**第二十三屆全國資訊安全會議**

**Cryptology and Information Security Conference 2013 (CISC2013)**

**一、舉辦目的**

全國資訊安全會議，每年定期於五月或六月舉行，迄今已舉辦二十二屆。此項學術會議，為我國資訊安全最重要的學術活動之一。該項會議提供學者發表最新電腦密碼學與資訊安全方面的研究成果，及提供相互討論的機會。會議的目的是為了促進學術界、政府單位、和產業界，在資訊安全研究成果的交流。「第二十三屆全國資訊安全會議」由南台科技大學負責主辦，將廣邀學術界、工商業界相關人士、公私立研究機構研究人員及資訊安全與電腦密碼學相關之專家，提供研究論文的發表，大會也將舉辦相關座談會，以提升國內在資訊安全學術領域之研究水準及應用層次，此外，並邀請國內、國際專家學者與會，發表專題演講，促進國際交流並提昇我國資訊安全領域研究之國際形象。

**二、舉辦日期與地點**

1.舉辦日期：中華民國102年5月23日(星期四)至5月24日(星期五)

2.地 點：南台科技大學 (71005 台南市永康區南台街一號)

3.組織成員：

主辦單位：中華民國資訊安全學會、南台科技大學資訊工程系

指導單位：教育部

協辦單位：行政院研考會、國科會工程處工程科技推展中心、國家通訊傳播委員會、工業技術研究院、國家實驗研究院國家高速網路與計算中心、國家實驗研究院科技政策研究與資訊中心、電信技術中心、資策會、中華電信公司等

**大會榮譽主席：**戴謙校長(南台科技大學)

**大會共同主席：**楊中皇教授(中華民國資訊安全學會理事長)、

盧燈茂教授(南台科技大學學術副校長)

郭聰源教授(南台科技大學工學院院長)

**大會指導委員：**(按姓名筆畫順序排列)

|  |  |  |
| --- | --- | --- |
| 方銘川主任(國科會工程科技推展中心) | 謝錫堃主任(國家高速網路與計算中心) | 楊鎮華司長(資訊及科技教育司) |
| 何寶中副執行長(資策會) | 余孝先副所長(工研院資訊與通訊研究所) | 吳宗成教授(台灣科技大學) |
| 洪豐玉院長(中華電信研究院) | 張真誠教授 (逢甲大學) | 謝續平教授(交通大學) |
| 魏學文委員(國家通訊傳播委員會) |  |  |

**議程主席：**

|  |  |  |
| --- | --- | --- |
| 雷欽隆教授(台灣大學) | 王旭正教授(中央警察大學) | 李南逸教授(南台科技大學) |

**籌備主席：**鄭錦楸教授、李育強教授(南台科技大學)

**出版委員：**陳福坤 教授 (南台科技大學)

**議程委員：**(按姓名筆畫順序排列)

|  |  |  |
| --- | --- | --- |
| 王智弘教授(嘉義大學) | 古東明教授(雲林科技大學) | 左瑞麟教授(政治大學) |
| 伍麗樵教授(雲林科技大學) | 江季翰教授(虎尾科技大學) | 何煒華教授(東吳大學) |
| 吳宗杉教授(海洋大學) | 吳建興教授(資策會) | 李永振教授(吳鳳科技大學) |
| 李育杰教授(台灣科技大學) | 李忠憲教授(成功大學) | 李金鳳教授(朝陽科技大學) |
| 李漢銘教授(臺灣科技大學) | 李維斌教授（逢甲大學） | 官大智教授（中山大學） |
| 林芬蘭教授(靜宜大學) | 林祝興教授(東海大學) | 邱榮輝教授(長庚大學) |
| 查士朝教授(台灣科技大學) | 洪國寶教授(中興大學) | 范俊逸教授(中山大學) |
| 孫宏民教授(清華大學) | 婁德權教授(長庚大學) | 張仁俊教授(台北大學) |
| 張光耀副院長(中華電信) | 張克章教授(長庚大學) | 曹偉駿教授(大葉大學) |
| 莊文勝教授(高雄第一科技大學) | 許建隆教授(長庚大學) | 許富皓教授(中央大學) |
| 郭文中教授(雲林科技大學) | 陳同孝教授(臺中科技大學) | 陳君明教授(臺灣大學) |
| 陳育毅教授(中興大學) | 陳宗和教授 (嘉義大學) | 陳嘉玫教授(中山大學) |
| 陳榮傑教授(交通大學) | 曾文貴教授(交通大學) | 曾育民教授(彰化師範大學) |
| 黃仁俊教授(淡江大學) | 黃心嘉教授(淡江大學) | 黃育綸教授(交通大學) |
| 黃宗立教授(成功大學) | 黃明祥教授(亞洲大學) | 楊吳泉教授(義守大學) |
| 楊明豪教授(中原大學) | 楊慶隆教授(東華大學) | 詹前隆教授(元智大學) |
| 詹進科教授(中興大學) | 廖鴻圖教授(世新大學) | 劉培文副所長(資策會) |
| 樊國楨教授(交通大學) | 鄧惟中教授(台灣科技大學) | 鄭伯炤教授(中正大學) |
| 鄭振牟教授(台灣大學) | 盧而輝教授(長庚大學) | 簡宏宇教授(暨南大學) |
| 顏嵩銘教授(中央大學) | 羅乃維教授(台灣科技大學) | 顧維祺教授(臺中教育大學) |

**產學交流委員：**產學合作委員會

**籌備委員：**

宣傳組： 李榮三教授(逢甲大學)、葉禾田教授(南台科技大學)

議程組： 張智超教授(長榮大學)、李泉明教授(樹人醫專)

出版組： 李添福教授(慈濟大學)、張勝麟 教授(南台科技大學)

接待組： 陳炳彰教授(南台科技大學)、楊政達 教授(南台科技大學)

**三、活動內容、議程、參加對象、人數及徵求論文和審查機制**

1. 活動內容摘要：:

此次會議建議以雲端安全、系統安全、資料隱藏、數位鑑識、網路安全、電子商務安全、資料庫安全、通訊安全、網路管理、稽核、入侵行為偵測、密碼學等相關領域論文發表為主，舉凡與資訊安全相關議題均在討論之列。

會議內容建議分以下幾個主軸：

(1) 學術論文發表

(2) Keynote演講

(3) 邀請演講

(4) 產學交流座談會

(5) 資安廠商產品展示

2.議程 :

|  |
| --- |
| 2013年5月23日（星期四） |
| 時間 | 內容 | 地點 |
| 08:30 – 09:00 | 報到 |  |
| 09:00 – 09:15 | 開幕 ： 戴謙校長 (南台科技大學)楊中皇理事長 (資訊安全學會) | 國際會議廳 |
| 09:15 – 10:05 | *Keynote演講(一)*主講人：行政院資通安全辦公室吳啟文副主任題目： 政府資通安全威脅趨勢及防護策略 | 國際會議廳 |
| 10:05 – 10:20 | 茶會 |  |
| 10:20 – 11:10 | *Keynote演講(二)*主講人：日本KDDI研究專員Koji NAKAO題目：Securing the network systems - Darknet based cyber-security technologies for global monitoring and analysis | 國際會議廳 |
| 11:10 – 12:00 | 資訊安全學會會員大會 | 國際會議廳 |
| 12:00 – 13:00 | 午餐(資訊安全學會理監事會議) |  |
| 13:00 – 13:30 | 賴溪松教授論文獎頒獎暨論文成果發表 | 國際會議廳 |
| 13:30 – 14:50 | 論文發表(一)

|  |  |  |
| --- | --- | --- |
| Session A1 | Session B1 | Session C1 |
| (國際會議廳) | (E1304) | (E1305) |

 |  |
| 14:50 – 15:10 | 茶會 |  |
| 15:10 – 16:30 | 論文發表(二)

|  |  |  |
| --- | --- | --- |
| Session A2 | Session B2 | Session C2 |
| (國際會議廳) | (E1304) | (E1305) |

 |  |
| 16:30 – 17:30 | 產學交流座談會主題：個人資料保護法衝擊與因應措施主持人：孫宏民 教授(清大資工系)引言人：樊國楨博士異術科技股份有限公司資訊長周天教授高雄第一科大個人資料保護中心主任邱映曦主任資策會科技法律研究所科技應用法制中心吳國維執行長 NII 產業發展協進會邱志傑理事長 中華民國資料保護協會 | 國際會議廳 |
| 18:00 – 20:00 | 晚宴 |  |

|  |
| --- |
| 2013年5月24日（星期五） |
| 時間 | 內容 | 地點 |
| 09:10 – 10:00 | *Keynote演講(三)*主講人：上海交通大學/杭州師範大學陳克非教授題目：資訊安全教育與人才培養 | 國際會議廳 |
| 10:00 – 10:30 | *Keynote演講(四)*主講人：陝西師範大學楊波教授題目：雲端運算中安全有效的容錯關鍵字搜索 | 國際會議廳 |
| 10:30 – 10:40 | 茶會 |  |
| 10:40 – 11:30 | *Keynote演講(五)*主講人：成功大學資工系黃宗立特聘教授題目：Probabilistic Quantum Key Distribution | 國際會議廳 |
| 11:30 – 12:00 | *Keynote演講(六)*主講人：上海交通大學劉勝利教授題目：Efficient Public Key Cryptosystem Resilient to Key Leakage Chosen Ciphertext Attacks | 國際會議廳 |
| 12:00 – 13:00 | 午餐 |  |
| 13:00 – 14:40 | 論文發表(三)

|  |  |  |
| --- | --- | --- |
| Session A3 | Session B3 | Session C3 |
| (國際會議廳) | (E1304) | (E1305) |

 |  |
| 14:40 –15:00 | 茶會 |  |
| 15:00 –16:40 | 論文發表(四)

|  |  |  |
| --- | --- | --- |
| Session A4 | Session B4 | Session C4 |
| (國際會議廳) | (E1304) | (E1305) |

 |  |

3. 參加對象：

學術界、工商業界相關人士、公私立研究機構研究人員、政府單位與資訊安全與電腦密碼學相關之學者、專家以及研究人員。

4. 參加人數：預估200 人。

5. 徵求論文及審查機制：

 第二十三屆資訊安全會議將於2013年5月23、24日在南台科技大學舉行，歡迎各界人士踴躍投稿。稿件必須具有原創性，且未曾發表之學術論文。會議主題包含密碼學以及資訊安全相關領域的理論、應用、實務、及經驗。論文可用中文或英文撰寫，請用A4大小，四邊各留25mm，單行行距，雙欄文章，不列印頁碼，每篇論文以12頁為限，英文字體Times New Roman 10點，中文標楷體10點（詳細格式請見論文參考格式）。請將論文全文的PDF檔案於投稿截止日期以前傳至本會議的網站，詳細傳送方式請參考會議網頁的說明。為確保論文正確送達，若於一週內未收到電子郵件回覆，請逕與承辦單位聯繫。

論文審查以匿名方式進行，審查結果將於論文接受通知日通知各論文的聯絡人。被接受的論文必須將修正後的版本於製版註冊截止日以前寄回。論文的修正，參照審查意見修改，並製作成PDF格式檔案傳送至本會議的網站。

本次會議將頒發『最佳學生論文獎』，請指導教授鼓勵學生參加，參加此項論文獎評選的資格為學生必須為該論文的第一作者並為資安學會會員，且須親自發表論文。評分重點包含論文品質與論文發表之表現。此外，本次會議將頒『最佳論文獎』，本獎項由評審委員從全部投稿的論文中擇優評選之。榮獲『最佳學生論文獎』或『最佳論文獎』之本會會員，資訊安全學會將補助其參加資訊安全相關國際會議之機票與註冊費用。

聯絡人：李南逸、鄭錦楸、李育強

聯絡電話： 06-2533131 Ext. 3200、3230、3223

聯絡地址：南台科技大學資訊工程系(71005 台南市永康區南台街一號)

電子郵件：stust\_cisc2013@stust.edu.tw

**四、預期成效**

在資訊教育及網路學習的應用上，資訊安全常被忽視，然而只有在做好資訊安全的前提下，使用上才能在隱私權不被侵犯下放心的進行安全的網路學習，同時教育內容提供者也才能在著作權不被侵犯下放心的將內容提供出來供教育學習使用，因此資訊安全在資訊教育及網路學習的應用上是非常重要的一環。透過資訊安全會議的舉辦，在全國資訊安全專家的集思廣益之下，可加速國內學術界、政府單位、和產業界，在資訊安全研究成果的交流，期能培育更多的研究人才，融合理論與實務並落實研究成果，為我國的資訊安全技術發展立下新的里程碑，進而提升資訊教育及網路學習應用之普及。

**五、邀請演講者簡介**

1. **吳啟文：**

美國聖地牙哥州立大學電腦科學研究所碩士，歷任行政院研究發展考核委員會資訊管理處資安組組長、「行政院國家資通安全會報」政府資通安全組主任、「行政院國家資通安全會報」網際防護體系執行秘書，現職為「行政院資通安全辦公室」副主任，負責「行政院國家資通安全會報」網際防護體系與政府機關資通安全技術服務及防護管理相關事宜，主要研究為資通安全、資訊管理、PKI與電子憑證應用等。

1. **Koji Nakao：**

Koji Nakao received the B.E. degree of Mathematics from Waseda University, in Japan, in 1979. Since joining KDDI in 1979, Koji has been engaged in the research on communication protocol, and information security technology for telecommunications in KDDI laboratory. After 2003, Koji has moved to KDDI head office to construct and manage its security systems. In 2004, he has started to additionally work for NICT (National Information Communication Technologies). His present positions are "Information Security Fellow" to manage all the security issues required in KDDI and "Distinguished Researcher" to manage research activities for network security technologies in NICT.

 Koji received the IPSJ Research Award in 1992, METI Ministry Award and KPMG Security Award in 2006, and Contribution Award (Japan ITU), NICT Research Award, Best Paper Award (JWIS) and MIC Bureau Award in 2007 and The Commendation for Science and Technology by the Minister of Education, Culture, Sports, Science and Technology (Prizes for Science and Technology: Research Category) in 2009. He is a member of IPJS and IEICE. Koji has also been a part-time instructor in Waseda University and Nagoya University.

1. **陳克非**：

上海交通大學計算機科學與工程系教授、博士生導師，上海交通大學信息安全工程學院副院長，國家自然科學基金委員會第十屆、第十一屆專家評審組成員，2002 年度國家自然科學獎評審委員會信息科學評審組成員,信息安全國家重點實驗室(中科院研究生院)以及計算機軟件新技術國家重點實驗室(南京大學)學術委員會委員, 上海市信息化專家委員會專家，《軟件學報》編委。1982 年在西北電訊工程學院獲應用數學學士，在西北電訊工程學院和北京中國科技大學研究生院完成碩士階段的學習，於1985年在西北電訊工程學院獲得碩士學位。1990年獲德國阿登納基金會資助，赴德國Goethe-Institut Mannheim學習，1991年進入Justus-Liebig-Uni​​versity Giessen，於1994年獲得博士學位。1985 年至 1990 年在西北電訊工程學院/西安電子科技大學應用數學系和信息保密研究所工作，曾獲 1989 陝西省科技進步二等獎、 1989 年國家教委科技進步二等獎、1990 國家自然科學四等獎、1993 年國家教委科技進步三等獎等。1996 年來到上海交通大學工作，創建上海交通大學密碼與信息安全實驗室。

1. 楊波：

1963年5月出生，漢族，九三學社社員，華南農業大學信息學院、軟件學院院長、教授、博士生導師，獲西安電子科技大學密碼學專業博士學位。研究領域：密碼學。曾任信息產業部信息安全技術專家組成員，陝西省信息及網絡安全保密專家顧問小組成員，西安電子科技大學特聘教授，西安電子科技大學通信工程學院信息工程系副主任，教育部計算機網絡與信息安全重點實驗室副主任，2005 年擔任第四屆中國信息和通信安全學術會議程序委員會主席，2009 年擔任中國密碼學會年會副主席，2010 年擔任The 5th Joint Workshop on Information Security (JWIS 2010) General Chair。現為廣東省“千百十工程”省級培養對象，中國電子學會高級會員，中國密碼學會密碼算法專業委員會委員。

1. 黃宗立

1980年畢業於成功大學獲得工學學士學位，之後，分別於1986年、1988年取得美國西南路易斯安那大學電腦學碩士與博士學位。歷任美國西南路易斯安那大學CACS 研究員(1988~1989)及國立成功大學資訊工程學系教授(1993 ~)，目前是國立成功大學資訊工程學系特聘教授。黃教授之研究領域包含密碼技術、網路安全、資訊安全、門禁系統、錯誤控制碼及量子密碼學。

1. 劉勝利

1995年7月在西安電子科技大學獲工學學士學位；1998年2月在西安電子科技大學獲計算機科碩士學位；1997年3月至2000年1月在西安電子科技大學通信工程學院信息安全與保密實驗室攻讀博士，獲密碼學博士學位；自2000年3月至2002年2月在荷蘭Eindhoven University of Technology（埃因霍溫理工大學）數學與計算機系離散數學組學習，並於 2002年2月26日再獲密碼學博士學位，導師為Henk van Tilborg教授；2002年4月至今在上海交通大學計算機科學與工程系工作，並在密碼與信息安全實驗室從事研究工作；2002年8月晉升副教授。