，學生們可以使用桌上型電腦或攜帶自己的筆記型電腦。但是我們使用的電腦教室並沒有專門的虛擬化教室設備，也沒有時間和金錢購置，因此我們選擇利用現成的開源軟體組合成以下具有經濟效益和模組化的解決方案。

因為不是所有修課同學都在同一個空間裡，所以為了支援講師和學生之間的即時互動，我們採用了實況軟體來廣播講師的電腦螢幕和聲音，並建立一個線上聊天室讓同學能遠端提問。

在這個環境中，我們使用了 Open Broadcaster Software（OBS）這一個開源工具在 YouTube 上實況課程，然後在其他教室的助教可以播放轉播給該校的學生看。OBS 還可以在使用的電腦端上產生影片的副本，這個備份檔讓我們可以在網路中斷時恢復影片。課程結束後，再根據講師的許可，在課程網站上提供 YouTube 影片或影片的備份檔，修課的同學未來也可以查看影片，從而增強學習體驗。

至於線上的問答平台，我們使用了一個簡單的網路聊天室 tlk.io，學生只需要透過發送訊息就可以向講師問問題，同學也可以選擇匿名使用聊天室，這讓那些在網路上比在現實生活中更活躍的同學更願意參與討論。但是由於 tlk.io 並沒有推播通知功能，所以講師有時候會忽略學生的問題。目前我們依賴現場的助教監督聊天室，並在有人發問時提醒講師。

我們在使用影片實況提供這樣跨校課程時面臨的主要挑戰是，如何讓那些沒有跟講師同在一間教室的學生們進行互動。因為線上聊天室提出的問題可能會被忽視；而且在發生網路延遲時，在情況恢復正常之前無法即時獲得口頭上或聊天室給予的回饋，因此導師很難調整授課速度；更何況講師無法從在遠端教室的學生那裡得到非語言的回饋如困惑的面孔等。

4.3.2 主題

EDUCTF 課程為期 18 週，提供三學分（每週三小時的課程）。在 2016 年秋季的課程主題和時間分配如表二所示。我們會保留一週用於安排期末考試。

表二：課程主題範例（每週三小時）

領域	週數	主題範例
總覽和基礎工具介紹	2	objdump, pwntools
網路入侵	4	XSS, SQL injection
二進位利用	3	buffer overflow, format string, use after free
密碼學	2	encryption modes (ECB, CBC), MAC, RSA
逆向工程	2	static analysis
自動化分析	4	symbolic execution, fuzzing

4.3.3 課程網站

由於我們的組成是多所大學的學生和助教，因此課程網站是分享資訊和公告的重要媒介。網站有三個主要組成：(1) 演講投影片和影片的連結，(2) CTF 題目和送出 flag，(3) 排名。

如前所述，擁有合法 IP 的任何人，即共同開設課程的大學的 IP 地址，都可以在課程網站上註冊帳號。學生可以自由選擇他們的帳號名稱，並可選擇是否要在個人資訊中提供真實姓名和學校標記。因此排行榜並不是完全匿名的，即使他只有顯示使用者帳號。這使得我們能夠在學生保持隱私的同時，也能追蹤到他們相對於其他修課同學的學習成果。

4.4 教學團隊

如果沒有許多頂尖的 CTF 選手和多個組織的資安專業人員的密切合作，這堂課程是不可能完成的。在 2015 年，除了兩位教授外，我們還邀請了五位研究生，他們都曾參加過頂尖的 CTF 戰隊，和三位來自知名資安企業的客座講師，如趨勢科技等。在 2016 年，除了台大、台科、和交大的三位教授之外，我們再次邀請八位台灣頂尖的 CTF 選手擔任講師和助教團隊。隨著課程的開設，許多修課學生後來也組成 CTF 隊伍在世界上征戰。而在 2017 和 2018 年的課程裡，我們也讓這些成為選手的學員，回到課程裡分享他們的經驗。

除了課程安排外，我們面臨的另一個挑戰是，如何管理由來自多所大學的數十名教授和助教組成的教學團隊。在我們的案例中，我們使用一個團隊雲端平台 Slack 來討論

和同步即將到來的課程任務，從而實現這個中型團隊的即時溝通和密切合作。Slack 免費版的缺點是會刪除老舊的訊息，購買教育版會是其中一種解決方案。

另一個挑戰是如何在資源分享和獨立的靈活性之間達成良好平衡，因為學生仍然需要在各自的學校中滿足一些行政上的要求。我們目前的解決方案是盡可能最大化的分享教學資源，如課程網站、投影片、回家作業和期末考試的問題，同時每所學校都各自保持自己的評分自由，如評分的組合和百分比、作業截止日和繳交作業的方法等。

4.5 評估學習成果

由於 CTF 是本課程教學和學習的主要渠道，因此課程的成功在很大程度上取決於 CTF 比賽的質量。我們很幸運地擁有一支強大的教學團隊，其中許多人曾贏得或是籌辦了像 HITCON 這樣的頂尖 CTF 競賽，因此能夠始終如一地創造出高質量的原創 CTF 題目。

2015 年的時候，我們在作業發佈了 17 個 CTF 題目。但是有部分的問題讓僅僅剛進入 CTF 領域幾個月的初學者難以解答。此外，CTF 解題的本質使得學生很難確定他們是否在獲得 flag 的正確道路上，因此如果他們在某些時候作出了錯誤的選擇，很容易就會陷入複雜的問題內而無法跳脫思維。因此在 2016 年，我們試圖將一些難題拆解成逐步型的子問題，最後在作業上就有高達 49 個題目。

傳統的課堂考試可以在一到三小時內完成，不同的是，我們的期末考試是可以「帶回家寫的」，它是一場持續數天的 CTF 比賽。因此比較重要的是，我們必須在學期開始前就決定好期末 CTF 比賽的日期，以便修課的學生可以提前安排時間，不與其他修習的課程相碰撞。

雖然說根據 CTF 的排名或是分數來給予學期成績是比較方便的做法，但它有幾個缺點：(1) 如果有人分享 flag 給其他人的話就無法被發現；(2) 教學團隊會幾乎無法獲得回饋來改進或調整未來的課程。因此，為了公平準確地評估學習成果，每個學生都需要繳交 write-up，來說明他為了解出 CTF 題目所採取的方法或思維。除了 CTF 的分數外，同學的學期成績也取決於這些繳交的 write-up，通過閱讀他們上傳的文字，我們較容易了解同學主要遇到的學習障礙，並相對應地調整課程內容。

值得注意的是，對於所有的 CTF 題目，我們鼓勵學生互相討論，透過網路搜尋知識並向助教發問，因為自學的能力是在不斷變化的資訊安全領域中取得優異成績的關鍵。但是他們必須靠自己獨立完成 write-up 並正確地標記所有用到的參考文獻。

4.6 同學的回饋

在由大學教務處所提供的官方教學評估中，修課的學生給予了高達 4.5 分的評價（滿分為 5 分），明顯高於一般課程的平均水準。有許多學生給予了正向積極的評論，其中

有一位同學評論說：「我在 CTF 競賽經驗中取得的最大成就，就是針對不同題目提出正確且有效的解法，然後拿到 flag。這是在其他課程中很難擁有的興奮感。」許多同學也提供了一些有建設性的回饋，如希望能有更多介紹基本工具和概念的課程，或是能有更多的課堂實作等。

伍、結論

在論文中我們說明了兩個資安實務課程——AIS3 和 EDUCTF 的經驗，並在過去四年成功在台灣舉行。我們最初的實驗結果非常成功，兩門課程都得到了很高的評價和學生的積極回饋，這有助於我們在未來可以完善和重新調整即將到來的 AIS3 和 EDUCTF。

未來我們亦希望能探索一些有趣的方向。我們預計對一些數據進行分析，例如 flag 的上傳時間、得分和隨時間的排名等。我們相信這樣的分析可以發現一些隱藏的問題，並為未來的課程進步提供有價值的資訊。因為確保系統的安全永遠不是靠一己之力就能完成的工作，所以學習如何團隊合作也是一個有趣的發展。我們希望我們的經驗可以促進學術研究人員和資安從業人員之間在進階資安教育上能有更多合作。

[誌謝]

本論文所介紹的課程相關活動，受教育部資安菁英人才培育計畫補助和支持。我們在此亦感謝所有支持和曾經參與本課程計畫的企業、組織和業師。

參考文獻

[1] APWG, “Phishing Attack Trends Report – 4th Quarter 2016,” https://docs.apwg.org/reports/apwg_trends_report_q4_2016.pdf, 2016.

[2] B. Boland, “Undeclared Cyber Wars: Cyber threat actors targeting Asia,” *2016 RSA Conference*,https://www.rsaconference.com/writable/presentations/file_upload/tta1-r01_undeclared-cyberwars-cyber-threat-actors-targeting-asia.pdf (2016/07/20).

[3] B. Chess and J. West, *Secure programming with static analysis*, Pearson Education, 2007.

[4] M. Howard and D. Leblanc, *Writing secure code*, Pearson Education, 2003.

[5] B. Schneier, “Applied cryptography,” *Cover and title pages* (1997), pp. 125–147.

[6] R. C. Seacord, *The CERT C secure coding standard*, Pearson Education, 2008.

[7] W. Stallings, *Cryptography and network security: principles and practices*, Pearson

Education India, 2006.

[8] J. Viega and G. R. Mcgraw, *Building Secure Software: How to Avoid Security Problems the Right Way, Portable Documents*, Pearson Education, 2001.