3-10　RFIDに対する不正アクセス対策の発見

3-10 Finding Solution to the Illegal Access in RFID

Ayoade John Olurotimi　滝澤　修　中尾康二
Ayoade John Olurotimi, TAKIZAWA Osamu, and NAKAO Koji

要旨

RFID システムにおいて、多数のリーダ（質問器）によるタグへのアクセス及び読み書きが可能なシステムでは、タグに記載されている情報が不正に改ざんされる恐れがあり、サービス不能化、タグの個人情報の侵害、さらにはプライバシー／機密情報の漏えいを招く可能性がある。

本論文では、タグ内の情報にアクセスする前にリーダの認証を行うフレームワークを提案する。提案する手法を認証処理フレームワーク（APF：Authentication Processing Framework）と呼ぶ。リーダは APF に登録され、リーダはタグにアクセスして読み書きするためのアクセス制御キーを APF から取得する。RFID システムにこの種のフレームワークを実装することにより、RFID システムの利点を損なう問題や障害となる可能性のあるセキュリティ及びプライバシー問題が改善される。

In a system where many readers have access to read from and write to a tag, one can fear that ill-intentioned persons may try to modify the information contained in the tag which could lead to the denial of service, intrusion into the personal/private information in the tag and eventually result into the violation of privacy/confidential information.

In this paper, we proposed a framework that will authenticate readers before they can access the information in the tags. The proposed procedure is called Authentication Processing Framework - APF. Readers will register with the APF and get the access control key that will allow them to have access to read from and write to the tag. Implementing this kind of framework in the RFID system will alleviate the security and privacy concerns which are some of the major potential challenges and impediments to the RFID system's benefits.

[キーワード]
RFID，認証，不正アクセス，APF
RFID, Authentication, Illegal access, APF

1　はじめに

RFID は Radio Frequency Identification（無線 IC タグ）の略で、リーダ、タグ、アンテナ、ホストコンピュータからなる自動識別システムをいう。無線 IC タグ（RFID）は、専用デバイス（タグ）が貼付されたものをすべて識別することを可能にする技術である。タグは、一定の範囲内にあるタグを無線で識別する固定式又は移動式の「リーダ」により読み取ることができる。この技術では車両の移動中にリーダがタグを読み取ることができるので、特に自動車、鉄道機関車、鉄道車両などの移動設備や輸送車両に有用である[1]。

1.1 RFID のセキュリティ

RFID のセキュリティがこれまで重要視されなかった理由は以下のとおり幾つかある。

- RFID がこれまでは主に閉じたシステムで使用されてきた。
- 読み取り専用のタグが使用されることが多かった。
- RFID 業界が性能（読み取り有効範囲）の向上とコスト削減を主眼に置いており、ユーザのセキュリティ要求条件にはあまり注意を払ってこなかった。

唯一の例外として自動車への応用（イモビライザー）がある。

「セキュリティ」という用語は非常に広い意味で使用されている。これを明確にするため、RFID のセキュリティを次のように定義する。

・データ・セキュリティ：これは、RFID システムの一部としてタグに記憶されたデータに対するアクセスの許可を指す。記憶された情報は、（無線インタフェースを介して）直接あるいは情報伝達経路途中のいずれかのポイントでタグを作動できる者により「観測可能」になる。こうした情報の提供者や所有者には、「許可された」受取人だけに内容を「知る」ことを許可する必要がある場合がある。このようなデータの知識をデータの「観測」として定義する。

・データ保全：これは、「無許可」の機器によって、タグに含まれるデータを意識的又は無意識に変更、修正できないようにするものである。このような修正には、データを使用不能（破損）にするものなどがある。

・データ有効性：この特性は、要求ソースから出ているタグから取得されるデータの「信ぴょう性」を指す。特に偽造タグによるデータ複製の問題に関連する[2]。

2 問題点

セキュリティ機能は、確実なデータ保全、認証に必要である。これは、場合によってはタグの無制限な読み取りは不適当であるという概念である。読み書き機能の場合には、タグに書き込む者を管理し、またデータがタグの一部として流れる場合には、制御コードと暗号技術、そしてオプションが使用できるシステムが必要な場合がある。こうした理由から、タグ内のデータにアクセスしようとしている者を管理することは重要である[1]。

図 1 は、タグに記憶された情報を読み取る目的で質問コマンドをタグに送るリーダを示す。また、タグはリーダに応答コマンドを送る。この応答コマンドには、タグの ID 番号とそのタグに記憶された情報を含むことができる。

ただし、ここでは不正リーダがタグに記憶された情報をタグの所有者に知られずに読み取ってしまう脅威がある。

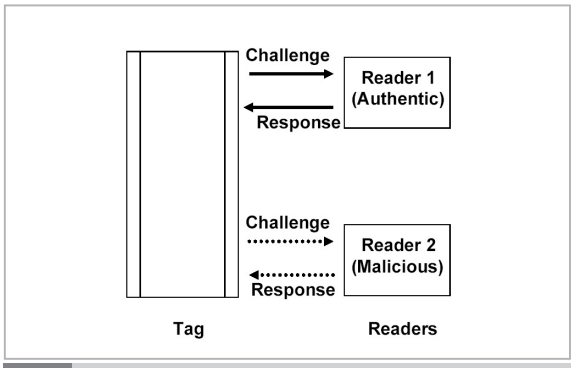


図1 タグ―リーダ間の質問／応答コマンド

図 1 の例では、リーダ 1 が認証されたリーダ、リーダ 2 は不正リーダである。この例から次のような三つの問題が生じる可能性があると考えられる。

(a) 機密性の欠如：リーダ 2 は、タグの所有者に知られずにタグ内の情報にアクセスし、タグにアクセスした後でタグ内の個人情報を盗む。これはタグの所有者のプライバシー／機密性の侵害につながる。

(b) 可用性の欠如：リーダ 2 が、リーダ 1 をタグ内の情報にアクセスできないようにする可能性がある。これはリーダ 1 のサービス不能化につながる。

(c) 保全性の欠如：リーダ 2 が、タグ内の情報を修正する可能性がある。

以上のような三つの問題があるが、ここでは機密性の欠如という最初の問題の解決のみを検討する。

2.1 これまでの研究

RFID のセキュリティと認証に関しては、これまで研究はほとんど行われてこなかった。

a キル・コマンド（Kill Command）の概念：Auto ID Center によって提案された標準の動作形態は、実際にはタグ付き製品を購入時に動作不能にするタグに関するものである。この提案では、特別な「キル」コマンドを送ってタグを動作不能にすることができる。ただし、「キル・コマンド」のように単純な手段は、プライバシー強化に望ましくない状況も多い。例えば、消費者が所有している RFID タグの動作状態を維持したいという場合がそれである[3]。

b　ファラデー箱手法：ファラデー箱を使用してRFIDタグを精査から遮へいすることができる。このファラデー箱とは、一定の周波数の無線信号を通さない金属メッシュ又は箔からなる容器である。万引き検出装置を作動させないよう、箔を内側に貼ったバッグを小売店で使用した盗難が幾つか報告されている[3]。

c　妨害（Active Jamming）手法：妨害手法は、タグを視界から遮る物理的手段である。この手法では、無線信号を積極的に送信する無線周波数装置を使用して、付近のRFIDリーダを作用させないようにすることができる。ただし、この手法は違法行為となる可能性がある。例えば送信出力が高すぎると、付近のRFIDシステムすべてを妨害するだけではなく、病院や列車などの規制領域内では危険や問題を引き起こす可能性がある[4]。

d　ブロッカー・タグ手法：ブロッカー・タグは、リーダの照会に対して模擬信号で応えるタグで、これによりリーダを混乱させるものである。妨害と同様、他の合法タグに影響を及ぼすことがある[4]。

このような手法はプライバシー問題に対して優れた解決策となり得たが、前述した問題点があるため、認められていない。本論文では、この問題に取り組むためには適切な認証手順が最良の選択肢であると考えた。したがって、ここで提案するAPFがプライバシー問題に対する解決策となり、RFIDシステムのセキュリティを高める。

3　提案する認証処理フレームワーク

本論文では、タグ内の情報へのアクセス権を取得する前にリーダを登録する認証処理フレームワーク（APF）を提案する。タグに読み書きする前にリーダを認証することにより、不正リーダのタグに対する無許可のアクセスを防止するため、不正リーダのタグに対する不正アクセスを解決する手順としてAPFを提案する。以下では、APFの処理手順と、プライバシーの侵害となるタグへの不正リーダによるアクセスの問題について、APFフレームワークを利用した解決方法について説明する。

図2ではAPFシステムの処理を逐次的に示す。まず、タグはそのID番号と復号キーをAPFデータベースに登録する。このときリーダもそのID番号をAPFデータベースに登録する。通常リーダは、タグにアクセスするために「質問」コマンドを送る。ただし、このAPFシステム・プロトコルの場合、タグは、タグID番号と暗号化データである「応答」コマンドをリーダに送る。タグからの応答メッセージは、リーダに対し、タグ内のデータを復号し読み取るためにAPFデータベースから復号キーを取得するよう指示する。正規のリーダはAPFデータベースに登録されているリーダであるため、正規のリーダのみが復号キーを取得してタグ内の暗号化されたデータを復号する。

各タグは、その固有のID番号とキーをAPFに登録する。

タグの記憶情報への不正アクセスを防ぐために、タグの記憶情報に対するアクセス制御を決める必要がある。前述のとおり、図3では、各タグは固有のID番号と復号キーをAPFデータベースに登録する。これは不正リーダからのタグの保護に必要である。タグがその固有のID番号と復号キーをAPFに登録すると、未登録のリーダは、タグ内の情報の復号キーなしでタグ内のデータにアクセスすることはできない。したがって、登録されたすべてのリーダは、タグ内の記憶データにアクセスする復号キーを取得する前に認証されることになる。以下では、認証されたリーダがタグ内の記憶データにどのようにアクセスするかについて述べる。

さらに、すべてのリーダはそのID番号をAPFに登録し、リーダがタグ内のデータにアクセスする復号キーを要求する前にそのリーダを認証させるようにする。つまり、すべてのリーダはその固有のID番号をAPFに登録し、APFは、リーダが特定のタグ内の暗号化データを読み取るためにリーダに復号キーを取得する前にその登録状況を確認するのである。

図4に示すように、すべてのリーダはその固有のID番号をAPFに登録する。リーダとタグの双方がそのID番号をAPFに登録するため、

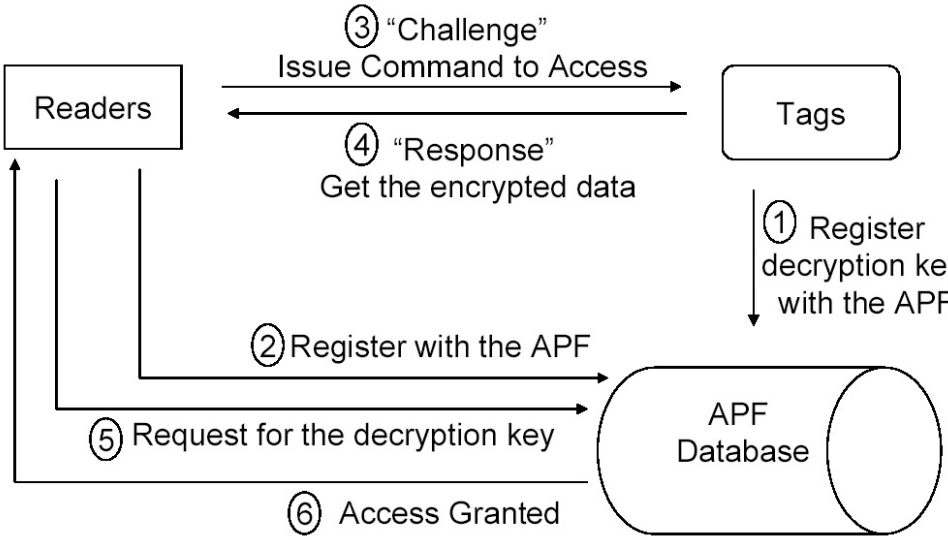
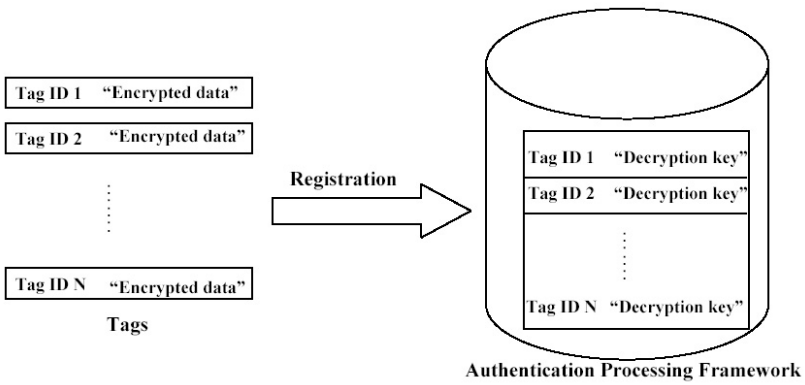


図2 APF フレームワークの流れ



Each transponder registers its unique ID number and key with the APF

図3 APF におけるタグの登録

相互認証が行われ、ユーザの抱える問題の一つである不正リーダからのタグ内情報保護が可能になる。つまり、APF システムを実装し使用することにより、タグへの無許可のアクセスを防ぐことができるのである。以下では、リーダの APF への登録とタグへのアクセス管理について説明する。

以上では、タグの固有の ID 番号と復号キーの APF への登録について説明した。また、タグ内の情報にアクセスする前のリーダの APF への登録について説明した。リーダがタグに「読み取り」コマンドを送ると、タグはその ID 番号と暗号化データを返す。すなわち、データは暗号化され、APF に登録されたリーダがこの暗号化データに必要な復号キーを取得することができる。キーを受け取ると、タグ内のデータを読み取ることができる。このフレームワークには二つの重要なプロセスがある。まず、リーダとタグを認証する相互認証が APF によって行われることである。そして、タグに記憶されたデータを不正リーダから保護するため、プライバシー問題が保証されることである。リーダがタグから取得した情報は暗号化されるため、情報にアクセスする復号キーを APF から受け取らない限りその情報は読み取ることができない。

また、図 5 に示すように、特定のタグに対する未登録リーダは、そのタグ内の情報にアクセスできない。例えば、図 5 では、リーダ 2 はタ

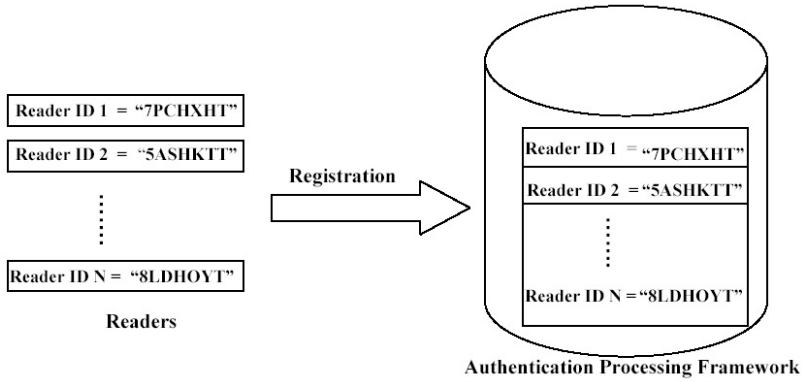


図4　APF におけるリーダの登録

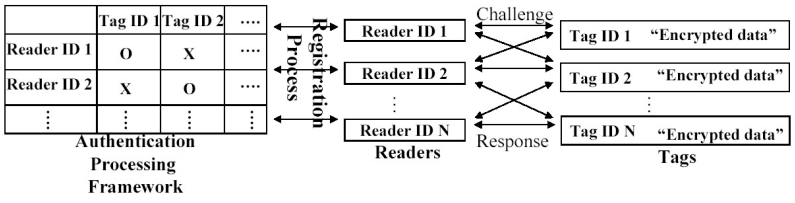


図5　リーダの APF への登録及びタグへのアクセス管理

グ 1 へのアクセスを登録していないため、リーダ 2 はタグ 1 内の情報にアクセスする復号キーを取得することができない。リーダ 1 はタグ内の情報にアクセスするよう APF に登録しているため、タグ 1 にアクセスする復号キーを取得することができる。また、リーダ 1 は、タグ 2 内の情報にアクセスするよう APF に登録していないため、タグ 2 にアクセスする復号キーを取得することができない。リーダ 2 は、タグ 2 内の情報にアクセスするよう APF に登録しているため、タグ 2 内の情報にアクセスする復号キーを要求することができる。

4　結論

以上で述べたような APF システムの認証手順は、不正リーダによる不正アクセスからのタグの保護を可能にする。また、不正（無許可）アクセスを防止するため、タグに記憶されたプライバシー及び機密情報の漏えいの防止にも不可欠である。さらに、以上のフレームワークでは相互認証を行うため、無許可のリーダによるタグ内の情報へのアクセスを防止するシステムを作成する。APF 認証処理フレームワークは、こうした目的の達成に必要な優れた手順であると考えられる。

参考文献

1 J.D.Gerdeman, RFID Radio Frequency Identification Application 2000, Research Triangle Consultants, Inc., 1995.

2 Alain Berthon, “Securityi n RFID”, http://www.nepc.sanc.org.sg/html/techReport/N327.doc July 27th 2000

3 Liu Dingzhe et al, Pretty-Simple Privacy Enhanced RFID and Its Application 2003.

4 Juels Ari et al, The Blocker Tag, Selective Blocking of RFID Tags for Consumer Privacy 2003, http://www.rsasecurity.com/rsalabs/staff

Ayoade John Olurotimi
情報通信部門セキュリティ高度化グループ専攻研究員　Ph. D.
情報セキュリティ

滝澤　修（たきざわ　おさむ）
情報通信部門セキュリティ高度化グループ主任研究員　博士（工学）
コンテンツセキュリティ、非常時防災通信

中尾康二（なかおこうじ）
情報通信部門 セキュリティ高度化グループリーダー
情報セキュリティ技術