出國報告（出國類別：研究）

「資安品質需求工程研習會」心得報告

服務機關：國防大學理工學院

姓名職稱：資訊科學系楊尚青上校副教授

國防科學研究所王憶魯少校博士學員

派赴國家：美國

出國期間：98 年 5 月 4 日至 98 年 5 月 15 日

報告日期：98 年 5 月 29 日

摘要

國防大學理工學院持續結合國防部資通安全策略、管理、研發、教育等各方面人員共同參與，經由 iCAST 跨國研究計劃之推動，將美國卡內基美濃大學（Carnegie Mellon University, CMU）之 CyLab、軟體工程學院(Software Engineering Institute, SEI)與電腦緊急應變暨協調小組（Computer Emergency Response Team Coordination Center, CERT/CC）共同在資安教育與技術領域的卓越成就，以辦理研討會方式共同研討交流。由國防大學理工學院與國立成功大學共同合作規劃籌備，在中研院總計畫辦公室經費補助下，此次「資安品質需求工程(Security Quality Requirements Engineering, SQUARE)研習會」由國防大學理工學院楊尚青副教授率領該校博士生王憶魯、成大研究助理張百成先生等人赴 CMU 與 iCAST 計畫在當地之各校學生計有：成功大學孫明功同學、林孝青同學；中山大學賴谷鑫同學；台灣大學陳力銘同學、廖耘同學；台灣科技大學葉倚任同學等人，一同參與「資安品質需求工程研習會」，透過 SQUARE 研習會互動式情境學習讓學員，得以了解需求工程於資訊安全品質之重要性。此外，並邀請相關專家學者進行相關學術研究議題之研討，建立未來合作研究議題的共識。

目錄

壹、目的

資安品質需求工程(Security Quality Requirements Engineering, SQUARE)方法係由卡內基美隆大學軟體工程學院 CERT 專案計畫資深成員 Nancy R. Mead 教授所領導開發的，係提供一個在軟體開發專案計畫中確認資訊安全需求的系統性方法。大家都認同需求工程是產業界任何開發計畫成功的關鍵因素，一些權威研究也顯示，因需求工程問題日後所導致的成本是在需求發展期間發現並立即更正所需成本的 10 至 200 倍。另外一些研究也發現在大部分的軟體開發計畫中，重作需求問題的成本占總計畫成本的 40-50%，由於需求工程所產生的問題占 50%以上，其成本約占總計畫預算的 25-40%。SQUARE 是一個軟體發展生命週期方法，此方法建議在整個軟體開發生命週期中進行一系列各種不同措施，以改善專案計畫的安全性。藉由國內成員赴美國參與 CERT/CC 之 SQUARE Workshop 期間，可與其他的研究團隊專家學者，進行研討與會談，拓展國際學術合作交流之機會，並於返國之後舉辦相同之研討會，藉此將該方法引進國內，對國內相關領域之產學研究將有所助益。

圖 1 SQUARE 研習會參與人員及綜合討論

(左圖人員由左至右：葉倚任、孫明功、賴谷鑫、林孝青、Nancy Mead、楊尚青、王憶魯、陳力銘、張百成、廖耘)

貳、過程與結果

SQUARE Workshop 過程與概況

（一）拜會 CyLab

5 月 5 日拜會 Gene Hambrick 先生(Director of corporate relations, CMU CyLab)，感謝其對此次 SQUARE 研習會及 iCAST 台灣學生所提供之相關協助，簡單敘舊間得知 Hambrick 先生計畫於今年十月間訪問韓國，有意願順道訪問台灣，當場表達歡迎之意並禮貌性邀請其能順道來訪，最後代表 iCAST 團隊致贈記念品。並分別拜會 Linda Whipkey 小姐(Manager of Corporate Memberships)及 Tina Yankovich 女士(Senior Administrative Coordinator)，感謝她們對此次 SQUARE 研習會及長期以來對 iCAST 台灣訪問學者(生)所提供之相關協助，並請 Tina Yankovich 女士提供 CIC2311 研究室鑰匙及印表機和其他後勤行政事項協助，最後代表 iCAST 團隊致贈記念品。接著拜會 Dr. Adrian Perrig (Technical Director)感謝其長期以來對 iCAST 計畫與研究團隊之支持與合作，並說明此行來參加 SQUARE Workshop 的目的，亦期盼能提供台灣與 CERT/CC 之 Insider Threat 及 NetSA 研究團隊進行合作的協助與幫忙，最後代表 iCAST 團隊致贈記念品。

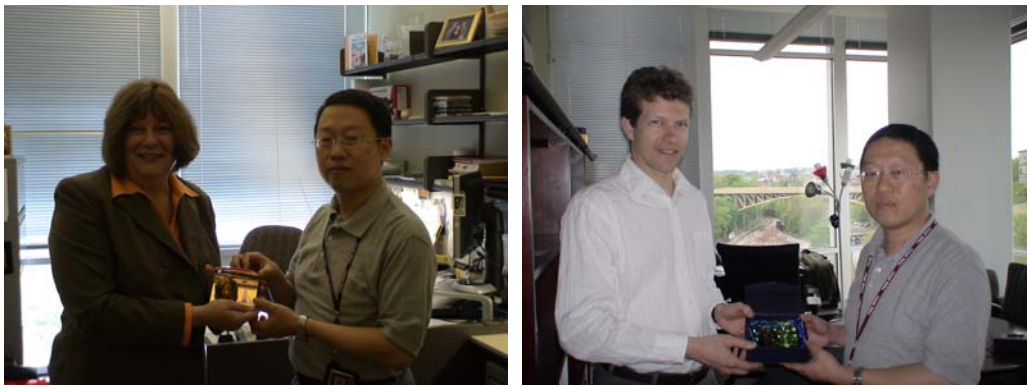

圖 2 致贈 Linda Whipkey 女士(左圖)及 Dr. Adrian Perrig(右圖) 記念品


圖 3 致贈 Tina Yankovich 女士(左圖)及 Gene Hambrick 先生(右圖) 記念品

（二）拜訪 CERT/CC 人員

5 月 6 日於 CIC2312 與 SEI/CERT Business Manager Joseph McLeod meeting 洽談雙方學術合作交流事宜，出席人員計有：國防大學楊尚青老師、王憶魯同學；成功大學張百成助理、孫明功同學、林孝青同學等。首先感謝 McLeod 協助促成此次 SQUARE Workshop 之順利舉辦，並討論希望能持續協助國內學界與美國 CMU CERT/CC 之 NetSA 接軌，並與 CERT/CC 之 Insider Threat 團隊持續合作。McLeod 回覆由於 NetSA 團隊主要執行美國政府機構、國防部及相關單位之機敏專案計畫，一直有協助洽談雙方合作事宜，但因困難度高，目前仍未有突破，建議現階段國內可藉由參加該團隊每年所公開舉辦的「FloCon」研討會來進行。代表 iCAST 團隊致贈記念品。

圖 4 致贈 SEI CERT Joseph McLeod 記念品

（三）SQUARE 研習會前內部研討與準備

5 月 5 日與參加 SQUARE Workshop 的所有 iCAST 台灣學生 meeting，包括成功大學張百成助理、孫明功同學、林孝青同學；中山大學賴谷鑫同學；中央研究院陳力銘助理；台灣大學廖耘同學；台灣科技大學葉倚任同學；國防大學王憶魯同學等 8 位。請所有人簡單自我介紹後，向所有人員說明此次研習會之目的及返國後的任務，並簡單介紹 SQUARE 方法及研習會及相關活動的時程安排規劃，希望能透過參加此次研習會將 SQUARE 方法引進台灣，期盼能引起台灣產、官、學、研各界對軟體安全需求工程(software security requirements engineering)的重視與興趣。此次所有參加人員將預劃於六月底前，於台灣公開舉辦一場相同主題的研討會(SQUARE@TW)。

5 月 6 日與 SQUARE Workshop 指導教授 Nancy Mead 博士進行 Telecon。確認 Workshop 教材及場地等後勤支援皆已備便及確認 Workshop 進行的相關事項。

圖 5 所有參加研習會的 iCAST 成員進行內部研討

（四）SQUARE 研習會概況

研習會地點爲 CIC Conference Room，由 Dr. Nancy Mead 針對 SQARE 簡介及概論，背景、SQUARE 方法論、SQUARE 步驟、SQUARE-Lite、SQUARE 在系統獲得的應用(A-SQUARE) 進行講授，並進行問題與討論。課程充將參與學員分成需求工程組(RE Team)(包括國防大學楊尚青老師、成功大學孫明功同學、中山大學賴谷鑫同學、中央研究院陳力銘助理)及客戶組(Client)(包括成功大學張百成助理、林孝青同學、台灣大學廖耘同學、台灣科技大學葉倚任同學、國防大學王憶魯同學)。研習會進行 SQUARE 細部的步驟實作，由兩組人員針對九大步驟逐一討論。

SQUARE 九大步驟爲：步驟(1)確定定義(Agree on definitions)、步驟(2) 確認資產與資安目標(Identify assets and security goals)、步驟(3) 發展相關物件以支援資安需求的定義(Develop artifacts to support security requirements definition)、步驟(4)評估風險(Assess risks) 、步驟(5) 選擇引出技術(Select elicitation techniques)、步驟(6) 引出資安需求(Elicit security requirements)、步驟(7) 分類 (Categorize requirements) 、步驟(8) 建立需求之優先順序(Prioritize requirements)、步驟(9) 檢視需求(Inspect requirements)。

每一個 SQUARE 步驟都包括下列事項：工作的描述、需求工程小組的責任、利害關係人的責任、雙方的共同責任、完成該步驟的準則(Exit Criteria)並進行小組實作練習。並討論應用 SQUARE 的現況，SQUARE 在隱私議題的應用(SQUARE for Privacy) 和進行相關工具的介紹。

研習過程中學，於午休時間參加 CyLab Seminar—Inside Theft of Intellectual Property in Organizations: A Preliminary Model, Speaker: Andrew Moore) ；以及參與 MSE 研究生 Spring 2009 End of Semester Final Presentation (聽取 SQUARE 研究團隊的期末報告)。研習會第三天進行非正式的研討、特定議題的討論、SQUARE 工具的討論、腦力激盪、未來計畫。最後並頒發課程認證。

圖 6 SQUARE 研習會活動照片

（五）拜會其他專家學者

研習會第三天(5 月 12 日)下午邀請 SEI CERT 資深技術人員 Andrew Moore 與所有學員研討內部威脅相關議題。

圖 7　楊尚青(中)與 Andrew Moore(左)及 Nancy Mead(右)合照

5 月 13 日上午於 CIC2312 與 ECE 及 CS 合聘教授 Roy Maxion 博士進行研討內部威脅相關研究討論，得以下共識：

1. Roy Maxion 教授可來台參加研討會或擔任 keynote speaker。
2. Roy Maxion 教授可來台講學。
3. 可選派研究人員赴 CMU 參與 Roy Maxion 教授研究團隊進行學術合作研究。

圖 8　致贈 Dr. Maxion 紀念品

5 月 13 日下午並拜訪 CMU Information Networking Institute (INI) Director of Admissions Kari Gazdich 女士，討論日後合作契機。

圖 9　致贈 INI Gazdich 女士紀念品

參、心得感想

一、Cylab 及 SEI 對於本次「資安品質需求工程」研習會的安排相當用心，相關課程 Dr. Nancy Mead 著重於課堂教學、討論及實務的實習或參觀，使 iCAST 受訓學員（成功大學張百成助理、孫明功同學、林孝青同學；中山大學賴谷鑫同學；台灣大學陳力銘同學、廖耘同學；台灣科技大學葉倚任同學；國防大學楊尚青老師及王憶魯同學等人）不僅能學習資訊安全等高科技的基礎，進而熟悉「資安品質」結合「需求工程」相關技術之應用，並透過參與 CyLab 安排專題討論資訊安全課程（內部威脅之智慧財產竊取），加強對資安相關技術的了解，對於學員返國之後續工作與研究方面具有相當大之助益。

二、藉由跨國資安合作，可了解國外一流學府目前進行中的重要研究方向與成果、並可藉此培養國內學生擴展國際視野，亦重視學生國際觀的養成與合作交流經驗，以提昇國際之競爭力。透過「資安品質需求工程」研習，吸取美國先進資訊成熟技術之特質，以增進國內學界之體驗，共同激盪創新之能力。

肆、建議事項

一、持續與 CMU 及相關 CyLab、SEI、CERT/CC 等機構進行學術交流與合作，以發展國內於「內部威脅防制偵測」或「資安品質需求工程」等資安教育訓練與學術研究；並期以 SQUARE, Insider Threat, Privacy 等相關研究整合運用於國軍 M-SOC 或政府 N-SOC 機制的實現。

二、建請考量未來與國內學術界、中研院、中科院、工研院及資策會等相關機構進行合作，以使未來技術移轉、整合與部署更有效益。