3W-05

学生証とパスワードの二要素認証を無線 LAN 接続の認証に用いる手法

仲野　弘一† 大平　健司‡ 谷岡　広樹‡ 佐野　雅彦‡ 松浦　健二‡ 上田　哲史‡
徳島大学　工学部†　　徳島大学　情報センター‡

1. はじめに

大学や企業などの大規模な組織では無線 LAN を組織内ネットワークに導入し運用を行っている．その際に組織内外からの不正接続を防ぐ技術として WPA/WPA2 エンタープライズによる認証が使われている．WPA/WPA2 エンタープライズは認証サーバとネットワーク制御を行うオーセンティケータ，クライアント PC で認証を行うためのプログラムであるサプリカントの 3 つで構成されており，認証サーバが認証を行わなければクライアントは内部ネットワークに接続を行うことができない．

認証に使われるプロトコルである EAP にはクライアントを認証する方法として入力されたユーザ名とパスワードを認証するユーザ名/パスワード方式とクライアントに事前にインストールされた電子証明書を用いて認証する電子証明書方式の 2 種類に大きく分けられる．一般的に高度なセキュリティが求められるネットワークにおいては電子証明書方式が採用されている．

上記で述べた 2 つの認証方式は単一の認証要素のみしか利用しておらず，パスワードや電子証明書の窃盗がアカウントの窃盗に繋がる．本稿では大学や企業で身分証に用いられている非接触 IC カードを用いて無線 LAN 接続で 2 要素認証を行う手法と認証システムについて提案する．

2. 従来手法

非接触 IC カードの通信の規格である NFC(Near Field Communication)を用いて無線 LAN 接続における相互認証の研究が行われている[1]．これは電子証明書方式で公衆無線 LAN 接続にする際に，サービス利用者を正しい登録サイトへ誘導するための手法として NFC を用いている．手法として，公衆無線 LAN におけるサービス利用者を登録する際に，NFC タグをスマートフォンで読み取り登録サイトへ誘導する．
登録作業を行った後に，電子証明書をダウンロード･インストールし，相互認証を実行している．この認証システムは NFC を認証に用いているが，NFC タグ自体は認証要素として用いられておらず，電子証明書単一の認証要素としているため，前項で述べた課題は解決していない．

また学生証を認証の一要素に用いる研究として，複数の大学で学生証等に用いられている IC カードを利用し，認証基盤システムを構築･運用している[2][3]．これは特定の Web サービスに対しての認証やクライアント端末へのログインを対象としており，基本的に認証システム全体が信頼できる通信路上に存在していることが前提となっている．しかし，無線 LAN における認証では認証情報を送信可能な信頼できる通信路が存在しておらず，二要素の認証情報を安全に送る手段が存在しない．

3. 提案手法

3.1 カードに格納する情報と格納方式

現在多くの大学や企業で身分証として使われている非接触 IC カードには大きく(1)カード固有の製造番号などの書き換え不可な識別データが格納されたデータ領域，(2)管理者が設定したカード鍵でのみ書き込み･読み込みの制御が可能なデータ領域の 2 つに分けられる．提案手法は(2)の領域に認証毎に書き換わる値(One-Time-Value)とユーザ識別情報を格納する．

3.2 認証情報の通信手順

提案システムにおける認証プロセスにおいて流れる情報を図 1 に示す．

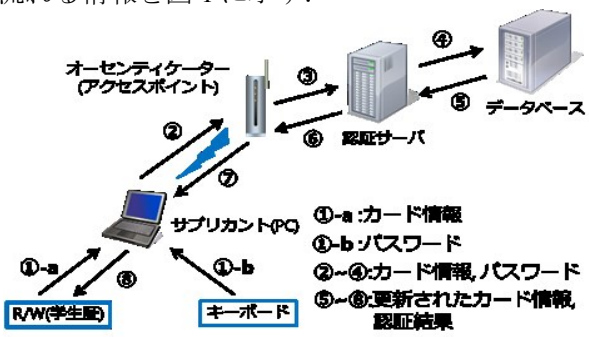

図 1. 提案システムにおける認証情報の流れ

1.　サプリカントは IC カードアクセス API を利

A method of two-factor authentication with a student ID card and a password to WLAN client authentication
†Hirokazu Nakano
†Tokushima University

用してカードリーダライタ(R/W)にかざされた学生証からユーザ識別情報と One-Time-Value を，キーボードからは入力されたパスワードを取得する．

2. 取得した情報を元にデータを加工し，認証サーバへ送信する．送信データを図 2 に示す．

ID = IC カードから取得したユーザ識別情報

PWD = HASH(password + One-Time-Value)

password ：入力したパスワード
HASH：ハッシュ関数

図 2. 送信データの詳細

また認証に用いる通信路は EAP-TTLS，EAP-PEAP のいずれかを用いる．

3. 認証に成功した場合，クライアント端末は認証サーバへ新たな One-Time-Value 生成の HTTP リクエストを行い，認証サーバは新たな One-Time-Value の生成を行い，HTTP レスポンスをクライアントへ送信する．その後データベース内の PWD を更新する．ハッシュを受け取ったクライアントは R/W を通して学生証の One-Time-Value が格納された領域を更新する．クライアントからの One-Time-Value 生成リクエスト及びレスポンスは SSL や TLS で暗号化された通信路で行う．

3.3 認証情報の初期値の設定手順

まず IC カードによる二要素認証を行う利用者は無線 LAN サービス管理者へ学生証に初回の認証に必要な One-Time-Value の格納とパスワードの登録の申請を行う．管理者は One-Time-Value をランダムに生成し学生証に書き込む．同時に無線 LAN 認証情報管理データベースにユーザ識別情報，パスワード，及び図 2 の生成手法によって生成された PWD を登録する．その後，認証サーバのデータベースへユーザ識別情報，PWD を登録する．

4. 評価実験

また，提案手法の実装において使用したソフトウェアやハードウェアデバイスなどを表 1 に示す．

表 1. 使用したソフトウェアなど

システム構成要素	使用ソフトウェア等
認証サーバ	FreeRADIUS 2.2.8
データベース	MySQL 5.7.16
クライアント OS	Ubuntu 16.04
サプリカント	wpa_supplicant 2.6
IC カードアクセス API	PC/SC Lite 1.8.14
カードリーダライタ	ACR1252
IC カード	MIFARE Classic 1K

実装において FreeRADIUS が認証に利用する認証用データベースと One-Time-Value，PWD の生成と更新に用いる更新用データベースの 2 つを用意した．更新用データベースを更新した後に認証用データベースと同期させることで提案手法を実現した．ハッシュ関数は SHA-256 を用いた．

5. まとめ

本稿では無線 LAN 接続における二要素認証の手法として，学生証等に用いられている非接触 IC カードを認証要素に加えた認証を行う手法を提案した．学生証は基本的には所持が義務付けられており，また他の多要素認証デバイスのように持ち運びなどに負担がかからないが，別途 R/W を用意してもらう必要がある．学生証を紛失した場合，無線 LAN サービス管理者側で該当ユーザの識別情報と One-Time-Value を失効させることで不正利用への対策が行える．NFC のエミュレート機能を搭載した携帯電話などによる学生証の偽装による不正利用もカード鍵で格納された領域を用いることで単純な読み取り可能データのみでは不正利用できないようにした．

運用面での課題としてはクライアント端末と R/W 間の通信は暗号化されておらず，キーロガー等でパスワードと One-Time-Value が傍受された場合，不正ユーザが認証に成功してしまうと正規ユーザの認証がそれ以降行えなくなる為，別途対策を行う必要がある．また全ての IC カードで同一のカード鍵を用いることから，カード鍵の流出は重大なセキュリティインシデントを引き起こすため，管理者が厳重に管理しておく必要がある．

利便性を高める為に Web ブラウザからの利用申請やパスワードの更新等を行えるようにプラグイン等の開発が挙げられる．

参考文献

[1]延ほか：“L-005 NFC を利用した公衆無線 LAN 相互認証(L 分野：ネットワーク･セキュリティ，一般論文)”，情報科学技術フォーラム講演論文集，2014，13(4)，pp.113-118
[2]松川ほか：“広島大学電子計算機システムにおける IC カード身分証の利活用”，研究報告インターネットと運用技術(IOT)，2011，3，pp.1-6
[3]河野ほか：“岡山大学事務情報システムにおける Shibboleth との連携を考慮した多要素認証の導入”，研究報告インターネットと運用技術(IOT)，2014，5，pp.1-6