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 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。

2015年度四月份主題為「智慧終端裝置與應用程式之安全分析與檢測(Smart Devices and Application Security Analysis and Investigation)」。近年來，隨著智慧終端的普及，許多政府單位、企業或其他組織紛紛要推出針對智慧終端的應用，而為了要快速提供因應不同智慧終端平台的應用，會採用開放應用程式介面(API) 的方式，讓其他第三方的單位可以運用所開放的介面而開發應用程式。然而，如果應用程式開發者所開發出的應用程式具有弱點或是埋藏有惡意程式，則會造成使用者的損失，反而造成開放應用程式介面單位商譽的影響。有鑑於此，需要有相關的理論、方法與技術，能夠協助去讓開放應用程式介面的單位能夠去檢測使用其程式介面所開發出之應用程式的安全性，乃至於在應用程式上加上一個檢查通過的標籤，而方便使用者辨識，從而促進應用程式安全。或者讓使用者在下載應用程式之前，能夠對應用程式的安全性進行檢查，而能識別出惡意程式或是具有弱點的應用程式。

除此之外，當攜帶個人智慧終端上班 (BYOD) 的議題興起後，對於企業或組織來說，如何篩選個人可以在公務使用的手機，也成為待解決的困難。因此，目前許多國家的政府單位也紛紛開始訂定智慧終端的安全檢測標準與檢測方法。

綜以上所述，凡是對於智慧終端與應用程式的安全檢測、分析、驗證，乃至於讓使用者能夠快速評估智慧終端或應用程式安全風險的理論、架構、方法、工具等，皆可成為本期資訊安全通訊想要探討的議題。

以下僅列舉部分的相關主題，但徵稿論文不受此限：

＊智慧終端檢測標準與規範
＊智慧終端與應用程式安全標章
＊智慧終端檢測方法與工具
＊智慧終端應用程式弱點與對策
＊智慧終端應用程式分析與測試方法及工具
＊智慧終端之信賴運算架構

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：104 年 3 月 20 日

論文接受通知：104 年 3 月 30 日

期刊發行日期：104 年 4 月

Guest Editor 聯絡方式

姓名：查士朝
單位：國立臺灣科技大學資訊管理學系
地址：台北市基隆路 4 段 43 號
電子郵件：csc@cs.ntust.edu.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/