出國報告（出國類別：會議）

參加 2018 年 IEEE 應用、資訊和網路安全年度會議（AINS 2018）

服務機關：內政部警政署、新北市政府警察局、嘉義縣警察局、中央警察大學
姓名職稱：警務正黃家揚、巡官蕭守晴、巡官吳玟瑩、學生趙苡婷、學生王婷琪

派赴國家：馬來西亞

出國期間：中華民國 107 年 11 月 18 日至 11 月 23 日

報告日期：中華民國 108 年 2 月 13 日

摘要

IEEE應用、資訊和網路安全會議（IEEE Conference on Applications, Information & Network Security, AINS 2018）於2018年11月21日至22日在馬來西亞蘭卡威舉行。此會議由 IEEE 馬來西亞分會主辦，會議內容以資通訊安全為主軸，討論包括物聯網、雲端運算、智慧型手機、無線網路、資料庫等資安防護議題。本次內政部警政署及中央警察大學以「基於靜態特徵構造偵測惡意程式之學習模型（Malware-Detection Model Using Learning-Based Discovery of Static Features）」、「利用決策樹方法識別 LINE VOIP 網路封包的IP位址（Strategy for Detecting IP Address of LINE VOIP Network Packets by Using the Decision-Tree Approach）」與「數位證據分析應用於網路犯罪調查（Digital Evidence Analytics Applied in Cybercrime Investigations）」等研究成果接受本次會議邀請發表3篇論文。本次於馬來西亞期間亦參訪馬來西亞皇家警察總部商業刑事偵查局，瞭解馬來西亞警方科技犯罪防制情形。藉由參與本次會議，除進行資安技術及學術研究上之交流，並與國際分享我國學術研究及實務經驗，瞭解國際間最新資安政策及威脅，掌握全球資訊安全發展脈動與趨勢，提升國家整體資安防禦能力。

目錄

壹、前言

一、會議簡介

IEEE 應用、資訊和網路安全會議（IEEE Conference On Applications, Information & Network Security, AINS 2018）於2018年11月21日至22日在馬來西亞蘭卡威 Holiday Villa 舉行，由IEEE馬來西亞分會（IEEE Malaysia Computer Chapter）主辦，會議主題為「應用、資訊和網路安全」，會議內容以資通訊安全為主軸，包括物聯網、雲端、智慧型手機、無線網路、資料庫等各項資安議題。與會人士能夠在本次會議中促進資通訊領域知識與技術的交流，對於各項資通訊應用和網路的安全有更多的對策和解決之道，提供國際研究人員參考之方向與指引。

圖一、AINS 2018 海報與研討會現場報到情形

此次AINS 2018會議邀請我國國立交通大學資訊工程學系林盈達教授與捷克共和國Hradec Králové大學Ondřej Krejcar博士發表專題演講，演講題目分別為「5G 行動邊緣運算：虛擬化、開源和安全議題（5G Mobile Edge Computing: Virtualization, Open Source, and Security Issues）」和「智慧化建立遍存計算之應用 （SMART Concepts in the context of Ubiquitous Computing）」，透過國際會議可讓世界各地學者、業者、組織機構聚集在一起，互相交流最新資通訊技術與研究成果，加速各領域國際間的創新、變革與融合，在社會科技發展議題上扮演重要角色。

圖二、交通大學林盈達教授發表專題演講

二、出席目的

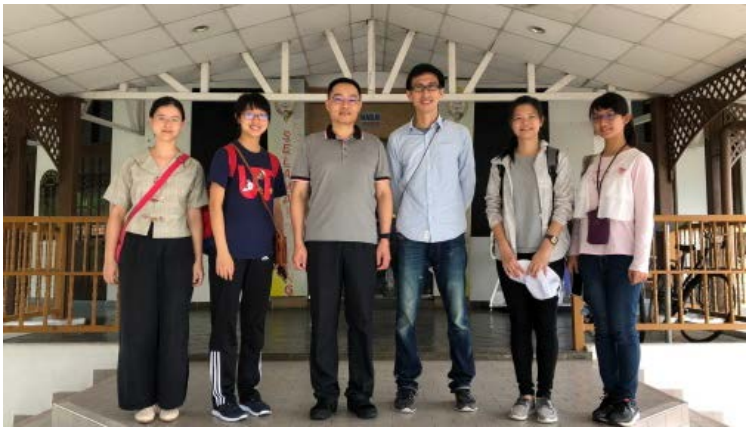
本次獲邀前往馬來西亞蘭卡威AINS 2018會議發表3篇資安相關論文，另為瞭解馬來西亞對於科技犯罪防制及資安作為，於吉隆坡參訪馬來西亞皇家警察總部商業刑事偵查局，由內政部警政署資訊室警務正黃家揚、新北市政府警察局海山分局巡官蕭守晴、嘉義縣警察局資訊科巡官吳玟瑩、中央警察大學學生趙苡婷及王婷琪等五人代表參加。藉由參與國際會議瞭解外國學者與專家的工作及研究成果，並探討在未來資通訊科技多樣化發展下，所衍生的各項資安議題。我國警政資訊實務除建置各項警用資訊系統，同時進行完善資安防護，亦須針對各種網路犯罪的趨勢和類型，分析偵查方法與應處之道；而藉由國際化之交流除可提升知識與技術之能力，增加面對問題時之專業與解決思路，觀摩專家學者所提出資通訊科技的未來議題，能幫助我國警政實務運作上進行更長遠、有效之規劃；透過參與此會議所建立之國際交流管道，使得我國與國際間的學術及實務交流能永續經營，國際交流的養分擴展至國內警察同仁間之互助，提升警察全體對資訊之相關知識與技能。

貳、活動過程

一、參觀馬來西亞警察博物館

2018年11月18日抵達馬來西亞吉隆坡國際機場後，先與我國駐馬來西亞的警察聯絡官張基銘學長會合，為理解馬來西亞當地警察運作模式與風格文化，前往位於馬來西亞吉隆坡市中心的警察博物館參觀，以瞭解馬國警察發展的歷史背景與過程。馬來西亞曾為英國的殖民地之一，其警察編制及服制文化受到英式文化影響，警察博物館內部介紹馬來西亞警察自早期及英國殖民以來的服裝、武器、標誌、歷代首長和官階體制等。博物館內的標誌展示區擺放來自世界各國警政單位與馬來西亞交流的紀念徽章與旗幟，其中亦包含我國警政署刑事警察局的紀念牌。博物館內的服裝展示區則展示馬來西亞警察歷代以來的服裝樣式，且不同行政區域的警察服裝樣式不盡相同。

馬國警察發展歷經獨立、反共、抗日等重大歷史事件，組織層級分為聯邦警察總部、州（市）警察總局、地方警區及警局等四個層級，各州設州警察總局（相當我國地方縣市警察局），各州分設數個地方警區（相當我國警察分局），每個地方警區，分設數個警局（相當我國分駐、派出所）；馬國警察階級從低至高分別為警員、伍長、警曹、警曹長、副警長、見習警長、警長、首席警長、助理警監、副警監、警監、助理總監、高級助理總監、副總監、總監、副警察總長、警察總長等。



圖三、於馬來西亞警察博物館前合影、馬來西亞警徽

二、參訪馬來西亞皇家警察總部商業刑事偵查局

（一）商業刑事偵查局介紹

為瞭解馬來西亞警方科技犯罪防制情形，2018 年 11 月 19 日由駐馬警察聯絡官安排前往位於吉隆坡的馬來西亞皇家警察總部(Royal Malaysia Police)商業刑事偵查局（Commercial Crime Investigation Department, CCID）參訪，商業刑事偵查局於 2004 年成立，為馬來西亞專責處理商業及科技犯罪的機關，由約 2,000 名的警職及文職人員所組成，並依據各類犯罪案件設置不同調查部門，包含：金融犯罪調查部門(Financial Investigation Division)、商業犯罪調查部門(Corporate and society Investigation Division)、土地詐欺及偽造調查部門(Land fraud & Forgery Investigation Division)、數位及多媒體犯罪調查部門(Cyber & Multimedia Investigation Division)等，商業刑事偵查局主要處理的犯罪類型包括信用卡詐騙案件、銀行詐欺案件、保險詐欺案件及其他類型詐騙案件等。

圖四、與商業刑事偵查局負責接待的副警監 DSP 鄭家倫合影

（二）參訪過程

本次參訪有賴駐馬警察聯絡官聯繫協調，馬方給予高規格的接待，除由商業刑事偵查局網路暨多媒體犯罪偵查處助理局長SAC Ahmad

Noordin Bin Ismail親自接待，另有該局十多位成員與會，會中首先由馬方副警監DSP Yeap Yoke Peng報告近年偵辦各詐欺案件成效，近年詐騙集團有轉移至東南亞等鄰近國家的趨勢，並使用VoIP等網路電話技術成立跨國電信詐騙機房，因應相關犯罪情勢，我國與馬來西亞、泰國等東南亞國家建立即時連繫管道及情資交換機制，以科技分析、國際合作等持續打擊跨境電信詐欺集團，近年接連破獲於馬來西亞雪蘭莪州電信詐欺機房，及台嫌出資管理、在吉隆坡詐騙泰國民眾的跨國電信詐騙機房等，成效良好。

圖五、本次參訪人員與商業刑事偵查局與會成員合影

我方由警政署警務正黃家揚報告近年我國運用大數據及警政科技之應用與成果，內容包含我國警政巨量資料、資料分析協作平臺、M-Police警用行動電腦等，馬方對於我國可將眾多治安相關資料整合為警政巨量資料庫表示高度興趣，並表示這些治安資料確為各國治安單位對於維護治安所不可或缺的重要資料，如能將偵辦詐欺案件時所需之話務及金流資料納入將更臻完備；另對於我國運用資通訊技術開發出M-Police警用行動電腦，提供第一線執勤員警多項即時的治安資訊表示佩服，並針對M-Police警用行動電腦配發數量、細部功能等進行提問，雙方對於如何利用資訊科技有效輔助警察各項勤務、偵辦案件之進行、如何跨機關進行資

料庫整合，與機關資訊安全對策等議題進行深度的討論。

圖六、警務正黃家揚報告我國警政科技運用成果

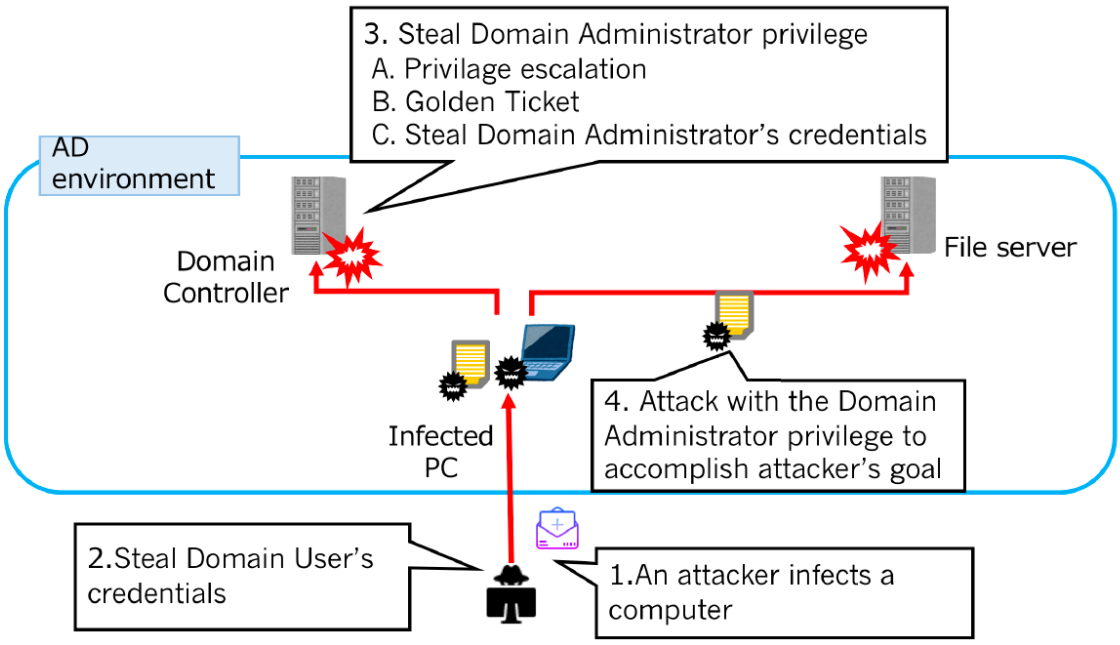
三、參加 AINS 2018 會議

（一）11 月 21 日議程

2018年11月20日搭乘馬來西亞國內線班機來到本次AINS 2018會議舉辦地點-蘭卡威Holiday Villa，會議第一天(11月21日)發表的論文主題圍繞在 FCT：動態檢查輔助的數位鑑識電子學習系統（FCT: Digital Forensics E-Learning System with Dynamic Examination Support）、用於智慧型手機防 Shoulder Surfing 屏幕鎖定：五十種非生物識別方法的探討 （Shoulder Surf Resistant Screen Locking for Smartphones: A Review of Fifty Non-Biometric Methods）、透過分析Windows 事件紀錄檢測攻擊者濫用網域管理者權限（Detecting Abuse of Domain Administrator Privilege Using Windows Event Log）、行動健康應用程式中的安全漏洞 （Security Vulnerabilities in Mobile Health Applications）等資訊安全相關的議題。

來自日本的 Mariko Fujimoto、Takuho Mitsunaga 及 Wataru Matsuda 等人共同發表的「透過分析 Windows 事件紀錄檢測攻擊者濫用網域管理者

權限（Detecting Abuse of Domain Administrator Privilege Using Windows Event Log）」一文，內容摘述如下：在進階持續性威脅（APT）攻擊中，滲透到組織網路中的攻擊者通常會長期潛伏直到他們達成最終目標，如竊取內部敏感資訊及商業機密等。在攻擊者滲透進入內部網路後，攻擊者會嘗試取得網域系統管理者的帳號權限（Domain Administrator Privilege），該帳號有權存取 AD（Active Directory）環境中的所有使用者和檔案。



圖七、攻擊者滲透及取得 AD 網域系統管理者帳號權限流程

攻擊者有多種方法取得合法網域系統管理者帳號，一種是利用 AD 系統上的漏洞，例如 CVE-2014-0317 即為一例，另一種是使用有名的密碼竊取工具，例如 mimikatz。成功取得管理者帳號權限後，攻擊者可能會建立一個後門帳號，偽裝成合法的網域系統管理者，以獲得長期的管理權限。如果攻擊者使用合法的網域系統管理者帳號，則很難區分出合法使用者和惡意攻擊者，為解決這個問題，現有數種透過分析 Windows 事件紀錄來檢測對 AD 系統攻擊的方法，每種檢測方法在特定條件下都很有用，但均不能涵蓋所有攻擊手法。在該研究中，除使用測試記錄檔實測評估現有方法檢測攻擊行為的有效性，並提出一種新的方法可以進一步提高檢測率。

（二）論文發表：基於靜態特徵構造偵測惡意程式之學習模型

本次與會發表的第1篇論文為新北市政府警察局海山分局巡官蕭守晴與中央警察大學資訊管理學系副教授高大宇共同著作的「基於靜態特徵構造偵測惡意程式之學習模型（Malware-Detection Model Using Learning-Based Discovery of Static Features）」，並由巡官蕭守晴於會議現場發表，獲得在場與會人士及專家學者的良好迴響，在場專家學者亦與蕭巡官多次互動提問討論，現今機器學習的議題實為大家重視的議題。

圖八、巡官蕭守晴發表論文

此篇論文說明目前資安議題中關注的惡意程式部分，內容摘述如下：惡意程式的快速增加與變種對政府機關、企業或個人都構成嚴重威脅，以往靜態特徵碼（static signatures）的防禦方式無法即時偵測到最新變種的惡意程式，甚至是零時差攻擊的惡意程式（zero-day malware）；因此，應用機器學習於惡意程式偵測變得日趨重要。以往的研究主要集中在學習模型的模式與實現方法，本研究的目標有二：優化惡意程式機器學習模型，以及將優化後的模型實作在真實網路環境中。本研究採用優化方法進行機器學習工作流程，包括減少雜訊(Noise Reduction)、初始分類（Initial Triage）、特徵工程（Feature Engineering）和集成學習（Ensemble Learning）。機器學習工作流程分為學習階段（Learning Stage）與偵測階段（Detection Stage），在學習階段先將 PE 可執行檔分為兩類：加殼與未加殼，再分別利用特徵工程與集成學習客製化訓練出加殼和未加殼兩種不同惡意程式偵測模型；在偵測階段，當遇到一個可疑的PE執行檔，使用

Noise Reduction 先過濾檔案是否已特徵碼建檔，若未出現在特徵碼資料庫中，再進一步分類並對應到分類結果的機器學習模型進行偵測。在此篇實驗部分，除對所提出的優化方法的效能進行驗證之外，亦通過比較分析來選擇效能最佳的方法應用於實際偵測。本研究使用三個評估指標測量效能：ROC Curve、Classification Accuracy 和 Classification Report。當 Variance Threshold 與 Random Forest Algorithm 搭配使用時，可產生未加殼惡意程式偵測的最佳效能，而當Feature Importance與Random Forest Algorithm一起使用時，可產生加殼惡意程式偵測的最佳效能。

（三）11 月 22 日議程

會議第二天(11月22日)發表的論文主題包括模擬資料庫取證調查的模型推導系統、論述異常偵測技術與評估方法、安全模式研究的分類與文獻探討等，來自馬來西亞的 Fiza Abdul Rahim、Gopinath Muruti 及 Zul-Azri Ibrahim共同著作「論述異常偵測技術與評估方法（A Survey on Anomalies Detection Techniques and Measurement Methods）」一文摘述如下：異常偵測已經在許多研究領域皆有顯著的研究成果，並且已經提出各種技術來識別不同資料集中異常的項目或事件，如資安事件偵測、詐欺行為偵測、醫療異常狀況偵測等應用。該研究利用清楚結構化的方式整理各種異常偵測技術，並進一步討論應用統計方式和機器學習於偵測異常之模型。透過比較所列異常偵測技術的優缺點，有助於全面瞭解各領域間所使用技術於異常偵測之技術。

圖九、與議程主席 Dr.Izzatdin Abdul Aziz 合影

（四）論文發表：利用決策樹方法識別 LINE VOIP 網路封包的 IP 位址

本次與會發表的第2篇論文為嘉義縣警察局資訊科巡官吳玟瑩、中央警察大學副教授高大宇與學生王婷琪共同著作的「利用決策樹方法識別 LINE VOIP 網路封包的IP位址（Strategy for Detecting IP Address of LINE VOIP Network Packets by Using the Decision-Tree Approach）」，並由巡官吳玟瑩及學生王婷琪於會議現場發表，內容摘述如下：隨著網路即時通訊軟體（例如：LINE、Skype、WeChat…等）的普及，以及使用者身分容易隱匿的特性，有越來越多詐騙案件以這類即時通訊軟體作為犯罪平臺，在通訊軟體開發商為非本國產業的情形下，欠缺軟體業者的即時配合，造成嫌疑人身分及位置難以追查，執法機關無法快速且有效識別匿名嫌疑人，為當前犯罪偵查上重要的挑戰。本研究選擇我國廣泛使用的 LINE 通訊軟體作為實驗標的，研究一種即時而有效的機制分析 LINE 網路電話功能中呼叫者的IP位址，而無需網際網路服務提供業者（ISP）或其他軟體供應商的協助。本研究提出一個資料分析架構，包含資料蒐集、模型學習及預測模型三大階段，透過在使用者端側錄進行LINE網路通話時的VoIP 網路封包，利用演算法進行學習，以決策樹方式展現在側錄封包中識別的使用者 IP 位址。

圖十、巡官吳玟瑩、學生王婷琪發表論文

（五）論文發表：數位證據分析應用於網絡犯罪調查

本次與會發表的第3篇論文為中央警察大學副教授高大宇、助理教授蔡馥瑔、學生趙苡婷及警政署資訊室警務正黃家揚共同著作的「數位證據分析應用於網絡犯罪調查（Digital Evidence Analytics Applied in

Cybercrime Investigations）」，內容摘述如下：隨著電腦犯罪案件的增加，數位鑑識已經成為執法單位不可或缺的重要領域。數位鑑識包含識別(Identification)、收集(Collection)、驗證(Examination)、分析(Analysis)及展示(Presentation)等步驟，本研究提出整合數位鑑識流程與步驟四階段，包含整備階段(Readiness Phase)、初始階段(Initialization Phase)、獲取階段(Acquisitive Phase)及調查階段(Investigative Phase)等，並在相對應階段中列出可使用的工具清單，以提升執法單位進行數位鑑識的效率及有效性。

圖十一、學生趙苡婷發表論文

參、與會心得及建議

一、與會心得：國際交流激發資訊科技新思維並活用於警察實務當中

國際會議是個各種不同視野及想法激盪的地方，本次參與AINS 2018會議接觸到世界各地的資訊安全研究人員，並與他們交流各項資安見解。會議各場議程均蘊含豐富的資安相關議題，從資料庫、資訊系統、及新興科技如物聯網等均可能具有資安風險，與會講者專業解說發表的文章內容，參與人員亦提出不同見解，激盪出更深層的討論，使該議題的輪廓更為完整。在會議聽到與會人員表達不同角度的意見時，可用不同觀點重新審視與思考，對於如何以資安的角度協助修補資訊系統或是進行維運，以及日益增加的科技執法與偵查，很多專家學者都提供不同的研究模型與成果，這些經驗有助於我國警政資安能量的提升。我國警政資訊單位除依據執勤員警需求開發警用資訊系統、透過科技輔助偵查與進行數位鑑識外，亦須注意整體警政資訊系統資訊安全防護設備與措施

，而透過國際交流的管道，可從中獲得許多新思維並應用於警察資訊實務之中。

隨著科技愈來愈進步、資訊設備朝向多元化發展，警察機關使用新科技之便利性強化各項勤務措施與偵查作為，但相對地，駭客攻擊手法與態樣亦不斷革新。再者，警政機關握有大量機敏資料與政策文書，可預見吸引許多滲透式攻擊，如APT攻擊等等。此次會議中有講者提到因應日前諸多 Webcam 遭入侵侵犯隱私，可建置如Honeypot之誘捕系統蒐集大量的攻擊樣本並作分析，除可以洞察駭客攻擊的手法、針對樣本進行分析，以利事先做好防禦措施，透過誘捕系統所蒐集之樣本亦可作為惡意程式機器學習模型之訓練集，面對不斷變種之惡意程式與攻擊武器，發展機器學習之惡意偵測方式為未來資安防護之趨勢。

二、建議事項

（一）持續參與國際交流，提升資安人員專業能力

國際資通安全威脅趨勢攀升，網路攻擊事件頻傳，本次參與AINS 2018會議與國際專家學者交流各項資安與科技訊息，如部分研究人員均提出有關機器學習於各種資安領域的應用，除可作為資安事件調查、惡意程式偵測，亦可以針對大量日誌紀錄進行資訊系統攻擊行為模式分析，諸多實際應用案例皆應證機器學習領域龐大的發展潛力。另本次進行「5G行動邊緣化運算」專題演講的林盈達教授亦談論到未來 5G 行動網路的應用與可能發生的問題，邊緣化運算的原理是將資料在來源端先行運算後再傳送至雲端，以達到縮小資料量、大幅減少傳送資料所需時間及延遲性，為虛擬應用和物聯網技術的一大突破，未來將依各國布建5G通訊基礎建設進度逐步進行商轉，然而新技術可能含有許多尚未被發掘之漏洞，這些漏洞都有可能成為潛在惡意攻擊者的利用機會，因應複雜多變的資安威脅，資安人員除應精進資安技術，更應持續就資訊安全及科技犯罪防制經驗與國際交流，瞭解國際間最新資安政策及威脅，研析駭客攻擊方法及對應的蒐證技巧，掌握全球資訊安全發展脈動與趨勢，

提升國家整體資安防禦能力。

（二） 發展事件紀錄分析系統，建立資安情資分享與機關聯防機制

以往的系統事件紀錄分析，是在資安事件發生後再根據可能攻擊者的IP位址、推估之攻擊時間去調取該時段之事件紀錄，且多以人工方式分析攻擊手法並查找攻擊源頭。本次會議中有兩篇文章針對Windows 事件紀錄分析之議題進行研究，其中一篇提及利用機器學習方式自動化辨識針對AD（Active Directory）系統的APT（Advanced Persistent Threat）攻擊，另一篇針對偽裝成AD使用者之攻擊手法進行Windows事件紀錄之過濾，兩篇文章皆利用Windows事件紀錄作為偵測依據，並由此發展出自動化偵測機制。若能藉由擷取網路封包及進行事件紀錄之自動化分析，在攻擊初始階段即發覺並進行告警，將能即時進行防禦並阻絕攻擊者進一步的攻擊行為，並將攻擊手法或漏洞等相關資安情資分享所屬機關或友軍單位，建立機關間資安聯防機制，落實各項資安防護作為。

附件

IEEE CONFERENCE ON APPLICATIONS, INFORMATION AND NETWORK SECURITY
（AINS） CONFERENCE PROGRAM

DAY 1 Wednesday, November 21

8:00 - 9:00 Registration: *Registration*

9:00 - 10:00

AINS-Ex1: *Networking Session 1*

10:00 - 11:00

11:00 - 11:15

11:15 - 13:00

13:00 - 14:00 Lunch: *Lunch*

14:00 - 15:00 AINS-1: *AINS-Session 1*

15:00 - 16:00 AINS-K1: *AINS-Keynote 1: Professor Dr. Ying-Dar Lin*

16:00 - 16:15 Afternoon Tea: *Afternoon Tea*

16:15 - 18:00 AINS-2: *AINS-Session 2*

18:00 - 18:15

Networking: *Networking Session 2*

18:15 - 20:00

20:00 - 23:00 Dinner: *Dinner*

DAY 2 Thursday, November 22

8:00 - 9:00 Registration: *Registration*

9:00 - 10:00 AINS-3: *AINS-Session 3*

10:00 - 11:00 AINS-K2: *AINS-Keynote 2: Professor Ing. Dr. Ondřej Krejcar*

11:00 - 11:15 Morning Tea: *Morning Tea*

11:15 - 13:00 AINS-4: *AINS-Session 4*

13:00 - 14:00 Lunch: *Lunch*

14:00 - 15:00

AINS-EX2: *Networking Session 3*

15:00 - 16:00

16:00 - 16:15

16:15 - 18:00

18:00 - 18:15 Closing: *Closing*