

**TO: ICCL**

**出席 International Workshop on Information Security  
Applications 2006 (WISA 2006), Jeju Island, Korea**

- 學而不疑知快活 免教虛作百年人 -

-

**(Aug. 28~30, 2006)**

中央警察大學 王旭正

2006.08.27 (日)

今天清晨仍如平常一般，約 5 時許打開眼睛，開始一天的工作。仍然希望先讀一些語言的叢書，然由於今日要啟程至韓國，故似乎在心情上多一項行程的顧慮/規劃。故索性將時間調整為行李的再檢查後，再來 Make Reading for the Beginning of Today.

此次的行程是與二位學生一起參與，也欲在此行程中，使學生能在無形中，多了些國際面觀，這些經驗絕對是非紙上談兵所能言喻的。整個會議的行程安排為 WISA 2006, Aug. 28-30, 2006, Jeju Island, Korea。為能順利參與行程，我預計前一日，即今日(Aug. 27)到達濟州島。

整個飛機的飛行算是順利，約三小時的時間後，即到達濟州。這是我第二次到 Korea 做學術性文章發表。第一次是 2001 年，當時 WISA 為第二屆，此次 WISA 已舉辦至第七屆，時間過的可真是快。也據我的觀察，WISA 自第三屆後，即開始在 Jeju Island 舉行，時至今年。另外主辦單位也努力將 WISA 能併入 LNCS

刊物，藉此提昇國際學術地位。LNCS (Lecture Notes in Computer Science) 是德國的一個出版社，稱為 Springer-Verlag，所辦的一個學術性研討會的綜合刊物。藉由在 Computer Science 領域裡，各研究領域所舉行的 Public Forums，並將之蒐集成 Proceedings (Springer-Verlag 除 Computer Science 外 亦包括相關的科學領域)。如此一來，一年的刊物即至少可累積 30~50 本(or more)的學術刊物，也使得這方面的研究文獻得以集中，並為有興趣的研究者得以參考。

2006.08.28 (一)

會議的開始由 0830AM 開始，在 Ramada Hotel 舉行。綜合個人對 Conference 舉行的一路走來/參與，大致 Conference 可在三種地方舉行，一為 Campus；二為 Hotel；三為 Convention Center。我個人較為喜歡在 Campus 舉行的環境，因為我可以藉此機會參觀該學校的環境與設施，也吻合個人工作環境的需求與閱歷的累積。然而 Campus 的舉行，對於住宿上，是對參與者較為不便的場所。因為住宿的場所非為參與者所設計，而是較屬於 Campus 的形式，格局是研究生或大學生的宿舍，故設備較為簡略，當然價格也便宜許多。至於第二種場地—Hotel，則在住宿方面，便利許多，然高昂的住宿費用，也讓一般的會議參與者，為此精打細算。最後的 Convention Center，則是一般位於較繁榮的區域，在此參加研討會可順道參觀附近的區域性建築物，感受科技/文化/商業的熱絡。

今天的會議，開場即為論文報告的安排，不似過去參與國際研討會將 Keynote Speech/Tutorial 安排至早場，為會議開序幕。我的朋友/研究同好—Prof. W.S. Chung，亦參與此次的會議。他的講題被安排在 Track A，所做的主題為

「Authentication in Wireless Communications」。事後與之聊述，對於 Security 的研究，由於在基礎理論研究上已臻成熟，故這 2、3 年來，對於 Security 的研究投稿，若所做的研究在創新的部份，若未能“感動” Journal Reviewers，似乎不甚容易被接受。

此部份的困難似乎正困擾著台灣的研究者，因為基植於基礎理論的應用，有大部份的主題皆已被研究過，該如何強調“創新的應用”，個人認為是新進/從事 Information/Communication Security 研究者得思考/轉型的目標之一。

另外本次我的 ICCL (Say it “Eagle”)亦投稿/發表一篇研究報告，篇名為“Flexible Key Management in Required Frequent Migrations Upon Secret Sharing Scheme”被安排在 Track 2B。並於下午由學生做論文報告，學生表現可圈可點，整個過程順利。對於 Session Chair 所提的問題，關於此方法是否存在缺點，在此一併說明：事實上，本方法所存在的三方通訊關係，即 Dealer, User 與 Third Party 的訊息傳輸，仍是十分複雜。如何再簡化或者釐清本方法在三方關係的互動，使得 User 在應用本方法時能夠透明化，訊息的彼此傳送與支援能夠更具連接性與必要/必然性，即是本方法得以再深入之方向/議題。

2006.08.29 (二)

第二天的 Meeting，時間同於第一天，仍是由 0830AM 開始，在跟 Prof. Chung 聊述的過程中，有感於韓國在 Security 研究上的全力投注與經營，非常值得台灣的同好者學習。現在 Korea Conferences, WISA 是其中一個。而台灣至今在 Conference 方面仍維持 Local Conference，亦僅有一個正式的會議。在面對國際化的趨勢下得以經常/常態舉行國際研討會來激發台灣資訊安全的研究能量，也提高舉行 Conference 的品質，訓練學生對於 International Conference 認知。並如何藉由國際化的定位，使學生/研究人員能以更高的規格來要求自己，也促使資

訊安全研究人員能自我提升研究／表達能力，進入國際研究的核心觀。

2006.08.30 (三)

進入第三天的議程，可以明顯的注意到 WISA-2006 時程表仍如歷年的方式，發表行程的時間，僅排至中午。如此而來，對於下午要搭機回去的參與者能更有充裕的準備時間在回程前做充裕的準備。在此次會議的一切會議準備工作與擺設與 2001 年我參與 WISA 時幾乎大同小異。而在網路電腦的使用上，隨著 Internet 的使用趨勢，大會亦將網路的連接以 Wireless 來加以實現。此部份雖給有 Notebook 者帶來便利，但對於若沒有攜帶 Notebook，卻無從與外界聯絡，也許因為是如此所以現代的科技人，幾乎人人得有一台隨身攜帶的 Notebook 才可以隨時隨地以此為工具，記錄生活亦或應付工作上的需求。

在這些天裡，抽空至韓國國立濟州大學走動。該校的校園的確有大學校園的風範，校園的面積、寬度、視野寬闊，看到 Campus 內學生，悠走於其中，享受校園生活的學習，這是一種自在。在該校的一棟建築物中，看到了 2 大行的直立中文字(中華文化影響著實深遠)，敘述著「學而不疑知快活」、「免教虛作百年人」。似乎是一種事物學習上的意境。「不徬徨的學習是一種真知，心中因此得以無限暢活」；「當走出校園免除了制式教育，亦能虛心自我求作學問，修得永續的學習心，才是百年真教育」。您又作何詮釋呢！

一個議程的結束，即是另一個階段的開始，人生歷程/旅程是如此微妙，坎坎坷坷/彎彎曲曲/坦坦蕩蕩/峰迴路轉/高低起伏/自由自在，生命之所以精彩，奧妙就在其中。個人的體會點滴在心頭，當然也因此造就若干生命中的萬種風情與千百面觀！該來該去，或走或留，高低輕重，所有事(當時)皆在運籌惟握的驚奇中，第三者(回憶)看/得以清清楚楚！