Seminar1 — IC 卡系統設計與應用

by 侯廷偉 教授 國立成功大學工程科學系

2003.10.28

報告撰寫者：政大資科所碩一 謝淳達 92753008

1 演講主題及摘要

介紹IC 卡的一些相關背景知識, 並且跟我們分享了教授在研究開發 IC 卡系統時的一些心得, 可說是非常寶貴的經驗。

2 要點整理

IC卡是一個蠻分工的行業, 而且要求蠻高的一個晶片。他有加上很多要防止人家破壞的動作, 要保護他。還有上面的軟體都要去經過認證, 代價很大的。

卡片的材質也是要要求的, 要牽扯到價值, 牽涉到這個環保。這張卡片做完之後呢, 要配對一個讀卡機, 我們叫 reader。reader 呢, 再配對你的應用程式。術語呢, 叫做 card interminal, 可以想成是一台 pc, 那接下來就是上 internet。那 internet 裡含著看各位要不要有 public key interstructure 那也就是保密的系統。

此外, 卡片還必須做到不會被別人破壞的要求, 像現在的健保 ic 卡, 一旦稍微被破壞, 就會出現粉紅色, 讓人一看就知道這張卡被破壞過了。

後台系統。一個 IC 卡的管理系統。去管一個這麼大的卡片的資料庫, 實際上是一個蠻困難的一件事情。

ic卡內可以內嵌 core processor, 使得卡片本身就可以自己做一些運算, 很適合用於金融類或信用類的應用, 但是相對價格也比較貴。內嵌 processor 可以使得資料在卡

片內部運算, 而不用透過其他機器, 降低資料外流的可能性。雖然內嵌的 core processor 時脈相當低, 只有5mhz, 但是對於現今的應用已經相當足夠。
我們現在用的悠遊卡介面的卡, 這種叫非接觸式介面卡。
卡片中有個元件叫做 mmu, 這是爲了避免卡片的內容被竊取。爲了避免資料外流, 卡片中的資料都是有加密過的, 而且每張卡片都有一個用來加解密的 key, 所以如果這個用來加解密的 key 一旦被找到, 那就等於資料外流了, 因此我們需要有個好的機制來隱藏這把 key 的位置, 而 mmu 可以幫我們把這把 key 隱藏起來, 不被他人所盜取。
ic卡有分接觸式以及非接觸式。接觸式的卡片包括金融卡, 信用卡等等需要較高安全等級的應用。而非接觸式卡片近年來由於它的便利性, 也越來越受歡迎, 適合用在需要快速讀取卡片的環境, 現在的悠遊卡就是屬於非接觸式卡片。
不過非接觸式卡片有個問題, 假設同時兩張以上的悠遊卡經過讀卡機的話很容易會有碰撞 (collision) 的問題, 就好像在作業系統或網路上會遇到的問題一樣,
爲了保護卡片本體, 卡片還會有些實體的防護措施, 例如防止晶片被打開, 或被強光照射而使資料遺失, 此外, 卡片上面還有 intuition sensor 的機制, 當卡片本身發覺到自己正被攻擊的時候, 就會啓動自毀裝置, 避免資料外流。另外還可以做的研究是可以在卡片上面增加指紋辨識的功能, 只有在卡片所有者接觸到卡片時卡片才生效。

3 評論

由於IC 卡與天俱來的安全、方便、容量大、有計算能力等優點, 使得各國在近年來紛紛想推動 IC 卡, 台灣也不例外, 尤其是在前一陣子發生連續金融盜領案之後, 更是加速了 IC 卡在台灣的推動。這一陣子台灣更是試圖推行全民健保 IC 卡, 看來 IC 卡的普及應該是勢在必行的。
不過 IC 卡除了目前大家比較熟悉的用途, 也就是金融交易、身分識別以外, 其實還有一個更重要的用途, 也就是電子錢包。我個人一直很希望有一天電子錢包這種東西能夠普及, 因爲電子錢包一旦普及, 有很多以往無法透過網路直接交易的一些商業行爲都可以獲得解決。

舉個例子, 現在很多人都透過網路來做一些產品的行銷, 包括個人所製作的產品 (軟體、音樂等)、拍賣等, 雖然這些行爲不是什麼新的商業行爲, 但是目前這些交易都無法把所有事情放在網路上進行,「錢」還是必須透過其他管道, 例如轉帳, 現金交易等等的方式, 才能完成一筆交易。這對於這些透過網路來進行交易的人來講是一大致命傷, 因爲他們必須花費而外的人力金錢只爲了「收費」這個動作, 此外, 對於消費者而言, 由於「收費」的手續比較麻煩 (這點對於跨國購物更是顯而易見) , 所以會降低大家的購買慾望。

例如以前有一些軟體的作者 (ex:cview), 他們自己寫了一個軟體想要賣, 但是由於是個人, 無法像一般公司那樣在一般商場鋪貨, 或是無法請人專門處理收費問題, 而使得即使有人想買, 也會因爲付費手續繁複, 而打退堂鼓。又例如我今天看到國外有人在賣一個很好的軟體或音樂, 我想跟他買, 但是卻因爲賣方不是本國人, 只能夠過特定的信用卡付費的方式付款, 當我看到付費這麼麻煩時, 即使是再好的東西我都會不想買。不過一旦電子錢包普及之後, 許多這方面的問題都將迎刃而解。

不過現在大家對電子商務最擔心的應該還是他的安全性問題。因此, 爲了提高 IC 卡在電子商務的應用, 資料的安全性是首要之務, 唯有資料在傳輸中完全的保密安全, 大家的接受度才會高。然而, 雖然目前政府有推動電子錢包, 但是申請手續以及操作手續過於繁複, 也是造成普及率不高的主因之一。因此, 要如何又方便又安全的讓民衆來使用也是很重要的課題。

另外, 爲了避免 IC 卡被盜用, 目前也有人推出具有指紋辨識功能的 IC 卡, 除此之外, 或許也可以嘗試將 IC 晶片植入人體, 就像之前流行在寵物上植入的辨識晶片一樣, 當然會不會有人願意在自己的皮膚上植入晶片又是另外一個議題了。