射頻識別（RFID）的保安

2008 年 2 月

目錄

摘要

射頻識別（RFID）技術的部署和使用正快速地在許多不同的行業中成長，開發者除了將此技術用在如資產或存貨追蹤的傳統應用系統之外，還應用於保安服務，如電子護照以及內置 RFID 功能的信用卡。然而 RFID 技術也引起了一些關於私隱權、保安與法律的執行[1]等令人關注的議題。

本文介紹 RFID 技術基本的概念及相關的保安與威脅之問題，並討論克服這些問題可行的措施。從而對此技術保安方面作進一步的了解。

[1] http://www.eecs.harvard.edu/cs199r/bd-rfid/lawEnforcement.pdf

I. 介紹

射頻識別（RFID）技術簡介

射頻識別（RFID）技術是一個非接觸式、自動辨識的技術。使用射頻訊號去辨識、追蹤、分類和偵測多種類的物件，包括人員、車輛、貨品和資產，而不需要直接接觸（如磁條技術）或視線範圍內接觸（如條碼技術）。RFID 技術可透過內建射頻掃描技術的網絡裝置在幾公尺外的距離追蹤物件的移動。

一種稱為 RFID 標籤（或簡稱標籤）的裝置是此技術的關鍵組件。RFID 標籤通常至少有兩個組件：

1. 調制（modulating）與解調（demodulating）射頻訊號並執行其它功能的集成電路
2. 接收跟傳送訊號的天線

RFID 標籤可以執行有限的運算並擁有少量的儲存空間。RFID 標籤有時候被認為是一種加強版的「電子條碼」[2]。

不包含集成電路的 RFID 標籤稱為無晶片（chipless）的 RFID 標籤（也稱 RF fibres）。這些標籤使用「*fibres or materials that reflect a portion of the reader's signal back and the unique return signal can be used as an identifier*」[3]，即可以把部份閱讀器訊號反射回去的材料，此獨特的反射訊號可被用來作為識別。

[2] http://www.eurosmart.com/Update/07-10/Eurosmart_White_paper_on_RFID_Oct07.pdf

[3] http://www.technovelgy.com/ct/Technology-Article.asp?ArtNum=28

RFID 是如何運作?

使用 RFID 技術的系統通常包含以下三個主要組件：

1. RFID 標籤或轉發器（transponder），載有物體識別數據。
2. RFID 標籤閱讀器或收發器，可讀寫標籤數據。
3. 後端數據庫，儲存和標籤內容相關的記錄。

每一個標籤包含獨一無二的識別碼。RFID 閱讀器發射低階射頻磁場把能量提供給標籤，標籤回應閱讀器的查詢並經由射頻波表示其所在位置，傳送獨一無二的識別數據。數據被閱讀器解碼並透過中介軟件將其傳送到區域應用系統。中介軟件是一個介於閱讀器和 RFID 應用系統之間的界面。系統在這之後會以儲存在主數據庫或後端系統中的資訊搜尋及比對識別碼，透過這樣的方式，根據閱讀器接收及處理來自數據庫的結果，可以給予或拒絕進一步的接達或授權。

II. RFID 的採用

目前在供應鏈管理、自動付款系統與空運包裹管理等行業中可以發現到 RFID 的商業應用系統，根據 RFIDupdate.com 數據顯示，沃爾瑪（Wal-Mart）與美國國防部（DOD）要求其供應商採用 RFID 技術[4]，成為 RFID 技術行業的催化劑之一。雖然這個市場並未如預期般快速或大規模地成長，這兩大集團的規定仍然是發展此一行業的重要先驅。

商業趨勢

2003 年 6 月，全球最大的零售商 Wal-Mart 要求其前一百大供應商在 2005 年前[5]「*put RFID tags on all cases and pallets of consumer goods shipped to a limited number of Wal-Mart distribution centers and stores*」，Wal-Mart 把射頻識別標籤放入貨品及貨箱中，透過船運到達一些集散中心或分店。當部署 RFID 計劃持續進行時，Wal-Mart 表示在 2006 年「*out-of-stock items carrying RFID tags could be replenished three times faster than they were before the project began*」[6]，即內建射頻識別標籤的缺貨貨品，在補貨速度上是未進行此計劃前的三倍。

然而，並非所有公司都覺得 RFID 技術是有利的。一些較小型的 Wal-Mart 供應商無法認同為符合 Wal-Mart 的要求而投放在供應鏈[7]上 RFID 的投資是值得的。

政府採用情況

如同 Wal-Mart 的做法，美國 DOD 在 2004 年 7 月開始的政策，要求供應商直接或間接供應貨品時，要把 RFID 技術整合到貨運的過程中[8]，此一要求觸發了一些 DOD 供應商去測試 RFID，或執行先導計劃以符合此一新的要求。

電子護照計劃是另外一個採用 RFID 技術的政府項目。在一些國家，傳統的紙本護照逐

---

4 http://www.rfidupdate.com/articles/index.php?id=1264

5 http://www.symbol.com/assets/files/Supplier_Compliance_with_the_DOD_RFID_Mandate.pdf

6 http://www.computerworld.com/mobiletopics/mobile/story/0,10801,109418,00.html

7 http://www.rfidgazette.org/walmart/index.html

8 http://www.symbol.com/assets/files/Supplier_Compliance_with_the_DOD_RFID_Mandate.pdf

漸被內建小型集成電路的護照取代，生物識別資料，如臉部特徵識別、指紋或虹膜掃描儲存在電子護照中。電子護照計劃起始於美國，要求所有參予免簽證計劃（Visa Waiver Program，VWP）的國家發行內含晶片的護照，主要目的是提供自動識別確認及更廣泛的邊境保衛與保安[9]。

[9] http://travel.state.gov/passport/eppt/eppt_2788.html

III. 安全與私隱權的論點

在採用 RFID 技術時，機構與個人都需注意不同的安全與私隱權的風險。

標籤數據

RFID 標籤被認為是很「愚笨」的裝置。不論誰傳送要求訊號，RFID 標籤只能接收與回應。這將造成標籤數據未經授權被接達與被修改的風險。換句話說，未經保護的標籤會有弱點如遭到竊聽、流量分析，仿冒或拒絕服務攻擊，以下將依序說明。

竊聽（或側錄）

從標籤和閱讀器傳送出來的射頻訊號，可以在數公尺以外被其它射頻接收器偵測到。因此可能會有未經授權的使用者接達 RFID 標籤中內含的數據。如果合法傳輸沒有做適當的保護，任何擁有 RFID 閱讀器的人，在未經適當的接達控制下也可查詢標籤並竊取標籤的內容。

美國的研究者展示了對 RFID 信用卡的側錄攻擊，透過此方式竊取未經適當加密的信用卡資料[10]，如持卡人姓名與帳戶等資料。

流量分析

即使標籤數據受到保護，也可能被使用流量分析的工具持續追蹤標籤的反應時間 ，分析相關數據從而建立一個關於活動情形、社交與財務交易的畫面。濫用流量分析將會對私隱權有直接的衝擊。

仿冒

根據竊聽與流量分析所收集到的數據，製造一個仿冒標籤是有可能的。舉例而言，一個

[10] http://www.nytimes.com/2006/10/23/business/23card.html?pagewanted=1&_r=1

在筆記薄型電腦或個人數碼助理上執行，名為 RFDump[11] 的軟件，若未經適當保護，將允許使用者在標準的智能標籤上執行讀或寫的工作。此軟件讓入侵者以假數據覆寫現存於 RFID 標籤的數據。透過仿冒合法標籤，入侵者可以欺騙 RFID 系統並改變標籤身份，以取得未經授權或不會被偵測到的好處，例如購買昂貴產品而欺騙其 RFID 價格顯示較便宜的價格來節省費用。

透過仿冒與竊聽兩項能力的結合，攻擊者可以「*query a tag, receive the information it sends, and retransmit this information at a later time*」[12]，即以查詢標籤接收其所傳送的資訊，並稍後重新傳輸資訊，這樣便可能進行中繼攻擊。

拒絕服務攻擊

當大量內部 RFID 數據在企業伙伴間分享時，環繞安全與信任的問題便大幅增加。若大量標籤被破壞時，RFID 基礎架構上便可能發生拒絕服務攻擊 。例如攻擊者若獲得接達標籤的密碼，可在 RFID 標籤上使用“kill”指令使標籤永久無效。此外攻擊者可使用非法的高能量射頻（RF）傳送器，阻塞 RFID 系統使用的頻率，造成整個系統停頓[13]。

RFID 閱讀器的完整性

就某些例子而言，RFID 閱讀器安裝的地點並沒有適當的實體保護。未經授權的入侵者可放置隱敝的閱讀器以獲取閱讀器傳送的資訊，或是破壞閱讀器以影響其完整性。未經授權的閱讀器也可接達沒有適當接達控制的標籤，從而危害到私隱權。

因此閱讀器所收集並傳送到 RFID 應用程式的資訊，可能受到未經授權者的竄改或竊取。RFID 閱讀器也可成為電腦病毒的目標，2006 年研究者展示 RFID 的電腦病毒是有可能的。屬於概念驗證而又自我複製的 RFID 電腦病毒，展示電腦病毒是可以使用 RFID 標籤，經由 SQL 植入式攻擊[14]而危害到後端的 RFID 中介軟件系統。

---

[11] http://freshmeat.net/projects/rfdump/?branch_id=61265&release_id=264928

[12] http://blogs.sun.com/ks/entry/rfid_technology_security_concerns

[13] http://www.eurosmart.com/Update/07-10/Eurosmart_White_paper_on_RFID_Oct07.pdf

[14] http://www.rfidvirus.org/

個人私隱

正當 RFID 逐漸應用於零售業與製造業時，附有 RFID 標籤的產品如衣服、電子產品等引起大眾對於個人私隱的關注。無論是否經過直接銷售的方式、或是否能透過晶片追蹤，人們關心的是其個人數據如何被利用。倘若個人身份連結至單一的 RFID 標籤上，他便會在未被通知及同意的情況下被追蹤。

例如，可清洗的衣物所放置的 RFID 標籤並不會被移除，這些晶片是經過特別設計，可以承受長年清洗與使用的磨損；因此只要有人購買這類衣物，他便可被識別、編號並持續追蹤，即使離開商店後仍能被追蹤得到。只要距離夠近，RFID 閱讀器是可以偵測到這些 RFID 標籤的位置的。

IV. RFID 的保安趨勢

RFID 成為新興科技以來，發展可保護儲存在 RFID 晶片數據的業界標準，仍持續開發與加強。發展與改善具有加密功能、對稱式加密、信息授權碼和隨機號碼產生器的硬件，將會增進 RFID 的安全性。此外，RFID 電路設計與製造技術的發展，也能降低發展時的成本，釋出標籤上更多的資源作其它功用，如分配電力消耗至保安功能。

如今，透過研究某些公開密碼匙技術，RFID 供應商也將其應用在某些個案中。這能協助改良機密性、使用者認證和 RFID 標籤及其相關應用的私隱。RFID 供應商也主導著關於 RFID 閱讀器之基礎建設、完整性與機密性議題的研究。現在，數據可透過使用動態的重發行密碼匙儲存在權標裡，特定的閱讀器能夠覆寫權標的憑證或簽名，而且可以查證權標的身份。然而，關於將公開密碼匙技術應用在 RFID 上所需費用與成效爭議，已影響它使用於關鍵性的保安應用系統上。

V. 處理安全與私隱問題的方法

處理 RFID 的安全與私隱問題之方法有很多，可以分成下面幾大類：

1. 標籤數據保護
2. 閱讀器完整性
3. 個人私隱

標籤數據保護的方法

標籤記憶的密碼保護

密碼可以作為保護標籤數據之用，防止標籤未經用户允許下被讀取。但如果所有標籤的密碼都相同，這些數據事實上等同於公開。然而，如果每一個標籤有不一樣或獨一無二的密碼，那麼就必須記錄上數百萬的密碼，意味著閱讀器必須查詢數據庫，並對每一項讀取動作執行大量比對。

標籤記憶的實體性封鎖

在標籤放置到一個公開環境前，標籤製造商會封鎖一些如標籤上單一的識別數據等資訊。換句話說，晶片是唯讀的，而且在製造過程中植入了數據，這提供了來源證明。

此方法的限制為標籤晶片無法再寫入數據。儲存修正或多出的數據需要額外的記憶體，且需要用算法幫助尋找最新的標籤數據，這會導致更高的記憶成本和更多的記憶空間。

標籤記憶裡始創者的認證

標籤的擁有人或始創者，以私人密碼匙將標籤數據加密（即數碼簽署標籤），並將加密數據、擁有人的名字、及沒有加密的公開密碼匙與算法寫入標籤記憶中。當閱讀器想查證資訊的真實性時，會從標籤上取出擁有人的姓名與其它未加密的數據，來確認此數據是由所宣稱的始創者寫入。然而若 RFID 閱讀器需要更新標籤上的數據，便需要密碼匙管理系統來管理私人密碼匙。

RFID 閱讀器完整性的解決方案

閱讀器保護

閱讀器可以拒絕標籤的異常現象，並對不符合標籤內容的實體特性如時間或訊號強度作出反應。使用被動式標籤是一種可預防仿冒的方法。

閱讀器也能使用隨機頻率，要求標籤遵照閱讀器的頻率。閱讀器能隨機改變頻率，使非經過授權的使用者不易在傳送中偵測與竊取數據。

最重要的是，在閱讀器與 RFID 應用伺服器之間傳送的數據，可要求驗證閱讀器的身份。認證機制可在閱讀器與後端應用程式之間執行，以確保數據是傳送至合法的處理器那裏。

偵測讀取的偵測器

RFID 的環境能配備特殊的裝置，以偵測未經授權的讀取意圖或標籤上頻率的傳送。如果將這些偵測讀取的偵測器加上特殊設計的標籤一起使用，這些標籤能透過保留的頻率傳送訊號，指出任何刪除或修改標籤的意圖，它們也許可用來偵測對標籤未授權的讀取或更新嘗試。

個人私隱的解決方案

刪除標籤

藉著在標籤產品上執行特殊的 “kill” 指令，會刪除 RFID 標籤並使其無法再啟動。此 “kill”指令能切斷天線或造成短路，確保此標籤不會再進一步被偵測，以保障產品擁有者的個人私隱。

但是，在某些情況下，標籤是不應被刪除的。例如某商店希望在顧客退回貨品後，能重新偵測到它的標籤；另外，內含 RFID 晶片作為接達控制的智能卡也需要被持續啟動。

法拉第籠 （**Faraday Cage**）

RFID 標籤可由一片金屬質的網或薄片作為外層保護，名為「法拉第籠」。這層薄片做成的容器能阻絕固定頻率的射頻訊號，使保護標籤產品不被偵測。然而，這方法也許不適

用在某些狀況，例如：用在寵物與衣物上的標籤，便很難用這層薄片包覆。

主動干擾 （Active Jamming）

對射頻訊號主動干擾，是指利用一種裝置廣播射頻訊號，達到阻斷任何附近 RFID 閱讀器的運作；這項實體性的覆蓋方法會阻斷附近的 RFID 系統。

然而利用這種裝置可能是違法的，其取決於裝置本身電波的強度，和政府的規範。萬一干擾電波太強，附近的 RFID 系統都會有被高度阻絕的風險。

RSA 選擇性阻塞器標籤 （Blocker Tag）

阻塞器標籤（Blocker Tag）是一項被動的 RFID 裝置，利用複雜的算法同時模擬許多普通的 RFID 標籤。它透過使用兩組天線同時反射二個數元，提供一系列不斷的回應給 RFID 閱讀器，如此一來能防止其它標籤受到讀取，作為一種被動干擾。

但這種方法給予個人很大的控制。此外阻塞器標籤會被惡意利用，藉此模擬多重的標籤識別，以避開 RFID 閱讀器的規則。

邏輯性的雜湊函數鎖 （Hash Lock）

當某標籤被鎖定時，此標籤接受到一個值（或 meta 識別碼），此值為回應碼或 PIN 的雜湊值。標籤會拒絕顯示其識別碼，直至輸入回應碼的值或 PIN 後解鎖。例如標籤在超市結帳時會鎖定，返家後利用 meta 識別碼和 PIN 解鎖。一般人可看得到這些 meta 識別碼和 PIN 解鎖，它們會被印在產品包裝內，或是購物時拿到的收據而非經由射頻訊號傳送。

此項方法的限制，在於個人需要管理鎖定/解鎖的特性，以及購買時標籤及 PIN 之處理，這需要知道某個 RFID 標籤是屬於哪個產品的。在標籤加密動作的過程中，此項方法也會導致額外的成本開銷。

VI. 結論

RFID 技術正被廣泛利用在各種不同行業時，需要小心地處理相關的安全性和私隱的議題。因為市場上有不同形式的 RFID 標籤，並沒有整體的和一般的 RFID 保安解決方案。有一些低成本、被動及基本的標籤，無法執行標準的密碼操作，如加密、嚴格的虛擬隨機號碼產生和雜湊。有一些標籤成本比基本的 RFID 標籤成本較高，能夠執行對稱式密碼匙加密的操作。因此希望利用 RFID 技術的機構需要同時評估成本、牽涉的保安考慮，及不同 RFID 技術與其解決方案的限制。