國立中山大學資訊工程學系
(07)5252-000 轉 4301, 4302, 4303
804 高雄市鼓山區蓮海路 70 號

每週演講心得分享 17

Weekly Seminar Memoir 17

徐瑞壕 教授

Prof. Ruei-Hau Hsu

107 年 11 月 30 日(星期五)14:10~15:40
Nov. 30, 2018 (Fri.) 14:10~15:40
電資大樓 EC1009 室
EC 1009, Building of EE & CS

發布日期： 107 年 12 月 02 日

演講資訊

講題 TOPIC

基於 5G 邊界計算的安全物聯網
Secure IoT and Proximity Communications based on Edge Computing

主講人 SPEAKER

徐瑞壕 教授/國立中山大學資訊工程學系
Prof. Ruei-Hau Hsu / Department of Computer Science and Engineering
National Sun Yat-sen University

摘要 ABSTRACT

物聯網為下一代的傳輸與計算技術的實現，使得廣泛的計算裝置能夠實現資訊的交換以及計算資源的分享，以支援各種資訊服務應用。然而物聯網標準以及應用的多樣性，使得其安全為一重大挑戰，因此本演講將介紹如何利用邊緣計算來實現物聯網的可重置安全以及安全近場通訊。

Internet-of-Things (IoT) is the practice of next-generation communications and computation technologies. It fulfills information and computing resource exchange among heterogeneous types of computing devices for various kinds of information services and applications. However, IoT security is extremely challenging due to the diverse types of standards and applications. Hence, this talk will introduce how to exploit edge computing to realize reconfigurable security and secure proximity communications in IoT.

心得分享

陳冠智

碩士班二年級，平行處理實驗室

本系徐瑞壕老師今日演講為我們帶來與網路安全相關的介紹，其中一個主題是關於近場通訊，比較常見的應用是智慧型手機的 NFC 功能，講的是提供裝置之間互動的環境(device to device)。互動模式可能為 1 對 1，甚至 1 對多，例如若想要交朋友，便會去搜尋許多人的長相、個性介紹、興趣等資訊，進一步挑選出自己認為合適的對象，不過裝置搜尋(身分識別)同時會存在隱私問題，有些人並不希望個人資訊公開或被搜尋到。徐老師便提到一個解決方案，可以透過中央管理機制去維護訊息的收發，也就是說，進行存取的控制，為檔案的存取建立一套制度(或一份名單)，針對不同身分的使用者，發送不同的金鑰，但是這種作法存在一個前提就是管理機制必須是能被信任的。

隨著網路日漸發展，物聯網(IoT)是近期較熱門的主題，最典型的例子是日常生活常見的監視器，人們總以為它們的存在目的在於防護治安，發生突發狀況即能捕捉關鍵證據，是相當安全的保障，卻不知它們本身就可能存在著漏洞。多數的電眼建置並沒有足夠的資安意識，像是只使用預設密碼就能登入管理端，造成這些監控畫面硬生生暴露，反而容易淪為犯罪的工具。

在這些情況下，如何做到安全的防護？對於即時系統(real-time system)而言，進行安全計算是一大難題，試想系統還在加密的過程，可能有突發狀況發生；物聯網的許多裝置都是透過遠端的存取，不容易受保護。

綜合以上實例都是我們可能正在遭遇或即將碰上的麻煩，如何兼具科技發展與資訊安全維護，更是你我都需要正視的問題。

朱可欣

碩士班一年級，平行處理實驗室

這次演講邀請到本系的徐瑞壕教授，為我們帶來基於 5G 的 IoT 安全議題。徐老師以淺顯易懂的方式介紹邊緣計算安全和 IoT 安全的重要性及如何維護。

他首先介紹基於 5G 的邊緣計算。與傳統計算需要移動設備連接到基站進行通信不同；新興的邊緣計算可以基於 5G 的裝置間（D2D）技術實現去中心化的通信，於是在 D2D 的過程中身分識別、信息洩露和通訊安全成了重要的議題。

徐老師還介紹了一種基於橢圓曲線的屬性加密方法，通過區域安全中心保管的生成鑰和公鑰實現基於屬性的加密協議。服務方（M-UE）向安全中心發起申請，基於服務屬性生成對應屬性的私鑰；用戶則使用從安全中心處取得的公鑰，發布對特定服務屬性的需求，安全中心在公鑰基礎上進行屬性加密，以保證僅持有該屬性私鑰的服務方可以看到內容。

徐老師接著還介紹現有 IoT 設備的危險性，以及 IoT 安全的重要性和面臨的挑戰，他也提到一種通過安全代理人來維護 IoT 設備間通訊安全的安全協議，IoT 設備間不使用易被竊聽和攻擊的直接認證，而是通過安全代理人來進行間接認證。該協議的另一個重點是基於加密來保證連安全代理人也無法直接得知裝置間的傳輸內容，並進一步保證 IoT 裝置的傳輸安全。

這場演講中徐老師介紹了兩項非常重要的 IoT 安全協議，雖然算法較複雜，但徐老師卻介紹的條理清晰，讓我們收穫頗深。

單　位：國立中山大學資訊工程學系
聯絡人：吳秀珍行政助理，分機 4301
　　黃莉萍行政助理，分機 4303
總　機：(07)5252000