Special Issue in Communications of the CCISA — Call For Paper

「資訊安全通訊雜誌」係由中華民國資訊安全學會發行，並定期於每年一月、四月、七月及十月出版與資訊安全相關領域有關之研究論著，每一期將邀請一位 Guest Editor 針對當期主題進行規劃與邀稿，且為了讓更多的研究者、同好共同開創資訊安全領域研究的天地，將在每一期中刊載下一期 Guest Editor 之規劃主題與論文徵稿方向，供研究者共襄盛舉，以豐富資訊安全研究之園地。

2014 年度十月份主題為「新一代攻防平台與技術(The new generation of attack and defense platform and technologies)」。對於高階資安技術人才的培育，除了各類資安理論的研究外，亦包含對實務經驗的累積。透過建立攻防平台，如 CTF (Capture The Flag)競賽，除了可訓練高階資安攻防人員的實務能力，亦可評估人員團隊的能量。攻防平台不侷限於 CTF 競賽平台，其他像是攻擊偵測系統、網路流量分析系統、以及各類攻防系統與相關技術，都是近幾年持續發燒的議題。另外，軟硬體攻防技術日新月異，都是極佳的研究方向：如美國史諾登事件中的稜鏡計畫中，採用的許多監控技術，其原理以及該如何反制、每年遭爆出的軟體漏洞，背後細節與成因、香港公投 DDoS 事件中所牽涉之攻防技術、雲端平台之安全可靠性等等，皆可成為本期資訊安全通訊想要探討的議題，希望包含理論及各種系統實作或實務經驗的分享。歡迎更多研究者共同參與此主題。

以下僅列舉部分的相關主題，但徵稿論文不受此限

＊CTF 攻防平台設計與規則
＊網路流量分析
＊軟、硬體漏洞成因與防治方式
＊雲端平台安全問題
＊自動化攻擊與分析平台
＊DDoS 攻擊手法與防治方式
＊各類監聽技術與防治

投稿須知：

1. 對於論文主題有任何問題，請以 E-mail 聯絡 Guest Editor。
2. 論文請不要有智慧財產與一稿多投之爭議，刊登論文之文責由作者自負。
3. 本刊物只接受電子檔投稿，稿件需以Microsoft Word 編輯，字體為 12 點標楷體(中文)或times (英文)，總頁數在 20 頁以內，並請參閱資安通訊雜誌論文格式http://140.127.40.50/download/isc2.doc
4. 投稿稿件請將含作者服務單位、聯絡地址、電話、傳真、email 信箱等之基本資料及投稿論文(論文內請勿含基本資料)email 至 Guest Editor 及本期刊編輯部。

重要日期：

論文投稿截止：103 年 9 月 10 日

論文接受通知：103 年 9 月 20 日

期刊發行日期：103 年 10 月

Guest Editor 聯絡方式

姓名：李倫銓
單位：中華電信數據通信分公司
地址：台北市信義路一段 21 號
電子郵件：lclee@cht.com.tw

本期刊編輯部聯絡方式

主編：王智弘 (wangch@mail.ncyu.edu.tw)
助理編輯：宋孝謙 (ccisa.editor@gmail.com)
CCISA: http://www.ccisa.org.tw/