主題二：行動網路安全

近年來行動網路的普及，帶動了各種行動網路技術的蓬勃發展。本研究主題涵蓋行動網路、智慧電網與物聯網等安全議題。在行動網路安全方面，行動網路作業平台 Android 與 iOS 的推出，更加速了使用者對行動網路的需求與依賴，同時，也顯示出行動網路安全議題的重要性。在現今的行動網路平台中，為了滿足使用者的消費習慣，同一行動平台上，常結合了多種異質性無線網路技術（如：WiFi 與 3G）。異質性行動網路結合時所產生的效率問題，以及衍生的安全問題（如確保身份資訊、資料保密等等），則是研究人員應著力的重點研究方向之一。

物聯網（Internet of Things，簡稱IOT）首次出現於國際電信聯盟（International Telecommunication Union，簡稱ITU）於2005年所提出的報告中。該報告指出，在網路化的時代下，人跟人之間可以透過網路相互聯繫、人也可透過網路取得物件的資訊。然而，現今的網路發展，物件與物件之間也可以透過互通的網路環境來互相聯繫與溝通。物聯網是新興網路，早期重點放在元件製造及環境建置上，對資訊安全方面並無國際標準，當物聯網開始進入實質應用階段，資訊安全必然成為注目焦點，相關應用與研究也逐漸成為國際資通訊領域的重點研發項目。

此外，智慧電網（亦屬一種物聯網）涵蓋的層面相當廣泛，從家庭網路（Home Area Network，簡稱HAN）、電力線通訊（Power Line Communication，簡稱PLC）、鄰里區域網路（Neighborhood Area Network，簡稱NAN）與廣域網路（Wide Area Network，簡稱WAN）等等。目前世界各國基於能源利用的考量，紛紛開始改善傳統電網的缺點，並編列大量預算發展智慧電網。由於智慧電網屬於國家的重要基礎建設，一旦遭到破壞，其後果將不堪設想，因此更加需要注重其通訊與控制安全。需要具備高度安全性的智慧電網（Smart Grid）也將成為未來數年內專家學者的重點研究方向之一，尤其如何安全的結合異質網路更將成為此領域的一大挑戰。

（一） 國內外發展現況

隨著各種網路應用的發展，網路電話、P2P、SIP 等通訊協定之相關安全議題逐漸受到重視，許多加強安全性的機制也因應而生。然而，為了解決 IPv4 網址不敷使用的窘境，世界各國正在建置的 IPv6 卻可能對現有各種網路系統間利用 IPsec 所建立的 VPN 通訊造成影響，其間安全議題正迫切需要研究，並找出因應之道。

近幾年，國內行動通訊網路相關的研究多限於個別網路環境中安全的身份認證機制，如 WLAN、GSM、3G、WiMAX 等通訊協定中的身份認證與金鑰管理機制。然而，設計通訊協定時，驗證與確保新協定的安全性是相當重要的，因此有部分研究致力於開發自動化的協定安全性驗證機制，以期快速地發現新協定的弱點，有效減少設計上的缺失與設計時程。此外，無線感測網路的崛起，也帶動了感測網路節點間資訊傳輸的安全研究。因此，這個主題所規劃之行動網路將涵蓋傳統的個人行動通訊網路、無線網路，以及無線網路感測等。

在異質性網路安全分析方面，因各種不同目的而發展出來的無線通訊技術，如 WiMAX、LTE、3G等等，目前正處於整合的階段。為了節省基礎建設與開發成本，疊加網路（Overlay Network）與異質性網路漫遊技術（Roaming）是非常熱門的研究重點，如何在異質性網路架構中維持資料傳輸安全是一大挑戰。另外，傳統網路在設計之初，並沒有考慮到安全性而造成許多弱點。為了避免重蹈覆轍，目前新一代的通訊技術在制定時便將安全性納入考量，因此相較之下如何培養使用者養成良好習慣、正確地設定安全參數則顯得更為重要。

目前國內對於單一網路的安全研究已經相當成熟，但是關於異質性網路的安全研究仍處於萌芽階段，尤其在身份鑑別、路由協定、安全有效的金鑰管理等機制的設計上，依然沒有突破，因此這個子領域具有相當的研究價值與空間。

在物聯網的發展方面，下列數項技術扮演了相當重要的關鍵，包括無線感測網路、無線射頻識別技術等：

1. 無線感測網路（Wireless Sensor Networks）：無線感測網路是一種可以測得週遭環境變化狀況的無線技術。此技術透過感知器和無線網路的結合，可以提供週遭環境變化的數據，並經由無線傳輸的方式把監測資料送到後端的資料收集中心或基地台，讓遠端的人員透過這些數據判斷環境發生的狀況。無線感測技術主要包括「環境感知技術」和「位置感知技術」。「環境感知技術」監測環境中的各項資訊，例如：溫度、溼度、光度、空氣品質等等而「位置感知技術」則利用使用者所攜帶配有GPS的手持裝置，例如手機、PDA等，感知使用者所在的地理位置，提供所需服務。目前已有許多學者針對無線感測網路的安全性提出各種解決辦法。
2. 無線射頻識別技術（Radio-Frequency Identification，簡稱 RFID）：RFID 通常是由一組感應器（Reader）和多組標籤（Tag）所建構而成的系統，主要是運用無線射頻的方式，在感應器和標籤之間進行非接觸式雙向傳輸溝通，達到隔空感應目標物和資料訊息交換任務的技術。目前日常生活環境中已普遍存在 RFID 的相關應用，例如捷運悠遊卡、金融卡等等。RFID 技術發展，也大大提升了物聯網的應用，像是運用在物流、供應鏈管理上將有助於降低物流成本、提升倉儲管理效率。目前許多文獻也針對 RFID 的安全議題提出討論。

此外，智慧電網（一種特殊的物聯網）的安全目標與一般的網路安全不同，主要考量網路服務的可用性。例如電力系統如果無法供電，企業或工廠將因為停電而損失慘重，甚至影響到國家經濟與安全。由於各國的傳統電力系統皆不相同，因此目前全世界有多種不同的標準，如下：

1. 美國：NIST IOP Roadmap
2. 歐盟：Mandate CEN/CENELEC M/441
3. 德國：BMWi E-Energy Program、BDI initiative – Internet der Energie
4. 中國：SGCC Framework
5. 日本：METI Smart Grid roadmap
6. 韓國：Smart Grid Roadmap 2030
7. IEEE：P2030
8. IEC SMB：SG 3 Roadmap
9. CIGRE：D2.24
10. 微軟：SERA

在國內，台灣電力公司（台電）預計在民國 101 年優先完成佈建約 2 萬 3 千戶高壓用戶 AMI；藉由本國資通訊（Information and Communication Technologies）產業技術優勢，推動 AMI 相關產業的發展。低壓用戶部份，在能源局的規畫下，台電初期預定在民國 101 年佈建 1 萬戶，並在評估效益後，配合國家政策，逐步推展擴大，期望在 104 年完成佈建 100 萬戶。與其他各國相比，台灣的 AMI 發展起步相對較晚，由於

台灣屬於特殊島國地形，如何發展出適合台灣使用的 AMI 架構，這一部分具有研究價值與目標。

（二）關鍵研究課題

1. 子題：網路安全協定設計與分析

(1) 網路安全協定設計與分析之概述

除了基本的通訊協定TCP/IP之外，隨著消費者對網路的依賴度增加，各式各樣的通訊協定也因應而生，如Peer-to-Peer（P2P）、Session Initiation Protocol（SIP）等。然而許多早期的網路通訊協定存在著安全性上的漏洞，為了解決這些嚴重的疏失，因而發展出『虛擬私密網路』(Virtual Private Network，簡稱VPN)，藉由結合IPsec、L2TP、PPTP、SSL、SNP等網路安全通訊協定，可以建立出一條安全通道來保護傳輸的訊息。透過此機制可以提昇網路身份認證與資訊保密的安全性。

網路身份鑑別的方法大致上可以分為兩類，第一類是以通行密碼為基礎的認證機制（Password-based Authentication Protocols），如PIN、PAP、CHAP、Kerberos。由於通行密碼具備高度實用性與低開發成本，因此這類機制在網路身份認證機制中的使用極為廣泛。第二類是以高安全性的電子憑證（Certificate）為基礎的認證機制，在需要較高安全性的網路通訊系統中，此機制是現今的主流，如IETF標準IKE/ISAKMP。

(2) 網路安全協定設計與分析之關鍵研究課題

A. 適用於各網路之身份鑑別協定與機制

B. 適用於各網路之安全路由協定與機制

C. 適用於各網路之安全時間同步協定與機制

D. 適用於低計算量平台之安全的金鑰交換協定與機制

E. 無線網路之弱點分析與防治

2. 子題：異質性網路安全分析

(1) 異質性網路安全分析之主題概述

隨著使用者對行動網路的漸增的需求與依賴，為了快速提供各種應用服務、降低建置成本，各行動組織陸續地提出多種異質性網路技術（如WiFi、3G、WiMAX、LTE、Ad-hoc、ZigBee）與架構。然而，專家學者卻也陸陸續續地找到這些網路中身份認證與資料保密的安全性弱點。尤其是整合異質性行動網路通訊技術架構、認證方式、資料保密方法、金鑰管理機制等等所衍生出來的問題，更是一大挑戰。此外，由於異質性網路架構龐大，如何移除或防堵被破解或入侵的節點，來降低對於後端控管中心的傷害，也是近年來的研究重點。

IEEE 802.21 是針對異質性網路之換手機制的一個標準，期望在整合異質性網路時，能達到無縫換手（Seamless Hand-off）的目的。然而，IEEE 802.21 標準卻明確地指出此標準並不考慮安全性問題，因此，許多專家學者開始著手研究不同網路換手時可能遇到的安全性問題，以及如何有效率、更安全地實現不同階層的認證、加密與金鑰管理機制。除此之外，在異質性網路架構中，如何提供安全的路由機制，確保資料可以可靠地傳送到目的節點，也是本主題應探討的研究重點之一。

(2) 異質性網路安全分析之關鍵研究課題

A. 整合於異質性網路下之身份鑑別協定與機制

B. 整合於異質性網路下之安全路由協定與機制

C. 整合於異質性網路下之金鑰管理機制

3. 子題：物聯網安全技術

(1) 物聯網安全技術之主題概述

物連網（IOT）最主要的概念是將訊息互連互通拓展到物與物之間。物聯網的實現有三個主要技術前提，分別是物體識別、環境感知與無線通信，以利辨識系統中的物體、感測環境因子，並透過無線通信將結果回報中控中心。

此外，智慧電網（Smart Grid）是一種特殊的物聯網系統，具備智能決策機制的電力能源基礎建設，通常必須具備下列特性：自我修復、雙向溝通、抵擋攻擊、增加電力品質、能容納各種電力生產與儲存、各種電力服務與效能最佳化。智慧電網整合了各種通訊技術與資訊科技，它涵蓋的網路範圍相當廣泛，從家庭網路（Home Area Network，HAN）、電力線通訊（Power Line Communication，PLC）、鄰里區域網路（Neighborhood Area Network，NAN）與廣域網路（Wide Area Network，WAN）。

智慧型電錶基礎建設（Advanced Metering Infrastructure，簡稱 AMI）是智慧電網的核心，主要由智慧型電錶（Smart Meter）、通訊系統、電錶資訊管理系統（Meter Database Management System，簡稱 MDMS）所組成。其中，AMI 可以取代傳統人工抄表，亦支援動態電價與提供用戶用電資訊，進而引導用戶自發性節電。

智慧電網的安全目標與一般的網路安全不同，可用性（Availability）的重要性是最高的，接下來才是完整性（Integrity）與保密性（Confidentiality）。因為在電力系統中，保持能源的可用性是第一要務，否則企業將因為無法供電而損失慘重，甚至影響到國家安全。智慧電網利用各種感應裝置來掌握各個節點的運作狀況，並且即時回報至後端伺服器來做決策，因此保持資料完整性是相當重要的一環。在所有的考量因素中，使用者的隱私（Privacy）通常是最後考慮的因素。為了將物聯網的構想應用於真實的商業、軍事或社會服務，讓這些應用建立在安全的前提之下，因此前述各項技術都必須重視相關的資訊安全問題。

(2) 物聯網安全技術之關鍵研究課題

A. 無線感測網路安全協定之研究與設計

B. 各種無線感測網路可能遭受的攻擊（Selective Forwarding Attack、Jamming Attack 等等）

C. 無線感測網路之應用

D. 無線射頻識別技術安全協定之研究與設計

E. 無線射頻識別技術隱私權之研究與設計

F. 物聯網之安全性議題之研究

G. 程序控制系統（Process Control Systems，簡稱 PCS）安全性

H. 智慧電錶安全

I. 電力系統狀態估測安全（Power System State Estimation Security）

J. 智慧電網通訊協定安全（Smart Grid Communication Protocol Security）

K. 智慧電網模擬與安全分析（Smart Grid Simulation for Security Analysis）

L. 台灣安全AMI系統（Secure AMI System in Taiwan）

M. 智慧電錶安全與隱私（Security and Privacy in Smart Metering）

（三） 參考文獻

[8-24] Todd Baumeister, “Literature review on smart grid cyber security,” Technical Report CSDL-10-10, Department of Information and Computer Sciences, University of Hawaii, Honolulu, Hawaii, 2010.

[8-25] Fang, X. and Misra, S. and Xue, G. and Yang, D., “Smart grid - the new and improved power grid: a survey,” accepted in IEEE Communications Surveys and Tutorials (COMST).

[8-26] Y. Jiaxi, M. Anjia, and G. Zhizhong, “Cyber security vulnerability assessment of power industry,” IEEE, 2006.

[8-27] A. Valdes and S. Cheung, “Intrusion monitoring in process control systems,” in Proceedings of the 42nd Annual Hawaii International Conference on System Sciences HICSS, pp. 1-7, 2009

[8-28] D. Watts, “Security and vulnerability in electric power systems,” in 35th North American Power Symposium, pp. 559-566, 2003.

[8-29] P. McDaniel and S. McLaughlin, “Security and privacy challenges in the smart grid,” IEEE Security Privacy Magazine, vol. 7, no. 3, pp. 75-77, 2009.

[8-30] R. Berthier, W. H. Sanders, and H. Khurana, “Intrusion detection for advanced metering infrastructures: requirements and architectural directions,” in First IEEE International Conference on Smart Grid Communications, pp. 350-355, 2010.

[8-31] C. Efthymiou and G. Kalogridis, “Smart grid privacy via anonymization of smart metering data," in First IEEE International Conference on Smart Grid Communications, pp. 238-243, 2010.

[8-32] G. Kalogridis, C. Efthymiou, S. Z. Denic, T. A. Lewis, and R. Cepeda, “Privacy for smart meters: towards undetectable appliance load signatures,” in First IEEE International Conference on Smart Grid Communications, pp. 232-237, 2010.

[8-33] NIST Working Group, “Guidelines for smart grid cyber security: vol. 2, privacy and the smart grid,” National Institutes Of Standards in Security, 2010.

[8-34] D. P. Varodayan and G. X. Gao, “Redundant metering for integrity with information-theoretic confidentiality," in First IEEE International Conference on Smart Grid Communications, pp. 345-349, 2010.

[8-35] G. Dan and H. Sandberg, “Stealth attacks and protection schemes for state estimators in power systems," in First IEEE International Conference on Smart Grid Communications, pp. 214-219, 2010.

[8-36] O. Kosut, L. Jia, R. J. Thomas, and L. Tong, “Malicious data attacks on smart grid state estimation: attack strategies and countermeasures,” in First IEEE International Conference on Smart Grid Communications, pp. 220-225, 2010.

[8-37] H. Li, L. Lai, and R. C. Qiu, “Communication capacity requirement for reliable and secure state estimation in smart grid," in First IEEE International Conference on

Smart Grid Communications, pp. 191-196, 2010.

[8-38] L. Xie, Y. Mo, and B. Sinopoli, “False data injection attacks in electricity markets," in First IEEE International Conference on Smart Grid Communications, pp. 226-231, 2010.

[8-39] A. Bartoli, J. Hernandez-Serrano, M. Soriano, M. Dohler, A. Kountouris, and D. Barthel, "Secure lossless aggregation for smart grid M2M networks," in First IEEE International Conference on Smart Grid Communications, pp. 333-338, 2010.

[8-40] H. Khurana, R. Bobba, T. Yardley, P. Agarwal, and E. Heine, "Design principles for power grid cyber-infrastructure authentication protocols," in Hawaii International Conference on System Sciences, 2010.

[8-41] F. Li, B. Luo, and P. Liu, “Secure information aggregation for smart grids using homomorphic encryption,” in First IEEE International Conference on Smart Grid Communications, pp. 327-332, 2010.

[8-42] H. K.-H. So, S. H. Kwok, E. Y. Lam, and K.-S. Lui, “Zero-configuration identity-based Signcryption scheme for smart grid," in First IEEE International Conference on Smart Grid Communications, pp. 321-326, 2010.

[8-43] J. Zhang and C. A. Gunter, “Application-Aware Secure Multicast for Power Grid Communications,” in First IEEE International Conference on Smart Grid Communications, pp. 339-344, 2010.

[8-44] T. Godfrey, S. Mullen, R. C. Dugan, C. Rodine, D. W. Griffith, and N. Golmie, “Modeling smart grid applications with co-simulation," in First IEEE International Conference on Smart Grid Communications, pp. 291-296, 2010.

[8-45] D. Kundur, X. Feng, S. Liu, T. Zourntos, and K. L. Butler-Purry, “Towards a framework for cyber attack impact analysis of the electric smart grid,” in First IEEE International Conference on Smart Grid Communications, pp. 244-248, 2010.

[8-46] G. Lu, D. De, and W.-Z. Song, “SmartGridLab: a laboratory-based smart grid testbed," in First IEEE International Conference on Smart Grid Communications, pp. 143-148, 2010.

[8-47] T. Kavitha and D. Sridharan, “Security vulnerabilities in wireless sensor networks: a survey,” Journal of Information Assurance and Security, vol.5, issue.1, pp. 31-44, 2010.

[8-48] H. Alemdar and C. Ersoy, “Wireless sensor networks for healthcare: a survey,” Computer Networks, vol. 54, issue. 15, pp. 2688-2710, Oct. 2010.

[8-49] Y. Zhou and Y. Fang, “Securing wireless sensor networks: a survey,” IEEE Communications Survey & Tutorials, vol. 10, issue. 3, pp. 6-28, Sept. 2008.

[8-50] M. A. Simplicio, P. Barreto, C.B.Margi,T.Carvalho, “A survey on key management mechanisms for distributed wireless sensor networks,” Computer Networks, no. 54, pp. 2591-2612, 2010.

[8-51] M. Langheinrich, “A survey of RFID privacy approaches,” Personal and Ubiquitous Computing, vol. 13, no. 6, pp. 413-421, 2009.

[8-52] D. N. Duc, D. M. Konidala, H. Lee, and K. Kim, “A survey on RFID security and provably secure grouping-proof protocols,” Journal of Internet Technology and Secured Transactions, vol.2, no. 3, pp. 222-249, Dec. 2010.

[8-53] J. S. Cho, S. C. Kim, S. S. Yeo and S. K. Kim, “Considerations on the security and

efficiency of RFID systems," Journal of IT Convergence and Services, vol. 107, 2012.

[8-54] F. Gandino, B. Montrucchio and M. Rebaudengo, "Tampering in RFID: a survey on risks and defenses," Journal of Mobile Networks and Applications, vol. 14, no. 4, pp. 502-516, 2010.

主題三：惡意程式行為分析與數位鑑識

持續性滲透攻擊 (Persistent Threat 或 Advanced Persistent Threat，簡稱 APT) 是目前網路資訊安全最大的威脅來源之一，尤其是發生於 2010 年 6 月 Stuxnet 事件，藉由持續性網路滲透測試、隱藏惡意程式行為、蔓延，進而攻擊工業控制用系統，造成伊朗核子電廠設施的實體損害。此類事件分別了一般性攻擊與目標導向的持續性滲透（Persistent Threat）的差異，卻也暴露出目前只能防範一般性、已知攻擊與病毒防護系統之不足，同時為了掌握與瞭解滲透入侵的途徑與方法，這些概念也融入、而成為重要的鑑識方法與技術。

因此我們針對此類型的威脅，整理以下幾個研究子題：包括如何蒐集與分析惡意程式（尤其是未知之持續滲透型惡意程式）、對資安設備的保護技術（例如防毒軟體，這是 APT 攻擊首要目標）、網頁安全（不管是網頁伺服器或瀏覽器，都是惡意滲透程式最常運用的途徑）、風險評估（尤其是 APT 的威脅，連實體封閉之工業電腦都能遭受滲透入侵，風險評估成為重要的資安評估與安全量化指標）、安全權限模型（智慧型手機成為滲透入侵主要的管道，APP 權限控管的失當，將是未來最大的資安威脅）、自動滲透攻擊程式產生（零日威脅或 Zero Day Exploit 是 APT 與 Stuxnet 主要運用之滲透方法，藉由自動產生之研究，可進一步瞭解與測試系統之風險）。

（一）國內外發展現況

惡意程式的蒐集已發展相當多年。業界防毒軟體公司也都有各自的蒐集系統在進行惡意程式樣本的蒐集。在蒐集方法上不外乎是透過客戶回報，由客戶提供可疑的程式樣本，或是透過如架設 Honeynet[8-55]系統，獵取具主動網路攻擊能力的惡意程式等作法。隨著近幾年網站跟智慧型終端裝置的盛行，惡意程式已不再侷限於傳統 Windows 等作業系統平台，比如說網站掛碼型蠕蟲（XSS worm）[8-56]，以及如在 Android 裝置上常見的各種惡意程式[8-57]等，也因此在蒐集渠道上必須要能與時俱進地發展。針對網頁型的惡意軟體之蒐集，國外有 Google 所作的相關研究[8-58]；針對 Android 惡意軟體之蒐集也有美國北卡州立大學所開發之 DroidRanger 系統[8-59]等例子。由此可見雖然惡意軟體蒐集已是一發展多年的課題，但隨著新型態的惡意軟體不斷的出現，這方面的研究仍舊相當地活躍。

在惡意軟體的蒐集上，在業界有趨勢科技長期地在進行相關的蒐集工作，然而其資料庫並沒有對外公開。另一方面，國研院國網中心於 2008 年 11 月加入了 Honeynet 國際組織，並從那時開始於全國學術網路佈建分散式的 Honeypot 誘捕系統[8-60]。國內一些大專院校亦有各自獨立架設的蒐集系統等。以學術界而言，我國目前在惡意軟體蒐集上主要還是著眼於傳統作業系統平台如 Windows、UNIX 平台上惡意軟體之蒐集。在蒐集方法上最常見的做法是使用如 Honeypot 等現成的工具進行蒐集，在蒐集方法上並沒有太多自己所特有的創新與發展。另一方面，或許是因為受制於國內較為保守的制度，對於所蒐集到的樣本的分享做的並不是非常的成功。而這也造成說投入了一堆資源，蒐集了一堆惡意程式，然後就沒有下文的現象，而這也是為何蒐集惡意程式的單位也就缺發動機與需求去對蒐集系統與流程去做創新與研發的主要原因之一。

惡意程式行為萃取可分為靜態跟動態萃取法。靜態萃取法是透過反組譯，然後將反組譯所得到的指令流進行語意分析[8-61]。然而靜態萃取法可輕易地被 Opaque Constants[8-62]等程式碼混淆法所擾亂，也因此在近年也開發出了動態的行為萃取方法，其中較廣為人知的系統包過如 BitBlaze[8-63]、TTAnalyze[8-64]、CWSandbox[8-65]、Anubis[8-66]等。動態萃取的做法是透過實際運行待測的惡意軟體，然後觀察其所體現

的行為（包括如網路傳輸、檔案系統存取、系統呼叫等）。常見的作法是將惡意軟體運行於如 QEMU 之類的模擬器中，然後由模擬器萃取其運行時期所展現出來的行為。然而此類做法的一大挑戰是單次的運行過程未必能觸及惡意軟體所有可能的執行流程，也因此對於觀察該程式完整惡意行為的目標恐會有遺珠之憾，針對此議題，在國外有非常多的相關研究，比如說 Symbolic Execution 技術[8-67][8-68]以及如惡意行為觸發條件之自動化偵測[8-69]等。另一方面，近期也有惡意程式具備反偵測模擬器環境的能力，當具備該能力的惡意軟體發覺自己身處於分析環境的時候，會特意地去隱藏其攻擊行為，以達到讓模擬環境無法萃取其惡意行為全貌的目的。針對此議題，國外亦有相關研究 [8-70] [8-71]特別針對此類惡意軟體開發相關的反反偵測機制。針對所萃取之行為的後續分析目前常見的作法是將所觀察到的系統呼叫結合汙染源分析技術，建構出對應的 Data-Flow Dependent System Call Graph [8-72][8-73]，然後透過圖形比對技術如 Tree Automata [8-74] 來進行判讀等。而當分析完成後，後續的問題是如何有效地對於大量的行為資訊進行索引歸檔，針對此議題國外亦有透過 Function Graph Call 資訊，搭配 B-Tree 結構的相關索引結構設計之研究[8-75]。

國內在惡意程式分析研究上最具代表性的為交通大學謝續平教授的研究團隊。該團隊基於 QEMU 模擬器開發出了由國人技術自製的 Malware Behavior Analysis（MBA）系統。該系統具備觀察程式動態行為、汙染源分析、線上反組譯等多項功能。由於惡意程式之萃取與分析是一項進入門檻相當高的研究。在前段萃取的部分需要對系統底層有相當的了解與動手修改與實作的能力，而在後段分析跟比對的部分又需要有演算法理論的基礎與天分。以現況來說，國內年輕一輩的教授從事這方面研究的相對稀少，其中有不錯具體成果的更是趨近於絕跡的狀態。有鑑於惡意程式分析是資訊安全中相當重要的課題之一，而資訊安全又是攸關國家安全的重要基石之一，希望國內有志之士能更積極地投入這方面的研究。

在一個網路系統中，程序或系統的漏洞，如設計不當或使用者行為不當等問題，讓攻擊者趁隙而入。不同的因素所可能引發的風險影響輕重不一，傳統的網路風險評估機制嘗試著找出可能被攻擊的弱點或來源，以利系統管理人員依據評估結果，適時地、適度地提出防衛計劃或修補策略。1998 年，Phillips 等人 [8-101]提出了一種方法建置網路攻擊與風險評估的模型。這個方法可以繪製網路中的攻擊路徑，並找出可能造成意想不到的網路狀態的路徑。Philips 所提的方法是一種以攻擊圖（Attack Graph）為基礎的評估模型，依據攻擊模型、系統配置，以及攻擊者的能力 [8-101][8-102][8-103]，可以繪製出可能的攻擊路徑。這個方法提供網路的詳細資訊，是一種可以有效分析潛在威脅性的工具[8-101][8-104][8-105][8-106][8-107][8-108]。然而，攻擊圖主要是依據系統的漏洞來繪製整個網路的攻擊圖；但是當新設備加入或離開該網路時，攻擊圖卻無法即時反應該網路當下的安全性。重新繪製攻擊圖固然可以解決這個問題，但是重繪攻擊圖的計算負擔，以及無線網路快速的動態變化，會讓攻擊圖的重繪變成整個網路管理的嚴重負荷。隨著網路技術的不斷推陳出新，不論是以攻擊圖為基礎、或是其他類型的風險評估研究都仍然廣受各方注目，此間相關研究依然相當地活躍。

資訊網路的資產價值、系統潛在遭受攻擊的機率、系統的弱點造成的影響範圍與強度，決定了整個資訊網路的風險值。這類的風險評估機制的設計與實現，除了國網中心、TANet 網路中心嘗試導入安全管理機制與培訓專業資訊安全管理人才外，目前僅有少數廠商致力於網路風險評估相關服務與產品的開發，例如美商 Juniper Networks 的網路安全性評估與風險消除服務、DragonSoft 中華龍網的安全漏洞掃描工具等。

在新興的安全權限模型議題方面，美國加州大學柏克萊分校 D. Wagner 教授的研

發團隊 2011 年開始陸陸續續提出 Android 應用程式、廣告之權限管理機制與工具[8-109][8-110][8-111]。其研究團隊於 2011 年所開發的 Stowaway 工具[8-111]可以在編譯 Android 應用程式時，即時地分析偵測該應用程式是否要求過度的權限。隨著手機應用程式的普及，不論是權限管理機制或是權限的安全分析模型，都開始受到各方重視。此間相關議題，是目前迫切需要研究的方向。

在發展自動攻擊程式產生系統時,符號執行與限制式求解都是重要的工具[8-121]。在符號執行方面，許多被發展並應用於動態測試領域，例如 DART [71] 結合真實與符號執行。CUTE[8-126] 處理則支援多執行緒與含指標程式。SAGE 是第一個具 Whitebox Fuzzing 測試之符號執行測試工具。另外 Catchconv 是基於 Valgrind[8-128] 之操控白箱測試工具。KLEE [8-124] 則是基於 LLVM[8-129] 具高涵蓋率之符號執行虛擬機器。在自動攻擊程式產生方面，主要研究方向包括 Metasploit 之 Pattern 產生器，藉由觀察失控指令指標暫存器之特殊樣式數值，可瞭解可能之攻擊輸入相對位置。最近的方法包括 APEG，具比對有問題程式與修補之版本差異，使修補版本之檢查失效。AEG[8-113][8-115] 以多步驟方式產生攻擊運用程式。首先運用符號執行找出可能之問題點,利用擬真執行蒐集執行期間之相關資訊,此方法處理堆疊溢位與格式字串弱點。AEG 是第一個端至端的攻擊產生器，並具備處理符號檔案、符號網路 Socket 能力之自動化系統。Heelan[8-114]則是第一個基於非原始碼的操控分析，檢查 EIP 是否被污染源所影響。另外!Exploitable 與 BitBlaze 等也都可被運用為檢測是否可被操控之偵測。

（二）關鍵研究課題

1. 子題：惡意程式蒐集

(1) 惡意程式蒐集之主題概述

惡意程式收集的目的可從兩方面說明。一方面是對於惡意程式相關研究，會需要有相應的惡意程式樣本作為研究題材,二方面是則是針對惡意程式防護所需之特徵碼，亦須要透過惡意程式的收集，方能持續地對特徵碼資料庫進行更新。此主題主要的著眼點在於惡意程式蒐集的流程與系統的研究。由於惡意程式千奇百怪，在收集上需要透過多種途徑去蒐集。另一方面，由於惡意程式滋生速度驚人，蒐集系統必須要具有快速且有效地蒐集到最新惡意程式的能力。

(2) 惡意程式蒐集之關鍵研究課題

A. 蒐集方法上的創新

B. 新型態惡意軟體（如網頁型、Android、iOS 平台等）之蒐集

C. 所蒐集之惡意軟體之共享及資訊回饋機制

2. 子題：惡意程式行為萃取與分析

(1) 惡意程式行為萃取與分析之主題概述

由於惡意程式數量龐大，再加上程式碼混淆（obfuscation）技術的成熟，惡意程式的判讀已無法單憑反組譯等靜態分析技巧來有效地進行。針對此一問題，在惡意程式的研究上發展出了所謂基於程式行為的比對與分析技術。透過實際執行（或模擬）惡意程式來觀察其動態行為並進行判讀。而這背後的挑戰之一在於執行環境的建置。所建置的執行環境必須要能夠讓惡意程式不疑有他，自然地流露出其攻擊行為。例如某些惡意程式僅在特殊的環境條件下（針對特定節日、特定網路區段等）才會展現其攻

擊行為，如何在實驗室環境中有效地萃取出這些惡意程式的行為，便是一個很重要的研究課題。另外對於觀察程式運行中的行為，比如說其所使用的系統呼叫，所存取的資料等，在當今多樣的化電腦系統環境中必須要有能對應各種系統平台，各種系統環境的萃取機制，而這也是相當困難，繁雜的一件工作。再者，惡意程式行為分析的另一挑戰在於所萃取出之行為的判讀。由於程式執行過程會產生大量的行為軌跡資料(如系統呼叫等)，再加上惡意程式的樣本數以千萬計，針對如此大量繁雜的資料，如何快速且準確地判讀出惡意程式的行為表徵是相當具挑戰性的一個研究課題。

(2) 惡意程式行為萃取與分析之關鍵研究課題

A. 新平台（如 Android、iOS）上惡意程式行為之萃取技術

B. 針對具備偵測分析環境能力的惡意軟體之行為萃取

C. Symbolic execution 行為模擬技術的發展

D. 對於觸發條件的偵測與處理

E. 惡意程式行為之正規描述模型

F. 惡意程式行為比對與判讀

3. 子題：資安防護工具與偵測工具的保護

(1) 資安防護工具與偵測工具的保護之主題概述

面對層出不窮、形形色色的各式攻擊，資安防護工具如掃毒軟體是現今最被廣為採用的防護工具，許多的系統甚至只靠掃毒軟體防護。因此當掃毒軟體失去其防禦的能力時，攻擊者便可如入無人之境，任意地控制失去防護的電腦系統。針對此現象，越來越多的惡意程式在入侵系統後，首先執行的工作便是關閉掃毒軟體，許許多多的方式被惡意程式的撰寫者發展出來，因此在增進掃毒軟體功能的同時，如何保護掃毒軟體亦成為一重要的議題。相同地，自動修補的功能讓程式發展廠商能及時地將程式漏洞與錯誤修補，以避免攻擊者利用相關漏洞入侵系統，因此，自動修補的功能亦是攻擊者鎖定的目標，防護其安全亦是重要的議題。

此外惡習程式偵測與分析工具如 VM、Debugger、Honeypot，由於可蒐集與分析惡習程式的行為，讓惡習程式的行為曝光，成為防禦的對象，因此許多的惡意程式會嘗試避免在偵測與分析工具構建的環境下執行，此外，惡意程式也會發展出許多的機制用以判斷其是否被這些工具觀察。因此發展出相關的反制之道，避免被惡意程式偵測亦一重要的議題。

(2) 資安防護工具與偵測工具的保護之關鍵研究課題

A. 反 VM 偵測技術[8-76][8-77][8-78]

B. 反 Honeypot 偵測技術

C. 反 Debugger 偵測技術[8-79][8-80]

D. 掃毒軟體的防護[8-81][8-82]

E. 自動修補（Auto-Patch）的防護

4. 子題：網頁安全

(1) 網頁安全之主題概述

網頁服務（Web Service）是現今最被廣為使用的網路服務之一。一個完整的網頁存取通常需使用到網頁瀏覽器、網頁伺服器、伺服器端應用程式及資料庫等功能強大與複雜的系統。網頁瀏覽器由網頁伺服器讀取網頁，因此網頁瀏覽器需處理處理外界輸入的資料。隨著網頁瀏覽器功能的增強，網頁瀏覽器已可動態執行撰寫在網頁內的腳本（Script）程式碼，並可利用各式各樣的新增元件（Plug-in） 動態地擴充網頁瀏覽器的程式碼與功能，然而隨著網頁瀏覽器的日益複雜，不同形式的 Memory Correction Error/Buffer Overflow Vulnerability 亦相繼地出現在網頁瀏覽器程式碼或 plug-in 中，攻擊者可根據這些漏洞產生惡意網頁，使瀏覽器在嘗試呈現這些惡意網頁時發生錯誤，進而導致程式執行的流程被導入至動態記憶體（Heap），再利用網頁中的腳本程式執行 Heap Spray 後，攻擊者便可很容易地透過網頁瀏覽器取得瀏覽器所在的電腦控制權。因此，保護瀏覽器使其免於成為攻擊者入侵系統的管道，是網頁安全的重要工作之一。為使一般使用者瀏覽惡習網頁，攻擊者可自行架設網站，誘騙一般使用者瀏覽其網站以發動攻擊。然而對攻擊者而言，更有效的方式是直接入侵高流量的網站，將惡意的內容插入已存在的網頁中。因此，保護網頁伺服器，避免攻擊者竄改網頁，也是研究網頁安全的重要議題。

當越來越多的工作是透過瀏覽器來完成時，使用者的瀏覽過程所構成的歷史紀錄，便成為透露使用者隱私資訊的可能管道。因此，找出所有可能洩露使用者隱私的資訊，發展有效徹底的清除工具，便成為保護使用者隱私的重要工作。常見的隱私資訊出現於網頁系統所使用的 Cookie 元件中。Cookie 讓網頁伺服器確保使用者網頁使用者的身份，然而，伺服器端應用程式如果對輸入的內容或指令沒有做妥善的篩選或確保，攻擊者便可以透過 XSS 或 CSRF 偽裝成 Cookie 的擁有者，使用該擁有者在該網站上所有可存取的資料及權限。因此，防止攻擊者偽裝成合法的使用者存取相對應的網站，便成為網頁服務安全防護的重要一環。

隨著網頁功能的提昇，透過單一的網頁將多個網站的內容相結合便成為一日益普及的服務，但如何避免在此種應用下，不慎破壞同一來源（Same Origin）的原則，便是一個必須妥善解決的問題。最近，HTML 5 的制定與蓬勃發展，使得網頁的功能更為強大，但新的標準所可能產生的新的安全問題，亦需被仔細的研究，以確保 HTML 5 能被安全的使用。

(2) 網頁安全之關鍵研究課題

A. Heap Spray 及 Drive-by-download 等攻擊[8-83][8-84][8-85][8-86]

B. SQL 注入攻擊[8-87][8-88][8-89]

C. XSS、CSRF 相關議題[8-90][8-91][8-92]

D. HTML 5 的安全問題[8-96][8-97]

E. 私密瀏覽[8-98][8-99][8-100]

F. 混搭（Mashup）的安全問題[8-93][8-94][8-95]

G. 釣魚網站的研究：包括建置與預防

H. 預防網頁竄改之相關技術

5. 子題：風險評估

(1) 風險評估之主題概述

所謂風險即是「因為系統的漏洞或弱點，造成某特定威脅可能引發的惡意攻擊事件，或不利整體網路組織的營運」[8-101]。近年來，由於無線網路動態變化的特性，使得網路的管理工作變成一項嚴峻的挑戰。為了協助網路管理人員有效地管理無線網路的安全性，相關的風險評估機制已經成為不可或缺的輔助工具。這類輔助工具或評估方法應能建置網路風險模型，依據網路的動態變化資訊，協助管理人員掌握網路的即時安全情況，並於必要時，採取適當的應變措施。

(2) 風險評估之關鍵研究課題

A. 攻擊圖的優化

B. 以其他統計理論為基礎的風險評估機制

C. 網路安全與風險評估模型設計

D. 風險消除服務

6. 子題：安全權限模型

(1) 安全權限模型之主題概述

隨著 Android 手機與平板作業系統的崛起，權限模型（Permission Model）的安全議題也逐漸受到各方的重視。開發 Android 應用程式時，有時須在 AndroidManifest.xml 指定該應用程式所需的相關權限，以利存取某些資訊或資料如位置、WiFi 網路狀態、手機電池統計資訊、建置暫存檔等等。在大部分情況下，使用者在安裝手機應用程式時，就必須同意這些權限的使用，但是，使用者在使用該手機應用程式的當時（應用程式的動態執行期間），並不樂意這些應用程式存取特定資訊或資源（如位置資訊）。因此，開發適當的權限管理程式，在手機應用程式啟動後或需要時，評估該應用程式所需的權限與對系統安全度的影響後，才給予存取資訊或資料權限，應該是目前需要詳細研究的議題。

(2) 安全權限模型之關鍵研究課題

A. 行動作業系統之權限許可分析

B. 權限安全分析模型：包括動態偵測、靜態分析

C. 行動作業系統之權限管理機制

7. 子題：自動攻擊程式產生

(1) 自動攻擊程式產生之主題概述

攻擊程式的產生通常被視為一種需要特殊技巧的人為工作[8-113]，需具備純熟之安全技能。然而基於最近的符號執行技術的突破性發展，已有多種雛形方法被提出。這些攻擊產生系統，產生包括控制流程攔截、SQL 注入、與跨網站腳本攻擊等方法，常被用來進行 Web 網頁程式的安全稽核[8-117]、IDS 比對碼產生器、並攻擊防護之用。此類研究主要著重於污染分析、並符號執行兩大主軸進行。另外的研究用途為市集軟體之安全驗證，確保軟體上架前必須安全可靠。此類研究的動機是根源於軟體的安全度問題。由於系統的失控當機無可避免，但大量的當機程式，便有迫切的需求來分析瞭解這些問題是否為可被運用之失控情形 (Exploitable Crash)。在軟體失控分析報告中[8-119]，有運用 BitBlaze[8-63]進行人為分析，並與 Exploitable [8-118] 進行研究比較，來確認這些失控的行為中，是否可被運用、並操控為安全弱點。目前的研究中，

主要是運用動態分析與符號執行的方法進行。這些方法偵測是否有被污染的命令指標，運用擬真執行的模擬執行，指引攻擊限制式，藉以操控命令指標。此類型的研究可以將軟體錯誤與安全弱點自動連結，藉以維繫軟體開發的品質、並與軟體安全緊密結合。在大量的軟體失控案例中，可藉以排序產生優先等級。其次是軟體錯誤在未來將可能被運用為後門。為了強化安全保護，彌補措施 (Mitigation) 的研究將是重要的研發方向。

(2) 自動攻擊程式產生之關鍵研究課題

A. 快速 Concolic 執行研究（Fast Concolic Execution）

B. 彌補策略分析（Mitigation Strategies）：包括 ROP、ASLR 與 EMET

C. 可利用的損毀分析（Exploitable Crash Analysis）

（三） 參考文獻

[8-55] Honeynet, “The honeynet project, ” available: http://www.honeynet.org/

[8-56] W. Alcorn, “The cross-site scripting virus,” available: http://www.bindshell.net/papers/xssv/

[8-57] Y. Zhou and X. Jiang, “Dissecting Android malware: characterization and evolution,” presented at the IEEE Symposium on Security and Privacy San Francisco, CA, 2012.

[8-58] N. Provos, D. McNamee, P. Mavrommatis, K. Wang, and N. Modadugu, “The ghost in the browser analysis of web-based malware, ” in USENIX HotBots, 2007.

[8-59] Y. Zhou, Z. Wang, W. Zhou, and X. Jiang, “Hey, You, get off of my market: detecting malicious apps in official and alternative Android markets, ” in Network and Distributed System Security Symposium, 2012.

[8-60] NCHC Taiwan, “Honeynet Project,” available: http://www.honeynet.org.tw/

[8-61] M. Christodorescu, S. Jha, S. A. Seshia, D. Song, and R. E. Bryant, “Semantics-aware malware detection,” in IEEE Symposium on Security and Privacy, pp. 32-46, 2005.

[8-62] A. Moser, C. Kruegel, and E. Kirda, “Limits of static analysis for malware detection,” in IEEE Annual Computer Security Applications Conference, pp. 421-430, 2007.

[8-63] D. Song, D. Brumley, H. Yin, J. Caballero, I. Jager, M. Kang, Z. Liang, J. Newsome, P. Poosankam, and P. Saxena, “BitBlaze: a new approach to computer security via binary analysis,” Information Systems Security, pp. 1-25, 2008.

[8-64] U. Bayer, C. Kruegel, and E. Kirda, “TTAnalyze: a tool for analyzing malware,” presented at the European Institute for Computer Antivirus Research, 2006.

[8-65] C. Willems, T. Holz, and F. Freiling, “Toward automated dynamic malware analysis using cwsandbox,” IEEE Security & Privacy, pp. 32-39, 2007.

[8-66] U. Bayer, I. Habibi, D. Balzarotti, E. Kirda, and C. Kruegel, “A view on current malware behaviors,” in Large-scale exploits and emergent threats: botnets, spyware, worms, and more, pp. 8-8, 2009.

[8-67] A. Moser, C. Kruegel, and E. Kirda, “Exploring multiple execution paths for malware analysis,” in IEEE Symposium on Security and Privacy, pp. 231-245, 2007.

[8-68] E. J. Schwartz, T. Avgerinos, and D. Brumley, “All you ever wanted to know about dynamic taint analysis and forward symbolic execution (but might have been afraid to ask),” in IEEE Symposium on Security and Privacy, pp. 317-331, 2010.

[8-69] D. Brumley, C. Hartwig, Z. Liang, J. Newsome, D. Song, and H. Yin, “Automatically identifying trigger-based behavior in malware,” Botnet Detection, pp. 65-88, 2008.

[8-70] M. Lindorfer, C. Kolbitsch, and P. Milani Comparetti, “Detecting Environment-Sensitive Malware,” in International Symposium on Recent Advances in Intrusion Detection, pp. 338-357, 2011.

[8-71] D. Balzarotti, M. Cova, C. Karlberger, C. Kruegel, E. Kirda, and G. Vigna, “Efficient detection of split personalities in malware,” in Network and Distributed System Security Symposium, 2010.

[8-72] J. Chow, B. Pfaff, T. Garfinkel, K. Christopher, and M. Rosenblum, “Understanding data lifetime via whole system simulation,” in USENIX Security Symposium, pp. 321-336, 2004.

[8-73] J. Newsome and D. Song, “Dynamic taint analysis for automatic detection, analysis, and signature generation of exploits on commodity software,” in Network and Distributed Systems Security Symposum, 2005.

[8-74] D. Babić, D. Reynaud, and D. Song, “Malware analysis with tree automata inference,” in International Conference on Computer Aided Verification, pp. 116-131, 2011.

[8-75] X. Hu, T. Chiueh, and K. G. Shin, “Large-scale malware indexing using function-call graphs,” in Conference on Computer and Communications Security, pp. 611-620, 2009.

[8-76] Peter Ferrie, “Attacks on more virtual machine emulators,” Symantec Advanced Threat Reseach.

[8-77] Alfredo Andr´es Omella, “Methods for virtual machine detection,” www.s21sec.com/descargas/vmware-eng.pdf

[8-78] Xuxian Jiang et al., “Stealthy malware detection and monitoring through VMM-based "Out of the Box" semantic view reconstruction,” ACM Transactions on Information and System Security (TISSEC), 13(2), Feb. 2010.

[8-79] Quynh Nguyen Anh, Kuniyasu Suzaki, “Virt-ICE: next generation debugger for malware analysis,” Black Hat, Las Vegas, NV, July 28-29, 2010.

[8-80] Nicolas Falliere, “Windows anti-debug reference,” Symantec Connect Community, 2010.

[8-81] Syed Nasir Alsagoff, “Manual removal of malware - is it still relevant?,” International Journal of Research and Reviews in Information Security and Privacy, Vol. 1, No. 1, March 2011.

[8-82] Jianfang Shen et al., “Implementation of program behavior anomaly detection and protection using hook technology,” Yunnan, China, 6-8 Jan. 2009.

[8-83] Manuel Egele, Peter Wurzinger, Christopher Kruegel, Engin Kirda, “Defending browsers against drive-by downloads: mitigating heap-spraying code injection attacks,” Proceedings of the 6th International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment, Como, Italy, July 09-10, 2009.

[8-84] Fu-Hau Hsu, Chang-Kuo Tso, Yi-Chun Yeh, Wei-Jen Wang, and Li-Han Chen, "BrowserGuard: a behavior-based solution to drive-by-download attacks," IEEE Journal on Selected Areas in Communications, Volume 29, Issue:7, pp. 1461 - 1468, August 2011.

[8-85] Manuel Egele, Engin Kirda, and Christopher Kruegel, "Mitigating Drive-by Download Attacks: Challenges and Open Problems," In Proceedings of Open Research Problems in Network Security Workshop (iNetSec 2009), Zurich, April 2009.

[8-86] P. Ratanaworabhan, B. Livshits, and B. Zorn, "Nozzle: a defense against heap-spraying code injection attacks," In Proceedings of USENIX Security Symposium, 2009.

[8-87] Michael Martin, Monica S. Lam, "Automatic generation of XSS and SQL injection attacks with goal-directed model checking," Proceedings of the 17th USENIX Security Symposium, San Jose, CA, USA, July 28 - August 1, 2008.

[8-88] Guo, P.J., Jayaraman, K., Ernst, M.D., "Automatic creation of SQL injection and cross-site scripting attacks," Proceedings of the IEEE 31st International Conference on Software Engineering, Vancouver, BC, pp. 16 -24, May, 2009.

[8-89] Viktoria Felmetsger, Ludovico Cavedon, Christopher Kruegel, Giovanni Vigna, "Toward automated detection of logic vulnerabilities in Web applications," Proceedings of the USENIX Security Symposium, Washington, DC August 2010.

[8-90] Riccardo Pelizzi et al., "A server-and browser-transparent CSRF defense for Web 2.0 applications," Proceedings of the Annual Computer Security Applications Conference (ACSAC), Orlando, FL, USA, pp. 5-9 Dec. 2011.

[8-91] Rupali D. Kombade, B.B. Meshram, "CSRF vulnerabilities and defensive Techniques," IJCNIS, vol.4, no.1, pp. 31-37, 2012.

[8-92] Joel Weinberger, Prateek Saxena, Devdatta Akhawe, Matthew Finifter, Richard Shin, and Dawn Song, "A systematic analysis of XSS sanitization in web application frameworks," Proceedings of the 16th European conference on Research in computer security, Leuven, Belgium, Sep., pp. 12-14, 2011.

[8-93] Shun-Wen Hsiao et al., "A secure proxy-based cross-domain communication for Web mashups," Proceedings of the Ninth IEEE European Conference on Web Services, Lugano, Switzerland, pp. 14-16 Sept. 2011.

[8-94] Philippe De Ryck et al., "Security of web mashups: a survey," Information Security Technology for Applications, 15th Nordic Conference in Secure IT Systems (NordSec), LNCS vol. 7127, pp. 223-238, 2010.

[8-95] Steven Van Acker et al., "WebJail: least-privilege integration of third-party components in web mashups," Proceedings of the 27th Annual Computer Security Applications Conference, Orlando, Florida, pp. 5-9, Dec. 2011.

[8-96] Trend Mirco, "HTML5 overview: a look at HTML5 attack scenarios," http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt_html5-attack-scenarios.pdf

[8-97] Michael Schmidt, "HTML5 web security," http://media.hacking-lab.com/hlnews/HTML5_Web_Security_v1.0.pdf

[8-98] H. Said et al., "Forensic analysis of private browsing artifacts," Proceedings of the

International Conference on Innovations in Information Technology, Abu Dhabi, pp. 25-27, April 2011.

[8-99] Z. Weinberg et al., "I still know what you visited last summer: leaking browsing history via user interaction and side channel attacks," Proceedings of the IEEE Symposium on Security and Privacy, Berkeley, CA, May 22-25, 2011.

[8-100] G. Aggrawal et al., "An analysis of private browsing modes in modern browsers, " Proceedings of the USENIX Security Symposium, Washington, DC, Aug. 11-13, 2010.

[8-101] S. Gray, G. Alice, and F. Alexis, "Risk management muide for information technology system," National Institute of Standards and Technology, July 2002.

[8-102] C. Phillips and L. P. Swiler, "A graph-based system network-vulnerability analysis," in New Security Paradigms Workshop, pp. 71 – 79, 1998.

[8-103] O. Sheyner, J. Haines, S. Jha, R. Lippmann, and J. M. Wing, "Automated generation and analysis of attack graph," in Proceedings of IEEE Symposium on Security and Privacy, pp. 273–284, May 2002.

[8-104] L. P. Swiler, C. Phillips, D. Ellis, and S. Chakerian, "Computer-attack graph generation tool," in Proceedings of Information Survivability Conference & Exposition II, pp. 307–321, June 2001.

[8-105] S. Jha, O. Sheyner, and J. Wing, "Two formal analyses of attack graphs," in Proceedings of the 15th Computer Security Foundation Workshop, pp. 49–63, 2002.

[8-106] V. Mehta, C. Bartzis, H. Zhu, E. Clarke, and J. Wing, "Ranking attack graphs," in Proceedings of Recent Advances in Intrusion Detection, 2006.

[8-107] J. Pamula, S. Jajodia, P. Ammann, and V. Swarup, "A weakest-adversary security metric for network configuration security analysis," in Proceedings of the 2nd ACM Workshop on Quality of Protection, pp. 31–38, 2006.

[8-108] L. Wang, A. Singhal, and S. Jajodia, "Toward measuring network security using attack graphs," in Proceedings of the 2007 ACM Workshop on Quality of Protection, pp. 49 – 54, 2007.

[8-109] L. Wang, A. Singhal, and S. Jajodia, "Measuring the overall security of ntwork configurations using attack gaphs," in Proceedings of the 21th IFIP WG 11.3 Working Conference on Data and Applications Security, 2007.

[8-110] Adrienne Porter Felt, Elizabeth Ha, Serge Egelman, Ariel Haney, Erika Chin, and David Wagner, "Android permissions: user attention, comprehension, and behavior," UC Berkeley Technical Report No. UCB/EECS-2012-26 (under review), 2012.

[8-111] Paul Pearce, Adrienne Porter Felt, Gabriel Nunez, and David Wagner, "AdDroid: privilege separation for applications and advertisers in Android," ACM Symposium on Information, Computer and Communications Security (AsiaCCS).

[8-112] Adrienne Porter Felt, Erika Chin, Steve Hanna, Dawn Song, and David Wagner, "Android permissions demystified," ACM Conference on Computer and Communication Security (CCS), 2011.

[8-113] Sutton, M.; Greene, A.; Amini, P. "Fuzzing: brute force vulnerabilty discovery," 2007.

[8-114] Avgerinos, T.; Cha, S.K.; Hao, B.L.T.; Brumley, D., "AEG: Automatic exploit generation," in Proceedings of the Network and Distributed System Security

Symposium (NDSS'11), San Diego, CA, USA, 2011.

[8-115] Heelan, S, "Automatic generation of control flow hijacking exploits for software Vulnerabilities," 2009.

[8-116] Schwartz, E.J.; Avgerinos, T.; Brumley, D., "Q: exploit hardening made easy," in Proceedings of the USENIX Security Symposium, 2011.

[8-117] Martin, M.; Lam, M.S., "Automatic generation of XSS and SQL injection attacks with goal-directed model checking," Proceedings of the 17th conference on Security symposium: pp. 31-43, 2008.

[8-118] http://msecdbg.codeplex.com/.

[8-119] Miller, C.; Caballero, J.; Johnson, N.M.; Kang, M.G.; McCamant, S.; Poosankam, P.; Song, D., "Crash Analysis with BitBlaze," at BlackHat USA, 2010.

[8-120] Kim, D.; Wang, X.; Kim, S.; Zeller, A.; Cheung, S.C.; Park, S., "Which crashes should I fix first?: Predicting top crashes at an early stage to prioritize debugging efforts," IEEE Transactions on Software Engineering, 37 (3), pp. 430-447, 2011. ISSN 0098-5589.

[8-121] Schwartz, E.J.; Avgerinos, T.; Brumley, D., "All you ever wanted to know about dynamic taint analysis and forward symbolic execution (but might have been afraid to ask)," IEEE Symposium on Security and Privacy, pp. 317-331, 2010.

[8-122] Ganesh, V.; Dill, D., "A decision procedure for bit-vectors and arrays," Computer Aided Verification, pp. 519-531, 2007.

[8-123] Chipounov, V.; Kuznetsov, V.; Candea, G., "S2E: a platform for in-vivo multi-path analysis of software systems," Proceedings of the 16th International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS'11), Newport Beach, CA, USA, pp. 265-278, 2011.

[8-124] Cadar, C.; Dunbar, D.; Engler, D.R., "KLEE: unassisted and automatic generation of high-coverage tests for complex systems programs," Proceedings of the 8th USENIX Symposium on Operating Systems Design and Implementation (OSDI'08) San Diego, California, USA, pp. 209-224, 2008. ISSN 978-1-931971-65-2.

[8-125] Godefroid, P.; Klarlund, N.; Sen, K. (2005). "DART: directed automated random testing," Proceedings of the ACM SIGPLAN 2005 Conference on Programming Language Design and Implementation (PLDI'05), Chicago, IL, USA, pp. 213-223, 2005. ISSN 1-59593-056-6.

[8-126] Sen, K.; Marinov, D.; Agha, G., "CUTE: a concolic unit testing engine for C," Proceedings of the 10th European Software Engineering Conference held jointly with 13th ACM SIGSOFT International Symposium on Foundations of Software Engineering (ESEC/SIGSOFT FSE'05), Lisbon, Portugal, pp. 263-272, 2005. ISSN 1-59593-014-0.

[8-127] Godefroid, P.; Levin, M.Y.; Molnar, D.A., "Automated Whitebox Fuzz Testing," Proceedings of the Network and Distributed System Security Symposium (NDSS'08), San Diego, CA, USA, 2008.

[8-128] Nethercote, N.; Seward, J., "Valgrind: a framework for heavyweight dynamic binary instrumentation," Proceedings of the ACM SIGPLAN 2007 Conference on Programming Language Design and Implementation (PLDI'07), San Diego, CA, USA, pp. 89-100, 2007. ISSN 978-1-59593-633-2.

[8-129] Lattner, C.; Adve, V.S., “LLVM: A Compilation Framework for Lifelong Program Analysis & Transformation,” Proceedings of the 2nd IEEE / ACM International Symposium on Code Generation and Optimization (CGO’04), San Jose, CA, USA, pp. 75-88, 2004. ISSN 0-7695-2102-9.

主題四：雲端計算安全

雲端計算（Cloud Computing）是一種新的運算模式，讓使用者可以透過無所不在與隨選服務的網際網路存取，來使用共享的計算資源與服務。雲端計算資源包含計算能量、儲存伺服器、公用資料、應用程式與服務等。由於資源存在於網際網路上，在電腦流程圖中網際網路常以一朵雲圖來表示，因而有了「雲端」服務之名，終端使用者不需要了解雲端資源的細節，不必具有相對應的專業知識，也無需對資源直接進行控制，只需關注自己真正需要的資源概念，以及如何透過網路來得到相應的服務，由整合連接的基礎設施與跨平台的使用介面，獲取持續且一致的使用經驗。雲端計算服務具備以下特徵：

- 基於虛擬化技術快速部署資源，資源整合
- 實現動態的、可伸縮的擴展
- 提供隨選服務
- 按需求提供資源、按使用量付費
- 寬頻網路服務，通過網際網路提供、面向海量信息處理
- 減少用戶終端的處理負擔
- 降低了用戶對於 IT 專業知識的依賴

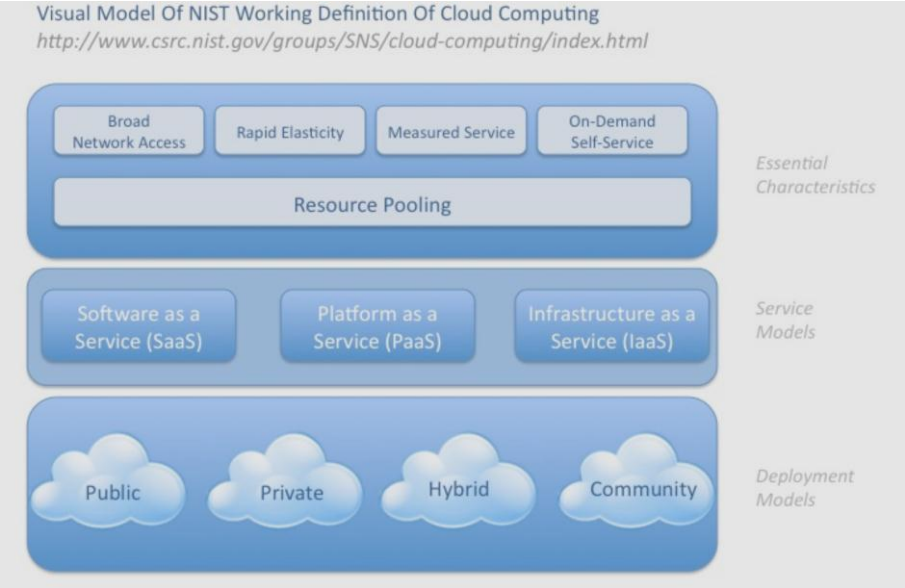

圖 8-1：NIST 的雲端計算模式

根據 NIST 的定義[8-138]，雲端計算服務可分為軟體即服務（Software as a Service, SaaS）、平台即服務（Platform as a Service, PaaS）以及基礎建設即服務（Infrastructure as a Service, IaaS）三類。其中，SaaS 可打破以往大廠壟斷的局面，軟體開發人員或公司都可以自由揮灑創意，面對全世界的使用者提供各式各樣的軟體服務。PaaS 可打造程式開發與作業系統平台，讓開發人員可以透過網路撰寫程式。IaaS 將基礎設備如資通訊設備、網路頻寬、資料庫等，整合起來，提供給個人、公司、機構等租用，減輕直接購置與管理的成本。後來還有許多相對應的觀念被提出來，例如 CaaS（Computing as a Service）等。

至於雲的種類，NIST 根據雲的佈建對象，分為私有雲（Private Cloud）、社區雲

（Community Cloud）、公開雲（Public Cloud）與混合雲（Hybrid Cloud），如**錯誤! 找不到參照來源。**所示。國際研究暨顧問機構高納德（Gartner）將通雲端計算的議題，區分為雲端服務與雲端技術兩類。雲端服務為一種新的服務方式，網路服務透過瀏覽器與網際網路來存取操作，使用者完全不必去擔心成長的問題。這一類的雲端計算可視為網格運算（Grid Computing）與 SaaS 的自然延伸。雲端技術涉及新的技術，採用多台電腦一同運算、儲存、相互備援，目標在增加運算能力、儲存能力、安全性等，邏輯上將集中運算隱藏在雲後,由巨型資料中心提供個別使用者難以生成的運算成果。雲端計算將啟發更多創新思維，譬如於雲端計算下，可能會因機房空間使用的減少、電力消耗的減少、IT 人員需求技能的改變等，而提供不受硬體限制的創新服務。使用者端擁有一個瀏覽器就可以使用所有雲端服務，譬如使用者端可以不要安裝文書處理軟體、不要安裝簡報軟體等軟體,因而使用者端電腦就不必購買功能強大的電腦設備。

雲端計算被視為繼 Web 2.0 之後，下一波科技產業的重要商機。根據美林證券估計，未來 5 年全球雲端計算市場規模將達到 950 億美元，占全世界軟體市場的 12%。高納德的報告則認為，至 2012 年有 80%財星 500 大企業會使用各式不同的雲端計算服務。國際數據資訊中心（IDC）的資料則顯示，未來 5 年雲端服務的平均年成長率可望達到 26%。根據 DIGITIMES 企業 IT 所執行的『2011 年台灣製造業 e 化大調查』，高達 68.3%的製造業資訊部門受訪窗口認為，未來三年內在台灣製造業 e 化進程中，雲端計算將有重要的影響。資策會於 2010 年第 2 季發表的「企業雲端服務需求調查」顯示，雖然目前僅 4.9%企業採用雲端形式的資訊系統，但是另有 36%的企業考慮在未來 1 年內將資訊系統與服務轉變成雲端架構。

當各界聚焦在雲端計算所帶來的便利服務時，新衍生的資安議題，例如雲端資料隱私與安全、使用者的隱私、資訊可靠度等，將會是下一波資訊安全的重要議題。一旦重要的資料中心發生資料洩露、系統離線暫停，或資安策略變更等問題，影響的範圍將更加廣大。例如，2011 年亞馬遜暫停其雲端服務，即致使採用其 AWS 服務的許多網站關閉逾 30 小時。中國大陸曾要求雅虎交出異議人士的郵件資訊，該異議人士即被以此定罪。Google 則因嚴苛的網路內容的審查制度等事件，於 2010 年退出中國大陸市場。新力的 PSN 網路遊戲平台及網上音樂平台 Qriocity 遭黑客入侵，近七千七百萬會員的個人資料被盜。標榜較臉書注重隱私的 Path，其 2.0 版在沒有徵求或告知使用的情形下，私自把用戶手機裡面的聯絡人資訊上傳到 Path 開發商的伺服器上，嚴重違反個人的隱私。大眾對於隱私權的關心，主要在於詐欺犯罪及商業騷擾,然而，政府基於國家與社會安全為理由，對於雲端服務的干涉卻為人忽略。例如，在 2001 年 911 事件之後，美國對人權的干涉與管制趨向嚴格；微軟為了符合『美國愛國者法案』的要求，將使微軟位於全球任何地點的雲端資料無法受到隱私保護。

雲端安全聯盟（Cloud Security Alliance）報告 [8-134] 中指出，雲端計算正面臨七大安全威脅：(1)濫用或利用雲端計算進行非法的行為；(2)不安全的介面與應用程式；(3)惡意的內部人員；(4)共享環境所造成的問題；(5)資料遺失與外洩；(6)帳號與服務被竊取；(7)未知的雲端風險模型。高納德亦曾在研究報告中 [8-136]，整理出七項使用雲端計算所需評估的安全風險的議題：(1)特權使用者的管理；(2)法規的遵守；(3)資料所在的位置；(4)資料的隔離；(5)回復能力；(6)支援調查的能力；(7)永續的使用性。這些報告顯示使用第三方的雲端計算平台佈署機密的資料與系統時，存在著風險，用戶在使用雲端計算架構與技術的同時，應該要同時考量到資訊安全、資料與系統可靠性、風險，及各國法規等相關問題。

（一） 國內外發展現況

2006 年 3 月，亞馬遜推出彈性運算雲端（Elastic Compute Cloud，簡稱 EC2）服務。2006 年 8 月，Google 行政總裁 Eric Schmidt 在搜尋引擎大會（SES San Jose 2006）中，首次提出「雲端雲算」的概念。2007 年 10 月，Google 與 IBM 合資超過 1,500 萬美元，建立 Google 101 大型資料運算中心，並開始在美國大學校園，包括卡內基美隆大學、麻省理工學院、史丹福大學、加州大學柏克萊分校及馬利蘭大學等，推廣雲端計算的計畫。2008 年 1 月，Google 宣佈將雲端計算定為未來的發展策略，在台灣啟動「雲端計算學術計畫」，與台大、交大等學校合作，將這種先進的大規模、快速運算技術推廣到校園。2008 年 7 月，雅虎、惠普和英特爾宣布一項涵蓋美國、德國和新加坡的聯合研究計畫，推出雲端計算研究測試床，推進雲端計算。該計畫要與合作夥伴建立六個資料中心作為研究試驗平台，每個資料中心配置 1,400 個至 4,000 個處理器。雅虎並將開源雲端計算框架 Hadoop，應用在自家搜尋服務的兩千台伺服器上，來處理超過 5 Petabytes 的網頁內容，建立整個網際網路的網頁索引資料。亞馬遜的 Web Services，透過虛擬化的技術，與計算服務及 EC2 及儲存服務 S3，提供各種不同規格的虛擬主機和儲存空間。微軟在雲端的策略則是『軟體+服務』，推出 Azure 平台，讓軟體開發者所撰寫的程式直接在微軟資料中心上線。VMware 與 Citrix 則在其虛擬機平台上，推出虛擬化桌面、應用程式等方案。2010 年 2 月，台灣趨勢科技公司宣布子公司騰雲計算 (TCloud Computing) 正式成立，將提供建置公用雲與私有雲所需的技術開發、系統整合、技術支援、教育訓練、與專業顧問等服務。2010 年 5 月，台灣中華電信提出 hicloud CaaS 服務，是採用雲端技術所全新開發之雲端產品，提供真實的虛擬運算環境，可以在多種作業系統上使用服務介面，達到穩定、安全、可靠的網路服務環境，使用者可以載入自訂的應用環境及程式，執行自己所要提供的網路服務。廣達的 Qmulu 計畫，在電腦硬體開發上加強與雲端的聯繫。國內許多科技業公司也積極發展雲端的設備與提供雲端服務，例如，華碩、台達電，宏碁公司等。

目前許多大企業正在積極建置其私有雲，如 2007 年 IBM 的藍雲計畫，提供導入雲端計算的工具和服務，允許企業將運算任務分成不同組件，且分派到最有效率的電腦系統執行，可解決企業尖鋒、離鋒時間的系統負荷量問題。同時大企業所建置的雲端計算環境所剩餘能量，可租借給其供應商與客戶，以分擔成本及增加收入。中小企業大都使用公有雲，或租借大型企業剩餘的雲端計算能量。

行政院於 2010 年 4 月宣布啟動「雲端計算產業發展方案」，預訂 5 年（2010-2014）內投入 240 億元於 15 項計劃，希望達成雲端服務應用體驗 1,000 萬人次，帶動企業研發投資 127 億元，促成雲端計算產值累計達 1 兆元的目標。在經濟部技術處的指導下，工研院、資策會、中華電信、台灣區電機電子公會與中華民國資訊軟體協會聯合規畫籌組「台灣雲端計算產業協會」，推動台灣 IaaS、PaaS 與 SaaS 雲端應用服務，發展軟硬體緊密整合的雲端系統平台，協助台灣產業朝系統解決方案及軟體服務的結構轉型。2012 年 3 月，啟動台灣雲谷，提供相關雲端產業一站購足式的服務，包括，解決方案整合研發，測試驗證，成果展示體驗，成果育成，業務轉介及技術交流等，帶動台灣雲端計算產業發展。工業技術研究院於 2009 年成立雲端計算行動應用科技中心，於 2011 年 5 月發表 Cloud OS 1.0 系統，該系統以虛擬化技術 Xen 為核心，整合運算資源管理機制、網路擴充能力、資料中心負載平衡機制和高可用設計等多種技術，是我國開發的第一個雲端作業系統。國科會於 2010 年開始啟動『雲端計算-安全技術與資訊安全技術研發專案計畫』，提供研發經費給學界從事雲端計算安全的研究與相關人才的培養。

（二） 關鍵研究課題

根據雲端安全聯盟[8-135]與 NIST[8-137]的建議，參考國科會雲端計算研發專案申請要點[1]及相關的資料，本規畫的雲端計算安全關鍵研究課題分為三大類『雲端計算安全技術』(Security in Cloud Computing)、『雲端計算的隱私保護問題』(Privacy in Cloud Computing)及『雲端計算的可靠性』(Reliability and Dependability in Cloud Computing)，相關研究子題規劃如下。

1. 子題：雲端計算安全技術

(1) 雲端計算安全技術之主題概述

雲端計算和以往的計算模式非常的不同，當使用者將資料放到公開雲中，並利用共享的計算資源處理資料時，同時暴露給攻擊者成為攻擊的目標，攻擊者取得空前的優勢，實在不得不慎。安全研究的首要課題是管理權（Governance），使用機構必須控制與監督政策、安全與隱私規範、標準、資料位置、程序等，對於使用服務的設計、實現、測試與監控要有掌權，才能有夠有好的開始。雲端計算的軟體與硬體架構是影響安全的重要因素，底層的硬體架構與系統是由提供者決定，虛擬機器是提供 IaaS 服務的基本單元，Hypervisor 介於作業系統與硬體平台之間，安全的研究課題包含架構的安全、虛擬機器之區隔、虛擬系統之資料穿透、Hypervisor 的安全、系統弱點檢測、系統的監控與安全防護、雲間與雲內的通道安全、虛擬網路的保護等。傳統的安全防護軟體，如防火牆及入侵防護系統等，需找出適用於雲端架構的解決方案。在安全即服務（Security as a Service）的發展上，可以發展提供阻斷式安全、電子郵件防護、網頁安全閘道、遠端弱點掃描、資安情報服務等資安應用程式。

在雲端計算上，使用者身份認證與資料的存取控制須有不同的做法，對於跨雲間的身份認證目前有 SAML（Security Assertion Markup Language）及 OpenID 標準，XACML（eXtensible Access Control Markup Language ）可用於雲端資料的存取控制。雲端軟體是由使用者共用，會在不同的虛擬機器上執行，如何做好軟體隔離是重要的課題。

(2) 雲端計算安全技術之關鍵研究課題

A. 雲端資料的私密性問題（Cloud Data Confidentiality）

B. 雲端資料運用、儲存與傳遞的安全問題（Security for Data In-use, At-rest and In-transit）

C. 雲端資料的完整性問題（Cloud Data Integrity）

D. 雲內與雲間的網路安全問題（Secure Communications and Networks Inner/Inter Clouds）

E. 公有雲與私有雲的安全通訊問題（Secure Communications between Public and Private Clouds）

F. 雲端系統的攻擊與防禦（Attacks and Prevention in Clouds）

G. 雲端系統的弱點偵測、監控、事件分析與防毒等（Cloud Security Testing, Monitoring, Event analyzing, and Virus detection）

H. 雲端安全政策：建立、自動化、實施、規範（Security Policies: Establishment, Automation, Enforcement and Compliance）

I. 隨選服務的安全控制（Security Control for On-demand Services）

J. 虛擬機器的隔離與獨立性(Virtual Machine Isolation and Independency)

K. 虛擬機器的監控與安全防護（Virtual Machine Monitoring and Protection）

L. Hypervisor 的安全防護（Security Protection for Hypervisors）

M. 雲端即時應用程式的安全：包括 Web、Web DB、Email 等（Security for Real-time Applications in the Clouds）

N. 終端裝置安全技術與管理（Security and Management for Cloud Clients）

O. 雲端攻擊技術（Cyber Attacks in Cloud Computing）

P. 雲端惡意程式分析（Analysis of Malicious Codes in Cloud Computing）

Q. 安全即服務應用程式的發展（Applications for Security as a Service）

R. 巨量資料之安全分析（Security Analysis of Huge Data）

S. 雲端計算的密碼技術：同態加密、分散式密碼方法、加密資料搜尋、資料授權等（Critical Cryptographic Technology for Cloud Computing）

2. 子題：雲端計算的隱私保護問題

(1) 雲端計算的隱私保護問題之主題概述

雲端技術的快速發展，使用者的過度依賴，私有資料儲存在遠端等等，都讓使用者的隱私暴露在危險中。當資料委外或放在公開雲上，雲端資料隱私性與完整性的問題格外重要，在密碼上，目前有同態加密（Homomorphic Encryption）及完整性檢測的技術，同態加密試圖讓雲端廠商看不懂加密的資料，但應用程式仍能對資料進行運算，這時資料與應用程式可以在同一個雲端伺服器上；完整性檢測的技術讓使用者確認資料確實存在與雲端伺服器上。Unhosted 技術源於對 Web 2.0 平台提供者的反撲，使用者希望對自己的資料擁有控制權，此技術可以延伸到雲端資料的隱私上，將資料與應用程式分由不同的雲來提供服務。

(2) 雲端計算的隱私保護問題之關鍵研究課題

A. 使用者的身份與權限管理（Authentication, Authorization and Accounting for Cloud Computing）

B. 雲端計算使用者的隱私與匿名（Privacy and Anonymity of Users）

C. 雲端資料的隱私性（Data Privacy in Cloud Computing）

D. 雲端資料探勘的隱私保護問題（Privacy Issues for Data Mining in Clouds）

E. 雲端資料存取、授權、分享與轉移（Data Access, Authorization, Sharing, Transfer）

F. 雲端計算的隱私政策：建立、自動化、實施、規範（Establishment, Automation, Enforcement and Compliance）

G. 雲端隱私的密碼技術：Unhosted 及 Homomorphic Encryption（Unhosted and Homomorphic Encryption）

3. 子題：雲端計算的可靠性

(1) 雲端計算的可靠性之主題概述

雲端應用的可靠性包含若干需求，如雲端的應用程式需可隨時存取 (99.999% 可

靠度)，伺服器架構需提供足夠的頻寬供系統擴充以因應後續使用者增加，所有的服務及使用者操作需具備安全保護機制等。在 IaaS 層級，資料中心從建築、電力到電腦系統，均須納入可靠性的考慮。虛擬化業者最常提供的方案是冗餘配置、多重網路連結等方案，藉由資源的重複配置如容錯硬碟及多重資料中心備份，以確保可用性。PaaS 層級，則可對虛擬機進行備份及遷移，以在系統重度負載或失效時，仍能提供服務；例如，VMWare 的 ESX，Citrix 的 Xen 及微軟的 VMM，均提供虛擬機不停機的遷移功能。將服務佈署到多重供應商，也可以避免服務的中段，蘋果為了保證 iCloud 雲端服務的穩定性，採多供應商策略以分散風險，由微軟和亞馬遜聯手提供伺服器支援。此間研究議題包括下列各項。

(2) 雲端計算的可靠性之關鍵研究課題

A. 雲端資料的可用性（Data Availability）

B. 資料的容錯性與可靠性安全技術（Fault-Tolerance and Reliability in Cloud Computing）

C. 雲端計算的正確性保證（Correctness Assurance of Cloud Computing）

D. 雲端資料與應用程式之維護與災害復原（Maintenance and Disaster Recovery of Cloud Data and Applications）

E. 雲端計算的風險分析（Risk Analysis for Cloud Computing）

F. 雲端服務的品質保證（Service Quality Guarantee for Cloud Computing）

G. 多代理環境之信任機制（Trustness in Multi-agent Systems）

然而，如果是將傳統資訊安全領域的研究成果直接運用在雲端計算上，則為不鼓勵之研究。因為雲端計算是新形態的運算模式，本主題規劃鼓勵雲端平台上的新創想法，或需發展適合雲端計算之額外技術。

（三） 參考文獻

[8-130] 「雲端計算與資訊安全技術」研發專案補助申請要點，國科會，2010，2011。

[8-131] 擁抱雲端計算：從掌握安全威脅開始。DIGITIMES 中文網，2010。

[8-132] 鐘嘉德、高天助、楊嘉栩，雲端計算與產業發展。研考雙月刊 34 卷第四期，2010。

[8-133] T. Mather, S. Kumaraswamy, S. Latif, “Cloud security and privacy: an enterprise perspective on risks and compliance,” O'Reilly Media, September, 2009.

[8-134] Cloud Security Alliance, “Top threats to cloud computing V1.0,” March, 2010.

[8-135] Cloud Security Alliance, “Security guidance for critical areas of focus in cloud computing 3.0”, September, 2011.

[8-136] Gartner, “Assessing the security risks of cloud computing,” June, 2008

[8-137] NIST, “Guidelines on security and privacy in public cloud computing,” SP 800-144, December, 2011.

[8-138] NIST, “A NIST definition of cloud computing,” SP 800-145, September, 2011.