行政院所屬各機關因公出國人員出國報告書

(出國類別：會議)

參加第 8 屆 International Conference on Cryptology and Network Security(CANS 2009)國際研討會報告

服務機關：行政院環境保護署
姓名職稱：黃素梅設計師
出國地點：日本金澤
出國期間：98 年 12 月 11 日至 12 月 15 日
報告日期：99 年 1 月 12 日

摘要

本次研討會在石川縣立美術館(Ishikawa Prefectural Museum of Art in Kanazawa)舉行，由日本「國家先進工業科學與技術研究所(AIST)」及「北陸先端科學技術大學院大學(JAIST)」主辦，其中 AIST 的研究領域涵蓋：環境與能源、資訊技術、生命科學與生物技術、奈米技術、原物料與製造技術、地質勘測與地球科學、計量與測量學等六類。

本次研討會的主題為“Cryptology And Network Security”，共有來自台灣、日本、新加坡、美國、中國大陸等 19 個國家約 106 人與會。大會以 10 個場次進行 7 個主題的研究發表(共計有 32 位發表人)，大會另外邀請了 Adam D. Smith, Adrian Perrig, Craig Gentry 等 3 位來賓針對隱私資料保護、網路認證技術、加密技術進行專題演講。

目次

附錄

壹、 背景說明及與會目的

論壇會議歷年來致力於資料加密技術及網路安全等議題研究，會議每年輪流在全球召開 1 次，除徵求各相關研究發表，也針對未來資訊安全相關技術發展邀請知名人士與會探討。

本次會議在日本石川縣立美術館(Ishikawa Prefectural Museum of Art in Kanazawa)舉行，由日本「國家先進工業科學與技術研究所(AIST)」及「北陸先端科學技術大學院大學(JAIST)」共同主辦，其中 AIST 是由日本政府資助的一所大型研究機構，其研究領域涵蓋：環境與能源、資訊技術、生命科學與生物技術、奈米技術、原物料與製造技術、地質勘測與地球科學、計量與測量學等六類。

本次研討會的主題為“Cryptology And Network Security”，共有來自台灣、日本、新加坡、美國、中國大陸等 19 個國家約 106 人與會，我國除了本署人員外，另有來自國立清華大學人員與會。

在全球化資訊社會中，各國政府機關為追求行政效能以實現便民、利民之目標，無不相繼利用電腦及網際網路提供創新服務或改善業務效率。我國亦積極推行各項電腦資訊化服務，唯在便利、快速的前提下，如何確保資訊安全，防範日新月異的網路威脅，是各公部門的一大挑戰。本次參與會議除了搜集資訊加密技術與網路安全技術發展趨勢，也希望藉由與會人士討論過程，汲取各專家學者所提供之實務應用建議。

貳、 會議過程

大會以 10 個場次進行 7 個主題的研究發表(共計有 32 位發表人)，主題分別為：Cryptographic Protocol and Schemes、Cryptanalysis、Wireless and Sensor Network Security、Privacy and Anonymity、Functional and Searchable Encryption、Authentication、Algebraic and Number-Theoretic Schemes，大會另外邀請了 Adam D. Smith, Adrian Perrig, Craig Gentry 等 3 位來賓針對隱私資料保護、網路認證技術、加密技術進行專題演講。

僅就三天議程之簡報發表摘要說明以下：

第 1 天：3 場次

- Cryptographic Protocol and Schemes
- Cryptanalysis
- Wireless and Sensor Network Security

上午於報到程序結束後，首先由 Mark Manulis 教授進行簡短的開場，隨即開始第 1 場研究發表以及美國賓州大學助理教授 Adam D. Smith 的專題演講，Adam D. Smith 即呼籲保有敏感的個人資料之政府或私人機構（例如醫療記錄，普查調查的回答，或網絡搜索記錄），於加值運用和公開發布統計數據時（例如政策和商業決定），也應同時保護個人隱私的記錄。

下午則有第 2 場及第 3 場的研究發表，當日最後一位上台發表的人員則是來自我國清華大學，議程進行到下午 6 點 20 結束，共有 12 篇發表。

第 2 天：4 場次

- Privacy and Anonymity
- Functional and Searchable Encryption
- Authentication & Block Cipher Design
- Cryptanalysis

以上 4 場共有 14 篇發表，包含 Carnegie Mellon University 的教授 Adrian Perrig 專題演講，議程進行到下午 6 點結束。其中，Adrian Perrig 即提到隨著網際網路日漸普及，越來越多的系統逐漸移到網路上，對於需要管制使用對象的系統，必須採用身分驗證機制，但是採用有效又安全的驗證方式才能確保網站系統的安全性。

第 3 天：3 場次

- Algebraic and Number-Theoretic Schemes
- Wireless and Sensor Network Security
- Cryptographic Protocol and Schemes

以上 3 場共有 9 篇發表，包含 IBM TJ 華生研究中心的研究員 Craig Gentry 專題演講，Craig Gentry 所提的即是如何在雲端運用加密技術，例如我們想利用搜索引擎搜集資料，但不想讓搜索引擎記錄我們的內容，即可運用其所提出的 fully homomorphic encryption scheme 達成。當日議程進行到下午 3 點 40 分，圓滿結束 3 天以來緊湊的研究發表。

參、 心得與建議

一、由於各類硬體晶片發展快速，在軟體配套的資通訊安全作法日漸豐富，未來在網路上施行各種申報或公務申報的安全性當可有效提昇，同時各種憑證的選擇性增加，例如生物晶片，智慧卡等，可依不同的公眾服務推動加以運用，相對的提高民眾的信賴度與使用意願。

二、無線網路及感測網路（sensor network）的安全性課題日益迫切：無線網路的技術層次快速成長，同時在商業應用層面也日趨成熟，目前結合手機的3.5G上網商業模式（600元-800元「無限上網」）正日益蓬勃，只要手機能通的地方就能上網，這種模式對傳統的Wi-Fi或是WiMAX構成相當程度的威脅。另一方面，透由手機上網的資訊安全課題，是各公私機構必須面對的新挑戰，如何避免機關員工，在上班期間利用私人筆記型電腦與3.5G手機上網，所衍生的資訊安全問題，除了技術層面的課題，在「管理」面更是值得探究和重視。本署為滿足同仁行動連網需求亦設有無線網路以及3.5G無線網卡借用服務，基於上述論及的安全課題，本署除了由技術層面的身分驗證管制機制，於本(99)年1月5日亦發布「行政院環境保護署無線網路管理規範」，期能藉由管理機制的落實，確保本署資通訊安全。其次，無線感測網路被廣泛應用於軍事國防、空間探索、環境監測、自然災害預防、危險救災、工程監控、醫療保健、智慧家居等方面，如何避免公部門機敏性資料遭竊聽、攔截、竄改等資通訊安全課題尤為迫切。

三、隱私資料保護的課題：本署較少記錄民眾之個人隱私資料，員工資料主要存放於人事及出納等專屬系統，需安裝特定程式與帳號權限才能登入。惟各業務單位保存有許多廠商的申報許可資料，且由各業務單位委外操作管理，對於隱私資料的保護除須建置軟硬體設備，最重要的仍是透過合約規範承商之保密義務。

四、身分驗證課題：隨著網際網路日漸普及，越來越多

的系統逐漸移到網路上，對於需要管制使用對象的系統，必須採用身分驗證機制，以確保網站系統的安全性。目前本署大多一個應用系統就提供一組驗證帳號密碼，特別是提供給地方環保機關及業者的系統，而大部分的使用者為了方便都習慣選取短小、有意義的密碼，所以攻擊者還是可以透過線上猜測密碼的方式來破解使用者的密碼，未來可否統一採用電子憑證方式進行身分驗證是值得思考的方向。

五、本署雖自96年即通過國際資訊安全管理系統（ISO27001）認證，對於資通訊安全的防護亦不遺餘力，惟網路攻擊樣態多樣化，所謂「道高一尺，魔高一丈」，隨著企業建置防火牆、防毒軟體、入侵偵測系統等各類防護機制，攻擊者與其威脅的複雜度只會增加而不會減少，尤其本署新建置完成機房共構專案，隨著資通訊架構的改變，資安課題必須緊隨而上，從技術面的加強與管理面的落實雙管齊下，以因應日新月異的資安威脅。