Dass 等人 RFID 認證協定之安全分析

Security Analysis to Dass et al.'s RFID Authentication Protocol

謝文恭
Wen-Gong Shieh
中國文化大學
資訊管理學系
教授
wgshieh@faculty.pccu.edu.tw

呂淑瑛
Shu-Ying Lu
中國文化大學
資訊管理學系碩士班
研究生
snady.kkkk@msa.hinet.net

摘要

在這個日新月異及資訊爆炸的時代，資訊的傳遞繁忙且巨量，網路通訊各方需要安全、有效的身份識別認證機制，以確保其通訊正確、安全。而現今已普遍使用的無線射頻身份識別（RFID）機制，因物聯網的廣泛應用，其認證技術之安全有效，更顯重要。在 2016 年，Dass 等人提出新的 RFID 認證協定，強調使用隨機亂數及簡單的演算法來達到 RFID 標籤識別機制的安全性。但是本研究發現，Dass 等人的 RFID 認證協定存在標籤仿冒的安全漏洞。攻擊者可以先複製並儲存讀取器與標籤之間傳送的訊息，再藉由簡單的邏輯運算來偽造被仿冒標籤回應讀取器的訊息，即可成功通過伺服器的辨識檢查，使伺服器誤認為攻擊者是真標籤，而仿冒成功。本研究提出攻擊的詳細步驟、探討其安全漏洞的成因、指出其解決之方向並提出一個可行的解決方法。

關鍵詞：認證、重送攻擊、標籤仿冒、無線射頻身份識別。

Abstract

In this ever-changing and information explosion era, the transmission of information is busy and huge. The Internet communication parties need a safe and effective identification mechanism to ensure that their communication is correct and safe. Due to the popular application of the Internet of Things, the security of the Radio Frequency Identification (RFID) mechanism becomes more and more important. In 2016, Dass et al. proposed a new RFID authentication protocol, emphasizing the use of random number and simple algorithm to achieve the security of the RFID tag recognition mechanism. However, this study found that Dass et al.'s RFID authentication protocol has a security flaw of tag counterfeiting. An attacker can copy and store the message sent between the reader and the tag, and then use a simple logical operation to counterfeit the legal respondent message to the reader in next tag reading, which can be successfully checked by the server. Therefore, the server mistakenly thinks that the attacker is the real tag, and counterfeit success. This study presents the detailed steps of the attack, explores the causes of its security vulnerabilities, points out the direction of its solution and proposes a feasible solution.

Keywords: authentication, replay attack, tag counterfeiting, RFID

1. 緒論

現今普遍使用的 RFID 技術已漸漸取代傳統條碼系統，舉凡物流、醫療、門禁、防盜、交通運輸等，都有採用 RFID 的案例[1]。因此，RFID 的隱私與安全問題受到關注與重視。近年來，由於 RFID 應用於物聯網的興起，RFID 的認證技術之安全有效，更顯重要。

2010 年，Yeh [2]等人提出一個 RFID 協定。然而，2012 年 Yoon [3]指出，Yeh 等人的協定有安全漏洞，同時提出一個改善的新協定。然而，謝文恭等人[4]在 2012 年發現，Yoon [3]提出的新協定，並不如其所宣稱的安全。攻擊可讀取機密的商品資料、假冒伺服器和竄改商品資料[4]。2016 年，Dass [5]等人提出新的 RFID 認證協定，該協定宣稱可抵抗重送攻擊、可抵抗中間人攻擊、可抵抗標籤與伺服器不同步、可抵抗標籤追蹤、且具備標籤匿名、標籤與伺服器交互認證等等的安全特性。但是本研究發現，Dass [5]等人的 RFID 認證協定，仍然存在標籤仿冒的安全漏洞。本研究將詳細說明攻擊者如何仿冒標籤，成功騙過伺服器的過程。同時探討該安全漏洞的成因，指出其解決之方向並提出一個可行的解決方法。

本文後續內容如下：第 2 節介紹 Dass [5]等人協定之流程，第 3 節詳述標籤仿冒攻擊的方法與程序，第 4 節探討安全漏洞的成因與解決方向，最後，在第 5 節的結論，我們提出一個可行的解決方法。

2. Dass 等人所提認證協定

2.1 協定的符號及假設

首先介紹 Dass [5]等人 RFID 認證協定中使用的符號，如下表 1：

表 1 使用符號表

N_R	Reader 產生的亂數
N_T	Tag 產生的亂數
S	標籤秘密
ID	標籤 ID
S_{new}	存在 Server 的標籤新秘密
S_{old}	存在 Server 的標籤舊秘密
PRNG(A)	用 A 種子產生的亂數
PRNG(A,B)	用 A 為種子，所產生第 B 個亂數。
h()	單向雜湊函數
⊕	互斥或運算
‖	合併運算

另外，在 Dass [5]等人的 RFID 認證協定中，假設每一標籤儲存一筆(ID,S)的資料，並假設伺服器在其資料庫中，已為每一標籤對應儲存一筆(ID,h(ID),S_{old},S_{new})的資料，且協定開始運作前，設 $S_{old}=0$，$S_{new}=S$。

2.2 協定的流程

依 Dass [5]等人 RFID 認證協定之程序，當讀取器讀取 RFID 標籤時，請參考圖 1，讀取器、RFID 標籤及伺服器將執行下列步驟：

1. 讀取器產生亂數(N_R)且傳送給標籤。
2. 標籤產生亂數(N_T)並計算 $V=PRNG(S⊕N_R⊕N_T)$ 和 $H=h(ID)$，然後傳送 V, H, N_T 給讀取器，讀取器再傳送 V, H, N_T ,N_R 給伺服器。
3. 伺服器收到這些資料後，搜尋資料庫中是否存在一筆(ID, h(ID), S_{old}, S_{new}) 的資料，滿足其中的 h(ID)和 H 相等，並依其結果執行下列工作：
   1) 如果找不到相等資料，則溝通中止。
   2) 如果找到，伺服器設 Flag=0，計算 $V'=PRNG(S_{new}⊕N_R⊕N_T)$，並檢查 V'和 V 是否相等，如果 V'=V，則確認之前的 session 是成功的且標籤存的 S 就等於伺服器的 S_{new} 值，並傳送 S_{new} 給讀取器。
   3) 如果 V' 不等於 V，伺服器計算 $V''=PRNG(S_{old}⊕N_R⊕N_T)$，並檢查 V''和 V 是否相等，如果相等，則設 Flag=1，且傳送 S_{old} 給讀取器，表示先前的 session 是不成功的，此時標籤存的 S 是伺服器的 S_{old} 值。
   4) 如果 V''和 V 不相等，則溝通中止。
4. 讀取器從伺服器得到 S_{new} 或 S_{old} 當作種子 Seed，且計算 $M=PRNG(Seed, N_R)$，$N=PRNG(M)$，並傳送 N 給標籤，傳送 M 給伺服器。
5. 標籤為了確認讀取器是合法的，標籤計算 $M'=PRNG(S, N_R)$，其中 S 是存於標籤的秘密值，

計算 N'=PRNG(M')，並查檢 N'和 N 是否相等，如果相等，標籤確認此資料是來自合法的讀取器以及伺服器，標籤計算 U=h(S||M')，且更新 S，即 $S=S\oplus U$。

6. 伺服器檢查 Flag 的值來更新資料:
   1) 當 Flag=0，代表標籤的秘密 S 符合 S_{new} 值，伺服器計算 $U=h(S_{new}||M)$，然後更新 S_{old} 與 S_{new} 的值，即 $S_{old}=S_{new}$，$S_{new}=S_{new}\oplus U$。
   2) 當 Flag=1，代表標籤的秘密 S 符合 S_{old} 值，伺服器計算 $U=h(S_{old}||M)$，然後伺服器只更新 S_{new} 值，即 $S_{new}=S_{old}\oplus U$，且 S_{old} 維持不變。

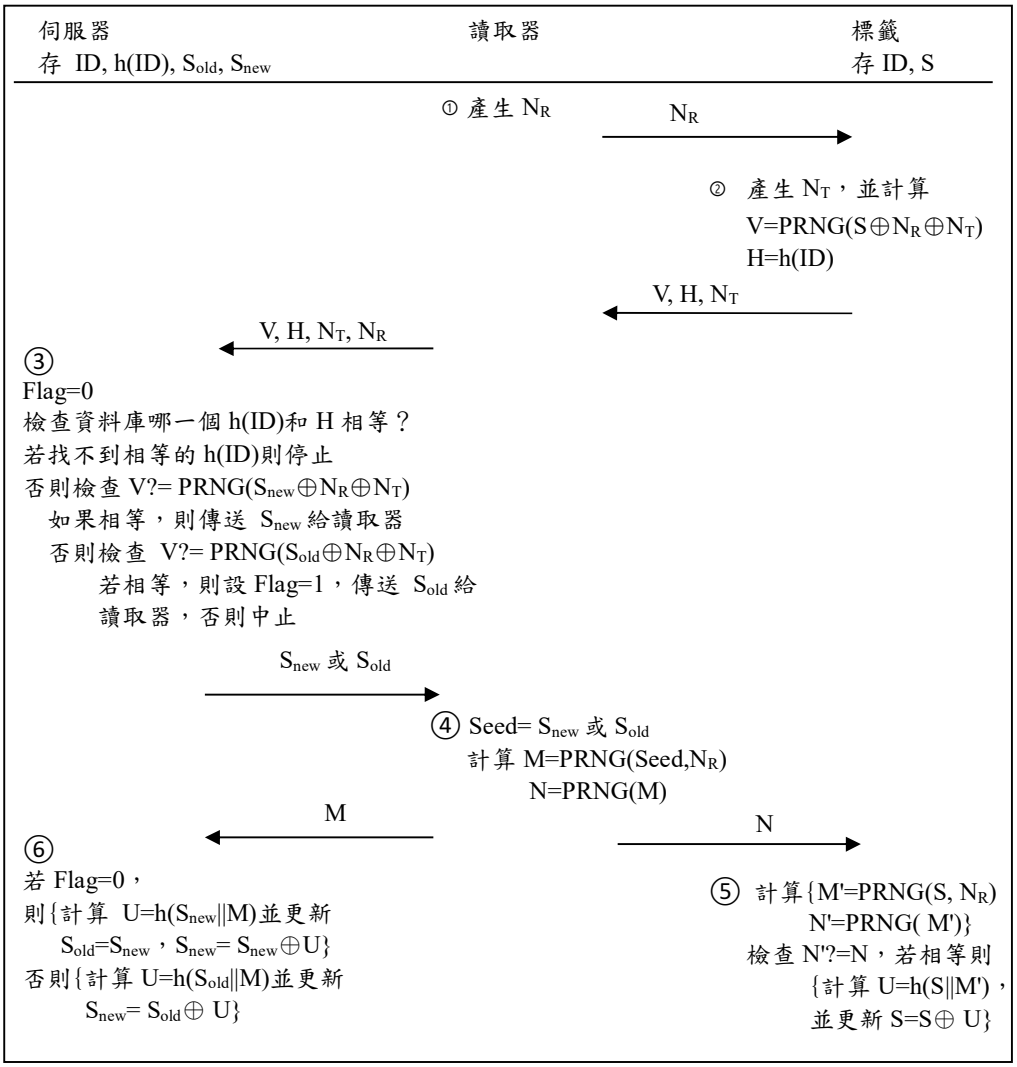

圖 1. Dass [5]等人的認證協定

3. 標籤仿冒攻擊

所謂標籤仿冒，例如仿冒合法標籤 Tag5，是指當讀取器在讀取某 RFID 標籤時，攻擊者操弄讀取程序中讀取器與 RFID 標籤之間傳送的訊息，使 RFID 系統誤認為讀取器讀取到的，是某特定的合法標籤，例如標籤 Tag5。但實際上，正被讀取的並非合法標籤 Tag5，甚至是沒有任何合法標籤正被讀取。

現在，配合 Dass [5]等人 RFID 認證協定之程序，我們介紹攻擊者執行標籤仿冒的程序。假設被仿冒的標籤是 Tag5。當讀取器讀取 RFID 標籤 Tag5 時，請參考圖 2，攻擊者、讀取器、RFID 標籤 Tag5 及伺服器將執行下列步驟：

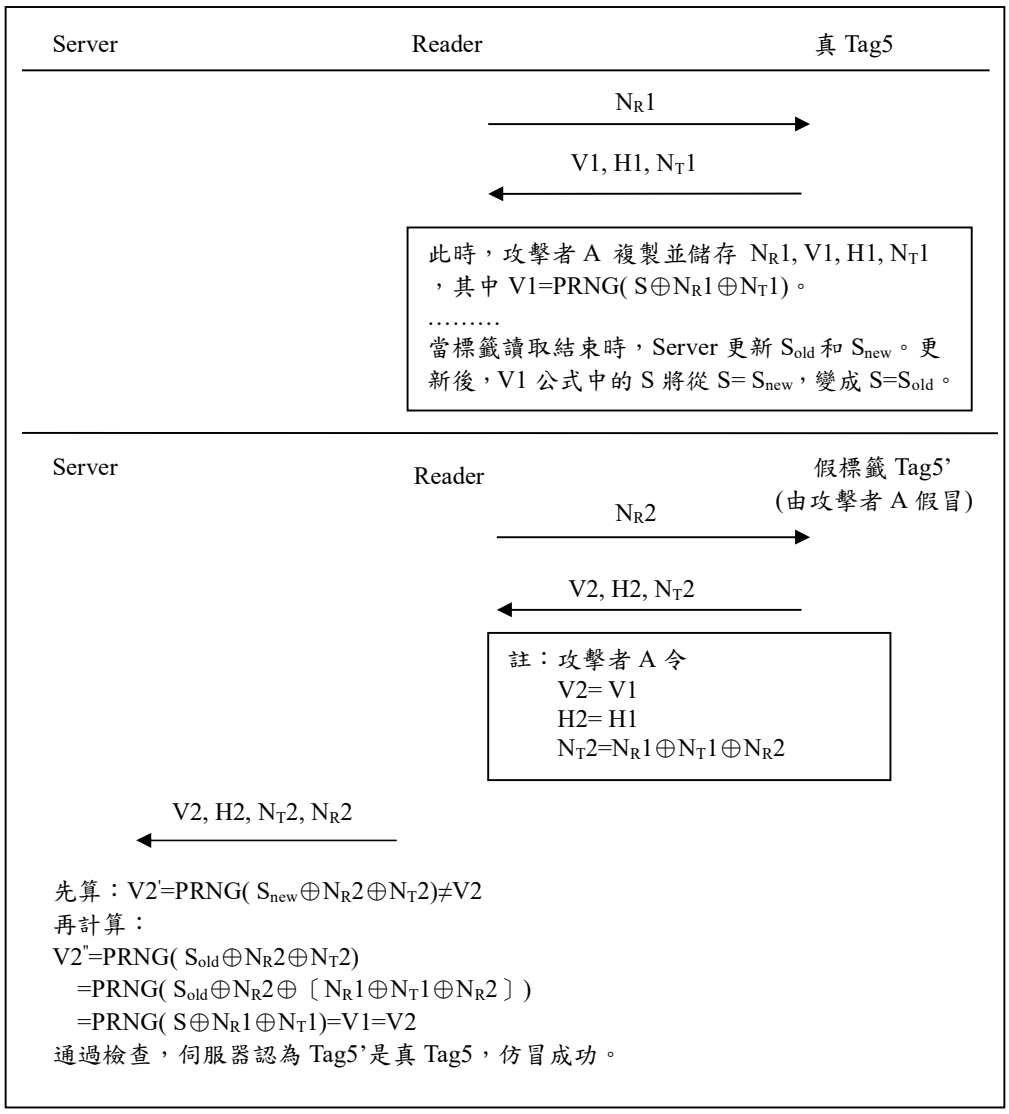

圖 2. 標籤仿冒攻擊

1. Reader 讀取真標籤 Tag5，傳送隨機數 N_R1 給真 Tag5，而真 Tag5 傳送 V1, H1, N_T1 給 Reader。於此同時，攻擊者 A 複製並儲存 N_R1、V1、H1、N_T1。請注意，其中的 $V1=PRNG(S\oplus N_R1\oplus N_T1)$。接著合法的 Server、Reader 和 Tag5 執行後續協定程序，結束時伺服器更新 S_{old} 和 S_{new}。此時，根據作者的協定，前面 V1 公式中的 S ，將從原來與 S_{new} 相等，變成與 S_{old} 相等，即 $S=S_{old}$。
2. 經過一段時間後，假設 Reader 尚未有機會再次讀取真 Tag5。此時，攻擊者 A 仿冒 Tag5，讓 Reader 再讀取一次 Tag5，但此時讀取的是假標籤 Tag5'，由攻擊者 A 假冒。
3. 當 Reader 讀取假標籤 Tag5'時，Reader 產生 N_R2 傳送給 Tag5'。此時，攻擊者 A 假冒的 Tag5' 則傳送 V2, H2, N_T2 給 Reader。其中，攻擊者 A 令 V2＝V1, H2＝H1 且 $N_T2=N_R1\oplus N_T1\oplus N_R2$。Reader 將轉送 V2, H2, N_T2 及 N_R2 給 Server。
4. Server 收到 V2, H2, N_T2 及 N_R2 後，先依 H2（即 H1）於資料庫中找到真標籤 Tag5 所對應的 ID、h(ID)、S_{old} 和 S_{new}。
5. Server 計算 $V2'=PRNG(S_{new}\oplus N_R2\oplus N_T2)$，Server 將發現 $V2'\neq V2$，理由如下：

   $V2'=PRNG(S_{new}\oplus N_R2\oplus N_T2)$

   $=PRNG(S_{new}\oplus N_R2\oplus〔N_R1\oplus N_T1\oplus N_R2〕)$

   $=PRNG(S_{new}\oplus N_R1\oplus N_T1)$……(1)

   而 $V2=V1=PRNG(S\oplus N_R1\oplus N_T1)$

   $=PRNG(S_{old}\oplus N_R1\oplus N_T1)$……..(2)

   比較(1)和(2)，由於 $S_{old}\neq S_{new}$，因此 $V2'\neq V2$。
6. Server 接著計算 $V2''=PRNG(S_{old}\oplus N_R2\oplus N_T2)$，此時，$V2''=V2$，因為：

   $V2''=PRNG(S_{old}\oplus N_R2\oplus N_T2)$

   $=PRNG(S_{old}\oplus N_R2\oplus〔N_R1\oplus N_T1\oplus N_R2〕)$

   $=PRNG(S_{old}\oplus N_R1\oplus N_T1)$

   $=PRNG(S\oplus N_R1\oplus N_T1)=V1=V2$

因為認證碼 $V2''=V2$，所以 Server 會把假標籤 Tag5'(由攻擊者 A 假冒)誤認為是真標籤 Tag5，即攻擊者 A 成功騙過 Server，達成標籤仿冒的目的。

4.安全漏洞的成因與解決方向之探討

究竟 Dass [5]等人 RFID 認證協定之安全漏洞如何形成？首先回顧本研究的攻擊方法。在前一節中，我們詳述攻擊者如何仿冒標籤 Tag5，成功騙過伺服器的過程。請注意，其中使用重送攻擊，即 H1=h(ID)和 $V1=PRNG(S\oplus N_R1\oplus N_T1)$被攻擊者重送。也即，攻擊者 A 令 V2＝V1, H2＝H1。另外，攻擊者始終不知標籤 Tag5 中的 S 之值，卻巧妙的運用互斥或運算 X⊕Y⊕Y＝X 的特性，令 $N_T2=N_R1\oplus N_T1\oplus N_R2$，使得伺服器計算的 $V2''$等於 V2。即 $V2''=PRNG(S_{old}\oplus N_R2\oplus N_T2)=PRNG(S_{old}\oplus N_R2\oplus〔N_R1\oplus N_T1\oplus N_R2〕)=PRNG(S_{old}\oplus N_R1\oplus N_T1)=PRNG(S\oplus N_R1\oplus N_T1)=V1=V2$。

因此可知，安全漏洞的關鍵在認證碼 $V1=PRNG(S\oplus N_R1\oplus N_T1)$之計算公式。其中的互斥或運算，$S\oplus N_R1\oplus N_T1$，提供了攻擊者重複使用認證碼 V1 的機會：只要令 $N_T2=N_R1\oplus N_T1\oplus N_R2$，且令 V2＝V1，即可使伺服器計算的 $V2''$等於 V2。換句話說，雖然沒有 S，攻擊者製作不出 V2，但攻擊者可使用舊的 V1，令 V2=V1，並運用互斥或運算 X⊕Y⊕Y＝X 的特性，令 $N_T2=N_R1\oplus N_T1\oplus N_R2$，即可成功仿冒標籤 Tag5。

了解安全漏洞的成因後，解決方向即可針對 $V1=PRNG(S\oplus N_R1\oplus N_T1)$之認證碼計算公式做修正。可能的修正方法很多，因超出本文之範圍，我們只建議三種修正 V1 的解決方向，包括：

1. 除了使用互斥或運算，加上其他運算，使 X⊕Y⊕Y＝X 的特性無從發揮。
2. 不使用互斥或運算，使 X⊕Y ⊕Y＝X 的特性根本無從發揮。
3. V1 之計算公式中，修改 S、N_R1 及 N_T1 之參數，使攻擊者無法利用舊的 V1。

以上三種修正，皆須在標籤及伺服器兩端的執行步驟內同步修正，由於內容超出本文之範圍，我們只建議上述三種解決方向，實際內容，包括修正後之安全性及成本效益分析，將列入本文之未來研究方向。

5. 結論

在 2016 年，Dass [5]等人提出新的 RFID 認證協定，該協定宣稱可抵抗多種攻擊，且具備標籤與伺服器交互認證等等的安全特性。但是本研究發現 Dass 等人的認證協定，仍然存在標籤仿冒的安全漏洞。本研究不但詳細說明攻擊者仿冒標籤的過程，同時探討該安全漏洞的成因，並指出三種修改認證碼計算公式的解決方向，包括：不使用互斥或運算，加上其他運算及修改參數。如此，即可阻止攻擊者利用舊的認證碼來進行標籤仿冒。

最後，我們提出一個可行的解決方法，採用前一節中的第 3 種建議：即修改認證碼 V1 中參數的解決方法。我們可以刪除 $V1=PRNG(S\oplus N_R1\oplus N_T1)$ 之計算公式中的 N_T1，使攻擊者無法利用舊的 V1。也就是將認證碼 V 之公式從 $V=PRNG(S\oplus N_R\oplus N_T)$ 改成 $V=PRNG(S\oplus N_R)$，即是可行的解決方法。因為 V 之公式中沒有 N_T，攻擊者就無法操弄 N_T2，令 $N_T2=N_R1\oplus N_T1\oplus N_R2$，也就無法使用舊的 V1。同時，因為 N_T 在協定中無具體其他功能，刪除協定中全部的 N_T，並不會對協定造成任何負面影響。如此一來，標籤不但不必產生 N_T，不必傳送 N_T，且計算認證碼 V 及傳送訊息時，也可以減少運算及通訊成本。由於修正後之實際演算及內容分析超出本文之範圍，包括修正後之整體安全性及成本效益分析，將列入本文之未來研究方向。

參考文獻

[1] 陳昱仁、廖耕億、許建隆、林仲志 (2009)，*RFID概論*，台北，華泰文化。

[2] Yeh, T. C., Wang, Y. J., Kuo, T. C., Wang, S. S., "Securing RFID systems conforming to EPC Class 1 Generation 2 standard," *Expert Systems with Applications*, vol. 37, no. 12, pp. 7678-7683, December 2010.

[3] Yoon, Eun-Jun, "Improvement of the securing RFID systems conforming to EPC Class 1 Generation 2 standard," *Expert Systems with Applications*, vol. 39, no. 1, pp. 1589-1594, January 2012.

[4] 謝文恭、何翊巍 (2012)，符合 EPC 第二代第一類 RFID 安全協定之探討與改良，*2012 第八屆知識社群國際研討會論文集*，中國文化大學，台北市。

[5] Prajnamaya Dass and Hari Om, "A secure authentication scheme for RFID systems," *Procedia Computer Science*, vol. 78, pp. 100–106, 2016.