具隱私權保護的 RFID 安全機制

RFID Security Mechanism with Privacy Protection

李俊叡
亞洲大學
資訊工程學系
mathew177@gmail.com

林詠章
亞洲大學
電腦與通訊學系
中興大學
資訊管理學系
iclin@nchu.edu.tw

曹世昌
亞洲大學
資訊工程學系
sctsaur@asia.edu.tw

摘要

隨著 RFID 技術的成熟及製造成本不斷降低，該技術已經被廣泛應用於許多領域如供應鏈管理，門禁系統、智慧家電、電子付費及生產自動化等。但是 RFID 技術帶來巨大商業價值和使用簡便的同時，也威脅到個人和組織的隱私與安全性。本論文介紹了 RFID 隱私與安全的基本問題，並探討目前一些有效解決 RFID 隱私與安全性問題的關鍵技術，針對學者 Ayoade 所提出來的 APF(Authentication Processing Framework)架構，提出一個具隱私權保護的 RFID 安全機制。

關鍵詞：RFID、MAC、APF、安全

1.緒論

1.1 RFID 基本架構

RFID的原理是利用發射無線電波訊號來傳送資料，使用無線的方式來做資料辨識與存取，如此即可達到物品內容識別的功能，基本組成元件如圖1所示[2]。

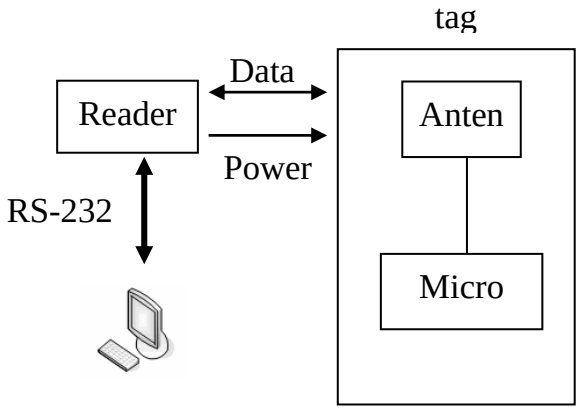

圖1 RFID基本架構

(1)Reader的組成模組

Reader用以接收主電腦的命令，可讀寫（Read / Write）Tag內的資料，其中大部分包含無線電模式（包括傳送器與接收器）、射頻模組、控制模組晶片及電源供應器；Reader的組成模組，Reader的組成模組如圖2[2]。

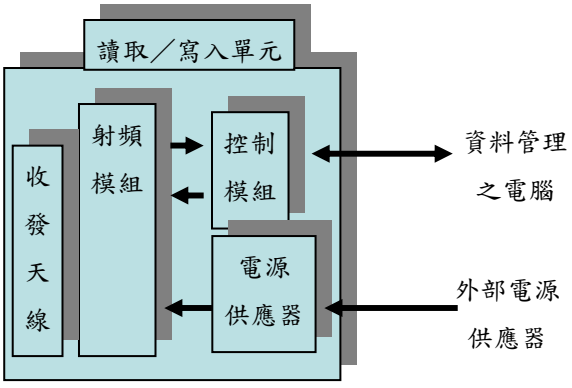

圖2 Reader的組成模組

(2) Tag功能

Tag通常放置在需要被識別的物體上，當Tag進入Reader所發射之RF電磁場範圍，Tag天線會感應此電磁能，經電容器充電至所需電源，再以內建之RF無線電波傳回Tag晶片內之資料；但此一數位信號必須不同，以免干擾。Tag的架構圖如圖3[2]。

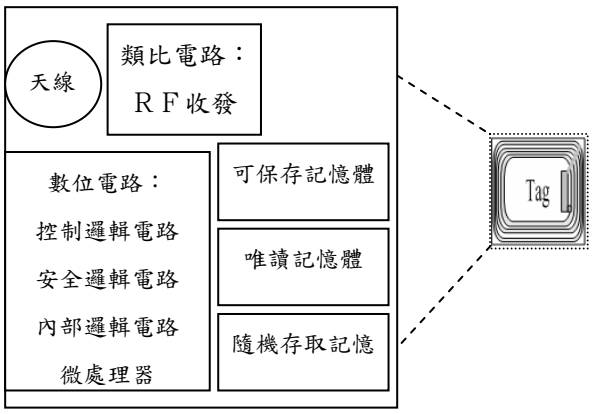

圖3 Tag功能

1.2 隱私與安全

近些年來，一些商業巨頭企業(如Wal-mart)看到RFID的應用優勢，開始推進RFID技術的廣泛使用。在這種形式下，各國政府也紛紛認識到RFID的實際利用價值和巨大商業前景，開始推動RFID在各領域的應用。例如，美國總務管理局鼓勵政府部門使用RFID技術，美國國防部規定所有軍需物資都要使用RFID技術。日本和韓國政府部門也通過各種措施大力推動電子標籤的應用[1]。

儘管目前RFID技術發展趨勢強勁，但和其他自動識別技術一樣，RFID在實際應用中還存在著許多涉及隱私與安全的關鍵問題尚待解決，茲說明如下:

(1)非法跟蹤

罪犯可以遠端識別受害者身上的標籤，掌握受害者的位置資訊，從而給犯罪活動提供更加便利的目標及相關條件[1]。

(2)竊取個人資訊和物品資訊

非法情報人員可以從標籤中讀出唯一的電子編碼，從而獲得使用者的相關個人資訊。搶劫貨車的不法分子可以用閱讀器確定哪些貨車更值得他們下手[1]。

(3)擾亂**RFID** 系統運行

缺乏安全措施的電子標籤十分脆弱，通過一些簡單的技術手段，任何人都可以隨意改變甚至破壞RFID標籤上的有用資訊，從而擾亂RFID系統的正常運行[1]。

(4)偽造**RFID**

隨著時代的不斷發展，RFID製造技術可能會被犯罪分子掌握。偽造的RFID會嚴重影響RFID在零售業和自動付費等領域的應用[1]。

從上述四個實例可以看出，不解決RFID的隱私與安全問題，RFID技術就很難得到更加廣泛的應用與推廣，也將影響RFID系統的可靠性。因此，隱私與安全已經成為制約RFID技術進一步發展的重要因素。

1.3訊息鑑別碼

MAC(Message Authentication Code)訊息鑑別碼，可以用來驗證文件訊息是否為約定好通訊的雙方所傳送，並且驗證文件訊息在傳遞的過程中是否遭到篡改，是一個非常實用的機制。本論文所提出的技術，便是利用訊息驗證碼所滿足所須的安全機制[3]。

2. 相關文獻

隨著RFID隱私與安全問題的日益凸現，國內外的研究人員都在積極尋求各種可能的解決方案。下面介紹一些核心技術與對策。

2.1 Kill command idea

Auto-ID中心提出的RFID標準設計模式中包含有“kill”命令。如果執行“kill”命令後，則標籤的所有功能都將被永久關閉並無法

被再次啟動。消費者可以在購買產品後執行這個“kill”命令使標籤實效，從而消除了消費者在隱私方面的顧慮。但是，這種方法限制了RFID標籤的進一步應用，例如產品的售後服務，廢品的回收等等[7]。

2.2 Faraday cage

利用電磁遮罩原理，把RFID標籤置於由金屬網或金屬薄片製成的容器中，Reader發送的信號將被遮罩，讓Reader無法讀取Tag資訊，Tag也無法向Reader發送資訊。顧客可以將自己的私人物品放在有這種遮罩功能的手提袋中，防止非法閱讀器的侵犯。但是，在很多應用領域中，這種安全措施是不可行的。例如，衣服上的RFID 標籤無法用金屬網遮罩[8]。

2.3 Active jamming

對射頻信號進行干擾是另一種保護RFID標籤被非法閱讀的物理手段。能主動發出無線電干擾信號的設備可以使附近射頻識別系統的閱讀器也無法正常工作，從而達到保護隱私的目的。但是這種方法在大多數情況下是違法的，它會給不要求隱私保護的合法系統帶來嚴重的破壞，也有可能影響其他無線通信[5]。

2.4. Blocker Tag

RSA安全公司提出的Blocker Tag是一種特殊的電子標籤。當一個Reader詢問某一個Tag時，即使所詢問的物品並不存在，阻塞器標籤也將返回物品存在的資訊。這樣就防止RFID閱讀器讀取顧客的隱私資訊。另外，通過設置Tag的區域, Blocker Tag可以有選擇性的阻塞那些被設定為隱私狀態的Tag，從而不影響那些被設定為公共狀態的Tag的正常工作。例如，商品在未被購買之前，Tag設定為公共狀態，商家的閱讀器可以讀取Tag資訊；而商品一經出售，Tag就被設定為隱私狀態，Blocker Tag保證顧客的物品資訊不能被任何閱讀器再讀取。這項技術的缺點在於，顧客必須持有Blocker Tag才能保證隱私不被侵犯，這給顧客帶來了額外的負擔[6]。

2.5 APF(Authentication Processing Framework)

Ayoade學者提出APF的架構。如圖4。

1. Tags向APF註冊Tag的ID和加密金鑰。
2. Reader向APF註冊。
3. Reader對Tag發送查詢。
4. Tag回應給Reader加密過後的資訊。
5. Reader會向APF要求這把解密金鑰。
6. APF經過判斷Reader是否為合法的存取者，如果合法APF會給Reader解密的金鑰。
7. Reader拿到解密金鑰即可知道Tag的資訊[4]。

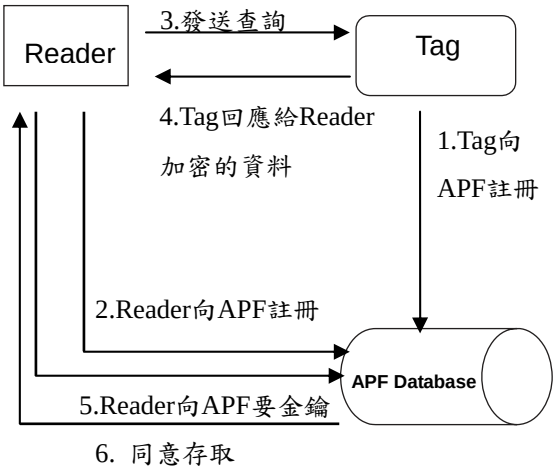

圖4 APF的架構流程圖

	Tag1	Tag2	TagN
Reader1	○	×	…
Reader2	×	○	…
ReaderN	…	…	…

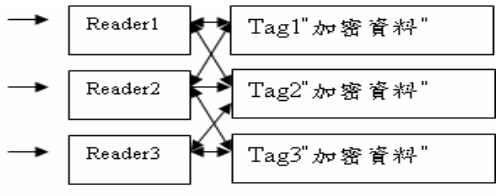

圖5 查詢Reader是否對能讀取Tag資料

3. 研究方法

本篇論文提出一個植基於APF架構的具隱私權保護RFID機制。

1. 一開始在資料庫產生一個金鑰 k然後用k與Tag的ID_i產生一訊息驗證碼 $k_i=MAC(k,ID_i)$。
2. Reader也存在一個RID_j，資料庫也存取一個Rk_j值在Reader中。令Reader的ID為RID_j，然後利用k與Reader的RID_j產生一訊息驗證碼$RKj=MAC(k,RIDj)$）。
3. Reader對Tag發送查詢要求。
4. Tag回應給Reader加密過後的資訊 $E_{k_i}(DATA)$和ID_i 。
5. Reader算出一個a值並把a，ID_i，RID_j送給database，其中$a=H(ID_i,RID_j)$然後database驗證Reader是否合法 DB : $a=?H(ID_i,MAC(RID_j,k))$）。
6. 如果正確就k_i給Reader。

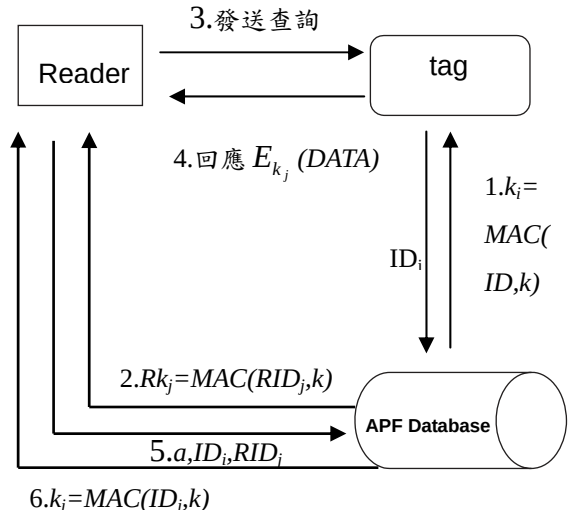

圖6 系統流程圖

4.效能分析

在此章節來探討以前的方法和本篇方法的好處和壞處。

Kill command:雖然這個方法可以保護資料的隱私性，但是把Tag抹除掉可能會產生日後的不便，例如產品的售後服務，廢品的回收等等。

Faraday cage:也可保護隱私，缺點是如果蹤到較大的商品就無法用金屬完全覆蓋，或者可能會有有心人士使用鋁箔把商品覆蓋住而逃避結帳。

Active jamming:可保護隱私，不過用這種方法大多情況是違法的，它會給不要求隱私保護的合法系統帶來嚴重的破壞，也有可能影響其他無線通信，如果位於一些重要的公共場所，如醫院、機場，可能會帶來人員傷亡。

Blocker Tag:可保護隱私，不過必需攜帶在合法Tag旁，此外也會讓顧客帶來額外的負擔。

APF 架構:可保護隱私，不過必需把每一個 Tag 的金鑰存到 database 上面，且 database 要核對 Reader 和 Tag 是否相互合法，會使用很多的資料庫空間，造成伺服器的負擔。

我們的方法:我們的方法不儘能保護隱私，且用 MAC 的方法做驗證，在存取的速度上的效率會比較快，Tag 也不用每一個都向 APF 存一把金鑰。

5. 結論

在本篇論文裡提出了一個方法能有效的解決 RFID 隱私的問題，它阻止存心不良的 Reader 來存取 Tag。對於 Tag 而言也有相對的便利性，對顧客而言，保護他們隱私資訊是很必要的，我們提出來的方法能確確實實的達到這個效果，避免未被授權的

Reader 存取 Tag 的資訊。

6. 參考文獻

[1] 彭皓、李泉林“**RFID**隱私與安全中的關鍵技術研究”， http://www.ie.tsinghua.edu.cn/~Liql/paper/RFIDC.pdf 。

[2] 曹世昌、韋一中“運用無線射頻辨識系統與網際網路技術建構停車場管理之連鎖企業”，2007 年。

[3] 黃明祥、林詠章，“資訊與網路安全概論-建構安全的電子商務系統”，第二版，美商 麥格羅.希爾國際股份有限公司，2007。

[4] J. Ayoade, “Security implications in RFID and authentication processing framework,” *Computers & Security*, Vol. 25, No. 3, May 2006, pp. 207-212.

[5] T. Hjorth. “Supporting privacy in RFID systems,” *Master thesis, Technical University of Denmark*, Lyngby, Denmark, December 2004.

[6] A. Juels, R. Rivest, and M. Szydlo, “The blocker tag: Selective blocking of RFID tags for consumer privacy,” In: *Proceedings of ACM Conference on Computer and Communications Security – ACM CCS*, Vijay Atluri, Editor, pp. 103–111, Washington, DC, USA, 2003.

[7] RFID specification from EPC Global. 13.56 MHz ISM Band Class 1 Radio Frequency (RF) Identification Tag Interface Specification, http://www.epcglobalinc.com/standards_technology/specifications.html .

[8] Wikipedia-The Free Encyclopedia. *Entry=Faraday Cage*, http://en.wikipedia.org/wiki/Faraday_cage .