資訊專題研討課程心得報告

講題:IC 卡系統設計與應用

演講人: 侯廷偉 教授 國立成功大學工程科學系

報告撰寫人: 林經緯 政治大學 資科所 一年級 g9232@cs.nccu.edu.tw

2003/09/30

1 前言

IC 卡具備運算機能、高安全性、記憶容量大和攜帶方便等特點。可以應用的領域舉凡醫療、金融、交通，幾乎生活的各個層面都用的，似乎輕薄短小的特性已成爲每個人生活的必需品了。

2 演講要點整理

2.1 IC基本技術介紹

IC 卡主要由符合 ISO 標準之塑膠卡片 (如 PVC、ABS) 和一個由微處理器或記憶體與控制邏輯所組合而成的晶片 (IC CHIP)。以及一個可提供與外界通訊的介面所共同構成。

IC卡的種類, 可依其結構劃分。第一種是不包含微電腦 (CPU) 的記憶卡 (Memory Card), 是由單純的邏輯電路與記憶體組成, 如預付卡和識別證等; 第二種則是包含微電腦的智慧卡 (Smart Card), 是由微電腦與記憶體組成, 如金融卡、信用卡和健保卡等。兩者的選擇考量因素在於成本與安全性。此外, 依照卡片的輸出入介面分爲接觸卡 (Contact Card) 、非接觸卡 (Contactless Card) 。

由於健保卡用的是 Smart card 的技術，因此以下我們針對 Smart 卡 做個簡單的介紹。

主要的 Smart 卡上的晶片架構, 包含 Processor(RISC)、Co-Processor、MMU、ISO7816、ISO14443等部分。ISO 7816的規格, 主要使用在接觸式的 IC 卡上;ISO 14443使用在非接觸式的卡上。在接觸式的 smart 卡內,Processor 和 Co-processor 主要用在特殊的運算;ISO 7816主要是

資料輸入輸出與電源相關的機制;MMU 則是做記憶體控管, 除了讓 CPU 可以有效利用記憶體的功能, 也可以對記憶體以特殊的方式來做到安全保護, 以避免被人以反向工程, 讀出系統運作時, 所產生的機密資料。非接觸式的 Smart 卡, 除了資料輸出入和電源相關的機制採用 ISO 14443外, 基本元件大致上都相同於接觸式 smart 卡。目前來說, 有安全需求的應用, 使用接觸式的 Smart 卡比較好。

Smart 卡常見的通訊協定爲 T=0 、T=1與 T=14。T=0的通訊協定是 Byte-oriented;T=1則是 packet-oriented;T=14的通訊協定類似 T=1, 對於傳送的資料可以做加密。T=1就是我們現在健保 IC 卡採用的規格。

2.2 IC卡安全性探討

Smart 卡製作的過程中, 必須通過重重的認證機制, 並且在通過認證的工廠或公司生產, 對於 Smart 卡內部的資訊必須完全保密。

由於 Smart 卡非常注重資料的安全, 因此各個環節都會在資料上作加密, 讓資料只有在晶片上處理, 或在特定的設備上運作。後端軟體平台在傳輸資料也必須注重加密的機制。

Smart卡本身提供資料的加密及解密的運算功能 , 透過 CRC、RNG、UART 和 Timer 的設定使用, 避免外部有意圖的試探和解密。對於其核心 CPU 和保存資料的保密 , 以及加解密運算是在智慧卡內一併完成 , 使得過程猶如黑箱作業一般 , 大大增加了卡片的安全性。

關於卡片內部安全技術的部份, 目前皆由國外的核心製造商所掌控。

爲了避免僞讀卡機假借健保局名義讀取機密資料 , 須具有健保局發行的讀卡機安全模組卡 (SAM)才能讀取晶片內資料, 這些模組就放了健保局的 key, 加上卡片裡頭也存有相對應的 key , 構成了嚴謹授權及相互認証機制。

具有醫師卡始能讀取醫療資料, 一般護理人員沒有權利查看病患隱私性資料。

IC卡設有密碼保護功能 (Pin code), 以個人密碼優於醫師卡之讀寫授權, 民衆可選擇是否輸入密碼解密, 一旦設定密碼, 一般人或掛號人員即使有讀卡機及安全模組, 亦無法讀取基本資料段以外之欄位資料, 必須民衆同意輸入密碼, 醫護人員始能開啓資料。

採用 VPN 封閉性專屬網路, 不與網際網路連結, 駭客無從由外部入侵。同時, 以 VPN 爲骨幹網路, 電信公司均可互相備援, 而網路頻寬隨使用量自動調整, 以確保網路傳輸品質, 有效減低網路塞車機率。

3 評論與心得

先前爲了簡化行政程序、控管醫療成本、加快理賠程序等原因, 健保局規劃發行健保 IC 卡要連同身分證資料、健保資料、醫療資料及衛生行政資料一同建入, 但最後因引發人權團體對隱私安全性的抗議而作罷，後來移至第三階段進行。

我深深感覺到，人的改變並不像程式一樣，改個 code 或是換個模組就可以變得更好，仍舊需要時間來適應。

前不久財金公司客戶資料外洩，還有信用卡公司，網路銀行資料外洩的問題，信用卡倒刷等問題，技術上的問題好像都防了很多事情發生，最後出了安全上的問題你會發覺都是人的問題。科技的技術不斷地在進步，相關的社會教育、法律懲治、管理制度如果無法適時跟上技術的脚步，最後只會導致社會的失序。

我覺得這是在凡事追求高科技化，技術導向的社會應該好好停下來深思的問題。

相關參考資料

[1] 電子健保卡 各國比一比 http://www.isecutech.com.tw/it$_F eature_C ontent.asp?Serial_n o =$ $839iSA : ¨mr\Upsilon|hm7¨http : //www.isecutech.com.tw/enews.asp$

[2] 健保　　卡惹風波 東元被疑洩密 http://forums.chinatimes.com/report/new0101/iccard5.htm

[3] 理性看待健保IC 卡的防疫光環 http://iwebs.url.com.tw/main/html/lipo1/781.shtml

[4] 健保IC 卡與病患隱私權益 http://www.dryahoo.org.tw/index.htm

[5] 中央健保局 IC 健保卡網站 http://www.nhi.gov.tw/IC$_C ard/news/news.asp$