抵擋 Tag Killing 攻擊的 RFID 安全機制

RFID Security Mechanism to Protect Tags from Killing

張凱評
亞洲大學
資訊工程學系
bigtony13888@gmail.com

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

曹世昌
亞洲大學
資訊工程學系
sctsaur@asia.edu.tw

摘要

無線射頻(Radio Frequency Identification，RFID)是已經被全球最大的零售商 Wal-Mart 及美國國防部採納，它的應用層面 遍及各行各業，但在廣泛的應用下，安全問題如資料隱私的洩漏或 Tag 被攻擊癱瘓等等，是目前最被探討議題之一。本論文針對 Han 等學者所提供 Tag Killing 攻擊方式在 Ohkubo 模型中加以探討，來找出一個新的方式來有效抵制 Tag Killing 攻擊，並防止標籤失效。本文所提出的方法，在效能方面上與 Ohkubo 的方法做比較為佳。

關鍵詞： Tag Killing、RFID

1. 緒論

無線射頻辨識系統(RFID)和條碼具有同時辨識大量標籤、較大的資料空間、可修改的身份辨識碼(ID)資料等優點，再加上成本低的誘因，使得近年來RFID應用迅速成長，並且運用廣泛。最明顯的例子就是美國零售業龍頭Wal-Mart，便是RFID最大的支持者，Wal-Mart藉由導入RFID技術，達到貨品的追蹤與管理自動化，也使物流更為有效率。

隨著被應用廣泛，RFID 安全也隨之被重視，但因為 RFID 標籤，只有較低的的運算能力和儲存容量，而使現今的安全技術發展不容易；安全又可分為攻擊和隱私洩漏，而本篇論文的方式是為攻擊癱瘓的，Tag Killing 的攻擊模組在 Ohkubo 的模型中，是無法倖免的，至於其他的攻擊方式如:前推安全(Forward Security)(FS) [5、8]、重送攻擊(Replay Attack) [5、8]等，在其他依照 Ohkubo 模型的方法是可以避免的[4、5、7、8]，所以本文是探討如何在 Ohkubo 模型[5、6、7、8]中，抵抗 Tag Killing 的攻擊，並且提出具體方法，本文中第一章為緒論，第二章我們介紹 RFID 背景和簡介，第三章則介紹 RFID 的相關研究，如：Ohkubo 模組方式、攻擊方式，第四章則是我們提出新的方法來抵制 Tag Killing [5、8]攻擊，第五章則是我們所提出的新的方法和舊的方法來比較分析，最後第六章是結論。

2. RDIF 技術背景

無線射頻辨識系統(Radio Frequency Identification，RFID)早在1969年即被發明出，但在被發明的三十年後，此技術才找

到許多重要的應用可行性，並被積極地應用於各種產業。例如從交通移動追蹤、製造業物料管理、門禁系統管理...等都可見其廣泛的應用。射頻無線辨識系統是一種電子式的資訊承載裝置，其所具備的無線讀取及高儲存量的特性，讓這項技術在自動化管理的應用領域日漸受到矚目。

2.1 RFID基本架構

無線射頻辨識系統的組成包含了下面幾個元件，分別為無線射頻訊號讀取器(RFID Reader)[1、3、5]、標籤(Tag)[1、3、5]及資料庫。

(1) Tag (如圖 1、圖 2) [1、3、5] ：

RFID 的 Tag 通常放置在需要被識別的物體上，並且其中通常包含了感應裝置及電子晶片(Microchip)；標籤主要可以分為兩大類(如表 1):

1. 主動式 Tag：體積較大較昂貴但因自備電源而讀取距離較遠。

2 被動式 Tag:體積小巧較便宜但須靠被動式感應產生電力所以讀取距離較近。

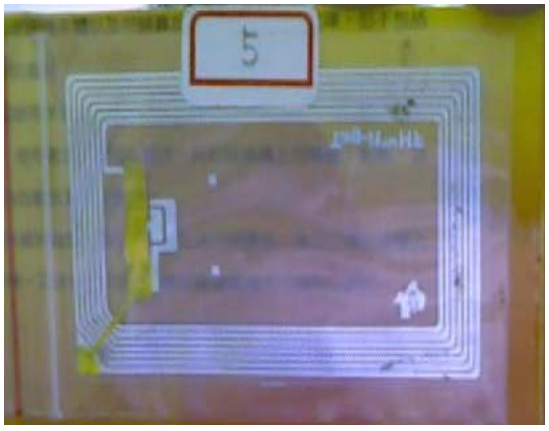

圖 1 RFID TAG

圖 2 RFID TAG

表 1 Tag 類別 [3]

	主動式	被動式
電源	自備電源(ex. 電池)	電力由 Reader 產生
體積	較大	小巧
價格	價格較貴	價格較便宜
讀取距離	較遠	較近

之後又可根據他們的計算資源分為基礎標記和智慧型標籤。

基礎標籤只能傳遞資料的標籤，無法做複雜的運算式子，而智慧型標籤可以運算較複雜的式子，如:悠遊卡;在本文裡，所提出的模型和方法都是屬於智慧型的標記。

(2) 辨識器(RFID Reader) [1、3、5] ：

可讀寫(read/write) 設計模式的辨識器，其中大部分都包含無線電模組(包括傳送器與接收器)、控制晶片及感應裝置。除此之外，有些 Reader 會配備有額外的介面(例: USB)，如此即可將接收的資料傳送到另外一個系統(例:PC)。

(3) 後端資料庫：

用來控制辨識器和標籤的資料來整合的一個資料庫。

2.2RFID 安全需求

(1)難以辨識性(Indistinguishability)(IND)

[5、8]：

即使攻擊者從不同的Tag獲得數個資料，但攻擊者不能辨識是哪一個Tag產出這些資料。

(2)前推安全(Forward Security)(FS)[5、8]：

即使目前的資料備洩漏出去給攻擊者，但在先前的資料仍是安全的。

(3)重送攻擊(Replay Attack) (RA)[2、5、8]：

攻擊者藉由攔截使用者的所發送的訊息，在下一次攻擊者可以發送這個攔截的訊息給伺服器，偽造一個合法的使用者。

(4)標籤殺手（Tag Killing）(TK)[5、8]：

攻擊者可藉由不合法的Reader對Tag重覆發送連接請求，使Tag記憶體存取最大量的記憶體資源，讓Tag無法再儲存任何Reader請求，或者造成大量令系統無法短時間解碼的Tag資訊，達到Tag的假性失效。

3. 相關文獻

由之前介紹的，我們得知RFID所存在的安全性問題，雖然現在已有許多模型、方法來解決目前的安全性問題，如：Ohkubo Type和Modified Ohkubo等，但在Tag Killing攻擊模式上還是無法有效抵抗，所以本篇論文就是提出一個新的方法來防止Tag Killing攻擊；以下先介紹Ohkubo類型和目前以Ohkubo類型為基礎的方法，之後在後面再提出改善的方法。

3.1 Ohkubo 模式:

我們介紹Ohkubo-Suzuki-Kinoshita所提出的原始Ohkubo模型[5、6、7、8]，Ohkubo模型(如圖3)是利用雜湊函數H和G來計算Hash的值來更新資訊包括標籤。

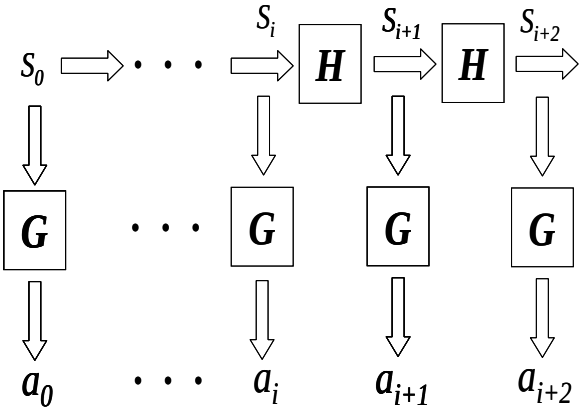

圖3 Ohkubo的工作模式[5、7]

TAG

存有一初始值S_1，此處假設Tag從沒存取超過N次最大循環。後端資料庫保存(ID，S_1)，而每一個TAG的S_1都不同，H、G為雜湊函數。

辨識器做i次的執行

1.辨識器：

首先辨識器對標籤傳送查詢請求。

2.標籤：

a.傳送$a_i = G(S_i)$給辨識器。

b.標籤將先前的S_i更新為$S_{i+1} = H(S_i)$。

3.辨識器：

辨識器傳送a_i給資料庫。

4.資料庫：

資料庫執行驗證a_i，使用公式$a_i' = G(H^i(S_1))$並比對資料庫的初始值S，直到相符合。

Tag Killing攻擊模式[5、8]

Tag Killing是阻斷服務攻擊(DoS attack)(Denial of Service)，廣播對Tag大量的Query，然後讓標籤停止其工作。

當Ohkubo模組受到Tag Killing的攻擊，有一個攻擊者一直對標籤傳送一個查詢的訊息，這時標籤收到訊息會一直產生S_{i+1}，當S_i值產生到一定的大小時，標籤就

會失去作用，而無法動作。

3.2 Modified Ohkubo[4、5、8]

TAG存有一初始值S_1，此處假設Tag從沒存取超過N次最大循環。後端資料庫保存(ID，S_1)，而每一個TAG的S_1都不同，H、G為雜湊函數。

辨識器做i次的執行：

1.辨識器：

首先辨識器對標籤傳送查詢請求。

2.標籤：

a.傳送$a_i = G(S_i \oplus r)$給辨識器。

b.標籤將先前的S_i更新為$S_{i+1} = H(S_i)$。

3.辨識器：

辨識器傳送a_i給資料庫。

4.資料庫：

資料庫執行驗證a_i，使用公式$a_i' = G(H^i(S_1) \oplus r)$並比對資料庫的初始值$S$，直到相符合。

本攻擊方法一樣也是無法抵擋Tag Killing攻擊模式，但比原始模組多一個抵抗重覆攻擊。

4. 提出的方法

本方法(如圖4)是由智慧型標籤以Ohkubo模組為基礎，針對他無法防禦Tag Killing的攻擊來做改善；首先標籤一開始會存放一個K_i值和ID值，而小i是代表每一個不同標籤，K_i值則是由後端資料庫中的k值經過$H(ID_i \,//\, K)$運算所得到的值；至於後端資料庫只有存一把K值，而標籤沒有存K值。

‧驗證步驟

1.辨識器：

首先辨識器對標籤傳送查詢的請求。

2.標籤：

a.先隨機產生一個nonce R值。

b.標籤產生$H(K_i \,//\, R)$值。

C.傳送R，$H(K_i \,//\, R)$，IDi給辨識器。

3.辨識器：

辨識器傳送R，$H(K_i \,//\, R)$，ID_i給資料庫。

4.資料庫：

a.先藉由得到的R和ID_i值，產生$K_i = M(ID_i \,//\, K)$

b.藉由剛剛a步驟的K_i產生$H(K_i \,//\, R)$

c.驗證資料庫的$H(K_i \,//\, R)$是否等於$H(K_i \,//\, R)$，如果相等就是驗證成功，不相等的話就結束整個驗證動作。

本方法因為標籤在驗證過程中未寫入任何資料，加上後端資料庫驗證失敗整個動作就結束，所以本方法可以有效的抵擋Tag Killing攻擊。

五.效能分析

本項針對了本方法和幾個方法(Original Ohkubo scheme、Modified Ohkubo scheme、Ohkubo scheme with grouping)來做安全比較(表2)和效率比較(表3)

安全方面，本論文能達到TK，對於IND、FS、RA攻擊也能夠加以防禦。下面加以詳細說明：

(1)難以辨識性（Indistinguishability）(IND)：

為了防止攻擊者從數個 Tag 中，能夠辨識所傳遞的資訊是從哪個 Tag 所傳出，Tag 在訊息傳遞前，會將相關資料資訊加密，以防止 Tag 資料能被追蹤。本論文就使用 MAC 加密，使攔截訊息者，不容易從訊息內容，得知 Tag 內容。

(2)前推安全(Forward Security)(FS)：

如果Tag當中某一段資料，或者Tag和資料庫認證的通行金鑰洩漏出去，那整個系統的通訊將變的不安全，為了防止通行金鑰一但洩漏，以前的資料獎被解讀出，本論文使用一隨機而不重複的亂數*R*，使攻擊者解密更加困難，即使目前的資料備洩漏出去給攻擊者，但在先前的資料仍是安全的。

(3)重送攻擊(Replay Attack) (RA)：

藉由重覆傳從Tag攔截傳遞的資訊，攻擊者很容易可以和資料庫進行合法認證。為了防止這漏洞，本論文因為標籤會隨機產生一個不重複的R值，來造成每個時間點Reader所傳的R值都不同，即使攻擊者攔截一段Tag傳送資訊，但是因每個時間點Reader傳送的R值都不同，使攻擊者無法由當次攔截到的訊息，去和別次通訊的訊息去做認證，所以以此方法可以達到防範重送攻擊。

(4)標籤殺手（Tag Killing）(TK)：

本論文Tag不存加密金鑰,所有金鑰都是由赫序函數計算產生；而資料庫也只存唯一的一把解密金鑰，不進行赫序函數運算,當次認證失敗,整個通訊即宣告結束。如此Tag不會因大量的Reader請求而佔據大量記憶體，資料庫也不會因為計算量過大，導致效能太差無法回應Tag認證，可以保證不受標籤殺手影響。

在效能方面(表3)，本論文簡化加密的步驟，讓整個處理速度比以往提出的方案更加快速，以下分析各部份效能比較：

本分析表(T_H:為赫序運算的次數，T_{XOR}:為XOR運算的次數)表示依造舉出各方案在三方面(標籤、辨識器、後端資料庫)所計算的次數來加以彙整，並且整理成表，由表可得知本文方法是最好的，運算次數是少的。

表 2 安全比較表(○:可以，X：不可以)

Security Methods	IND	FS	RA	TK
Ohkubo Scheme[5、7、8]	○	○	X	X
Efficient Ohkubo Scheme[8]	X	○	○	X
Modified Ohkubo Scheme[4、5、8]	○	○	○	X
我們的方法	○	○	○	○

表3 效能比較表

	Computation Time		
Security Methods	Tag	Reader	Database
Ohkubo Scheme[5、7、8]	2 T_H	No Time	NM T_H
Efficient Ohkubo Scheme[8]	2 T_H	No Time	N T_H
Modified Ohkubo Scheme[5、4、8]	2 T_H + 1 T_{XOR}	No Time	NM T_H
我們的方法	2 T_H	No Time	1 T_H

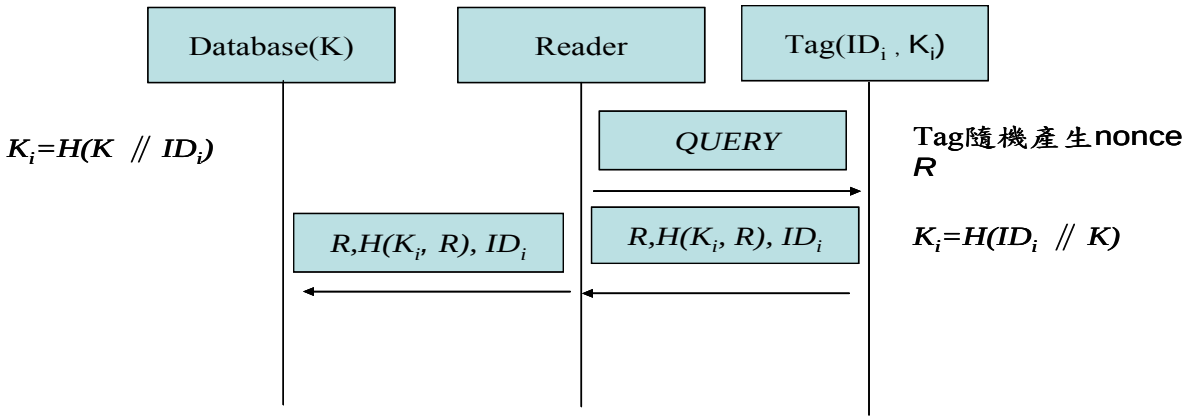

圖4 我們的方法

六、結論

本論文所提供的方法,不但保有原先抵擋的安全方式(IND、FS、RA)，又多增加可以抵擋Tag Killing攻擊方式可以有效的抵擋Tag Killing攻擊方式，雖然本文所提供的方法多抵擋一種攻擊方式，但他的效能,並沒有因此變差,還比之前的方法好，運算次數小，而且後端資料庫只需存檔一個K值就好，所需的硬體設備並不用很好，而且可以降低成本，並且比原先的方法運算量較小、速度較快、後端資料庫只有存入一個k值就可,節省後端資料庫配備的需求，所以本文提供的方法可有效的抵擋Tag Killing的攻擊模式。

在日後發展可以再多結合其他的安全需求，如:所有權轉移…等需求來研究。

參考文獻

[1]. 黃國祐,“RFID 安全性議題之研究”，亞洲大學碩士論文，2006 年 6 月。

[2]. 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。

[3]. 周學忠、曹世昌,“運用無線射頻辨識技術建置供應商庫存系統”,2006 年。

[4]. G. Avoine, E. Dysli, and P. Oechslin, “Reducing time complexity in RFID systems,” In *Proceedings of Selected Areas in Cryptography* (SAC 2005), LNCS, Springer-Verlag, pp. 291-306, 2005.

[5]. D. G. Han, T. Takagi, H. W. Kim, and K. I. Chung, “New security problem in RFID systems tag killing,” In *Proceedings of ACIS 2006*, LNCS, vol. 3982, Springer-Verlag, pp.375–384, 2006.

[6]. Z. Luo, T. Chan, J. Li, E. Wong, W. Cheung, and V. Ng, W. Fok, “Experimental Analysis of an RFID Security Protocol,” In *Proceedings of IEEE ICEBE*, pp. 62-70, 2006

[7]. M. Ohkubo, K. Suzuki, and S. Kinoshita, “Cryptographic approach to privacy-friendly tags,” In *Proceedings of RFID Privacy Workshop,* MIT, USA, 2003.

[8]. K. Osaka, T. Takagi, K. Yamazaki, and O. Takahashi, “An Efficient and Secure RFID Security Method with Ownership Transfer,” In *Proceedings of*

International Conference on Computational Intelligence and Security, CIS 2006, LNAI 4456, pp.778-787, 2007.