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 10

Weekly Seminar Memoir 10

ARIJIT KARATI, Ph.D.

107 年 10 月 26 日(星期五)14:10~15:40
Oct. 26, 2018 (Fri.) 14:10~15:40
電資大樓 EC1009 室
EC 1009, Building of EE & CS

發布日期： 107 年 10 月 28 日

演講資訊

講題 TOPIC

Cryptography and Its Usage in Our Modern World

主講人 SPEAKER

ARIJIT KARATI, Ph.D. / Post Doctoral Research Fellow
Laboratory of Applied Cryptology
Department of Computer Science and Engineering
National Sun Yat-sen University

摘要 ABSTRACT

Nowadays, the communication and transaction ensue in a digital form, so, security threats and protections become the integral part of their successful design and implementation and it becomes more important when public/untrusted communication are involved. Cryptography is a branch of science that deals with the design of security techniques in diverse areas including data confidentiality, integrity, authenticity, availability etc. So, we discuss a cryptographic technique with its implementation point of view.

心得分享

劉雅典

碩士班一年級，生醫訊號暨影像處理實驗室

今天演講主題是在現代社會中密碼學和它的應用，講者是本系博士後研究員，來自印度的 Karati 博士。演講內容大致分為(1)在現今社會中資安的重要性 (2)密碼學的應用 (3)公鑰的基礎簡介 (4)進一步討論密碼學中的公鑰 (5)結論。

密碼學是提供資料安全及隱私的科學分支，其重要性質有 confidentiality, authentication, data integrity, non-reputation, availability, ... etc. 如果能適當維護這些性質，便可使得存放的資料更加安全。密碼學簡單來說，就是原本的明文透過加密演算法及加密金鑰後得到的密文，再由接收者以解密演算法及解密金鑰獲取傳送者的原始文件。

Karati 博士也提到密碼學還分為對稱式 (Symmetric) 及非對稱式 (Asymmetric)兩種。簡單來說，對稱式加密法是由相同的 key 加解密，而非對稱式則是由公鑰及私鑰兩把鑰匙進行加密解密。他還提到 Elliptic Curve(ECC)演算法，這是新一代的公開金鑰演算法，而且可以使用較短密鑰長度就可達到與較長金鑰 RSA 演算法相當的安全強度，非常適合在智慧卡等資源有限的環境下使用。

聽完今天演講後，我學到了許多平日不曾聯想到的資訊安全應用，也讓我知道原來資訊安全在 computer science 屬於非常重要的一環，在現今駭客橫行的時代，懂得保護好自己的資料是非常重要的，與自己息息相關的實例就是能避免即將要繳交的作業不翼而飛！

林佳臻

碩士班一年級，生醫訊號暨影像處理實驗室

今天的書報討論是有關資安領域的專題演講，主要為密碼學的應用，從加解密的基本原理講起，以及這些技術如何被應用在日常生活中。

在日常生活中絕大多數訊息傳遞都會使用到加解密技術，這項技術保障了訊息的隱密性，一般情況下即使傳遞過程中訊息被攔截，攔截者也不一定能得知原文內容。但隨著技術快速發展，加解密機制也有可能被破解。攻擊者分為兩種： passive attack 是在訊息傳送過程中監看資料以竊取個人資料；另一種 active attack 則是攔截訊息之後再竄改資料。因應各種網路攻擊的不同情況，加密技術也不斷地更新。講者還介紹了 IBE（Identity-based Encryption）技術，是近年來較常應用的方法，利用身分的指定，只有特定接收者能夠解出該密文，這種機制增加了安全性，但 IBE 同樣的也有缺點，像是在指定接收者的時候，如果加密時身分訊息輸入錯誤，也會造成無法順利解密。另外，講者也提到密碼學在 IoT 的相關應用，從網路訊息傳送到遠端門鎖的遙控，在在顯示密碼學的應用已與我們的日常生活息息相關。

今天的演講讓我更加了解資訊安全的重要性，以及其中許多複雜運算，在現今網路發達的時代，隱私權以及個資逐漸成為大家所關注的焦點，若是沒有安全機制好好保護資料，有可能被有心人士利用，因此，資訊安全已成為人類相當重要的研究議題。

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