無線ホットスポットサービスのセキュリティ

清水 渉, 小林 稔幸
早稲田大学大学院理工学研究科
情報科学専攻 後藤滋樹研究室

概 要 : 近年無線 LAN を利用したホットスポットサービスが各地で始まっている。多くのユーザにネットワークのコネクションを提供することになるが、当然盗聴やなりすましなど不正利用の防止といったセキュリティ対策が必要になる。しかし現在行われているサービスの多くは、チャンネルさえわかればすべての通信内容を受信できるという無線 LAN の特性を考慮していないものであり、サービスを展開するには危険である。本論文ではいくつかの実際に行われているサービスにおけるなりすましの方法を検証し、実証実験を行う。

Security of Wireless HotSpot Service

Wataru Shimizu, Toshiyuki Kobayashi
Information and Computer Science
Graduate School of Science and Engineering
Waseda University

abstract : Recentry, Hotspot services with wireless LAN system are starting over and over. They offer network connections to many users at the same time. It is necessary to defend unjust access for extending services. However, current wireless LAN system has security problems. For example, if even a channel understands, whoever can receive all contents of the communication. And both terminals don't make sure communication partner each other. Most of current services are dangerous because they are not be thought those problem. This paper is going to consider improvements and perform actual experiment.

1 まえがき

近年 IEEE802.11b を中心とした無線 LAN 製品が普及しつつある。それに伴い、無線ホットスポットサービスというサービスが登場した。ホットスポットサービスとは、喫茶店やファーストフード、駅や空港など人が多く集まる場所に無線 LAN 技術を用いてインターネットへのコネクティビティを提供するサービスである。

無線 LAN の規格は徐々に定まりつつあるが、そのセキュリティに関しては安定した規格がまだ存在しない。無線 LAN のセキュリティとして現在いくつかの方法が普及しているが、これらのいずれの方法にも問題が存在し、安全とは言えない。多くのホットスポットサービスではこれらの技術を組み合わせたり応用することによってサービスを提供して

いるが、そのセキュリティレベルは低いと言わざるを得ない。本論文では具体例を挙げながら実証実験を行い、そのセキュリティについて検証する。

2　無線 LAN とセキュリティ問題

無線 LAN では、 Access Point (以下 AP) というデバイスを介して通信を行う。しかし AP のネットワーク上の仕組みはマルチポートリピータと同じである。即ち、一人のユーザがネットワーク上に流した情報は、そのセグメントに接続している全ユーザが受け取ることができる。有線ネットワークにおいては、マルチポートリピータの利用は物理的に制限されており、マルチポートリピータとケーブルを管理しておけば第三者がネットワークに触れることはできない。しかし無線 LAN の AP では、物理的な制限が極めて少なく、その電波を受け取ることができる場所であれば、そのネットワーク上に流れる情報を簡単に盗聴できることになる。

無線 LAN における通信において、利用者を特定するために一部の事業者が用いているのは ESS-ID, WEP, MAC アドレス認証の 3 つの方法である。まず ESS-ID は元々セキュリティ保持のための技術ではなく、電波の解析によって割り出すことができる。 WEP は信号から鍵を計算することができるというセキュリティホールが見つかっている [1]。そして MAC アドレス認証はパケットに MAC アドレス情報が含まれているため、これを読み込んで偽装することによって通過が可能となる。

また、 ESS-ID 及び WEP は AP に接続してコネクションを確立するために必要な情報であり、AP はこれらの情報を複数同時に使用することは難しい。従って多くのユーザが 1 つの AP に接続するホットスポットサービスでは、これらの値を共通の値にせざるを得ない。

3　ホットスポットサービス

ホットスポットサービスは無線 LAN 技術を用いてユーザにコネクティビティを提供するというものである。このサービスを提供するために解決しなければならない課題は以下の通りである。

- あらかじめ登録した複数のユーザに平等にコネクティビティを提供する
- サーバ側がコネクションとユーザの情報を 1 対 1 に結び付けて管理する
- 第三者もしくは他のユーザに通信内容を盗聴されないようにする
- 第三者もしくは他のユーザがコネクションを利用できないようにする

4　A 社のサービス例

4.1　認証方式

A 社のホットスポットサービスをユーザが利用するにあたり、必要となる手順は以下の通りである。

- ユーザがクライアント端末に ESS-ID 及び WEP キーを設定 (この値は全ユーザ共通)
- 正しい ESS-ID 及び WEP キーが設定されたクライアントに対し、 AP が仮の IP アドレスを割り当て
- ポート番号 80 番に対して何らかのアクセスがあった際にポリシールーティングによって SSL 対応の認証ページへ誘導
- RADIUS によって認証を行う。ユーザは ID とパスワードを入力し、コネクション確立

4.2　セキュリティ問題

A 社のサービスにおいて、コネクションを確立するまでの手順でセキュリティ上の問題は見られない。しかし接続後においては、内容が暗号化されないまま通信を行うことになる。そのため、正しい ESS-ID 及び WEP キーが設定された端末であれば通信内容を盗聴することが可能となる。この 2 つの情報は全ユーザ共通の値であるため、一度でも A 社のユーザとして加入した者は知り得る情報である。

ここで読みとられるのはパケットに含まれる全情報であり、サーバ・クライアントが通信相手を一

意に識別するための情報もここに含まれる。A 社のサービスにおいて、クライアントが保持する一意な情報は IP アドレス・ MAC アドレスの 2 つである。前述の通り、この 2 つの情報は暗号化されないまま無線リンクで流れることになる。そしてこの 2 つの情報は悪意のあるユーザは簡単に偽装することができる。

また、ホットスポットサービスにおいて、ユーザが接続を明示的に切断することなく利用を止めることは珍しいことではなく、その前後に悪意のあるユーザが接続性を確保すれば、そのユーザは完全に接続性を乗っ取ることが可能となる。また、被攻撃側端末に近い位置で妨害電波を出すことによって、意図的に被攻撃側端末の接続を切断させることも可能となる。

更に、このような方式の場合、 AP の成りすましをされる危険性もある。悪意のある第三者が、事業者が提供する AP が用いるものと同一の周波数チャンネル、 ESS-ID 及び WEP キーによって通信を行うことができる AP を設置した場合を考える。ユーザがサービスを利用しようとした際に、電波状況によってこちらの AP に接続してしまう。このとき、事業者の認証サーバが出力する認証画面と同一のものをこの第三者が出力した場合、ユーザはその画面が事業者のものでないことを知る術がない。そのためユーザは認証を行うためにユーザ ID・パスワードを送信してしまう。この瞬間、悪意のある第三者はユーザ ID・パスワードの取得に成功する。

4.3 実証実験

実験は通常通りの利用を想定した PC (以下被攻撃側端末) と不正利用を想定した PC (以下攻撃側端末) の 2 台を用いて行った。なお、実験では正規にアカウントを登録された利用者の正当な利用権を用いた。

まず被攻撃側端末が通常通り認証し通信する。攻撃側端末は ESS-ID と WEP キーを設定し、 tcpdump を用いて被攻撃側端末の IP アドレスと MAC アドレスを得る。この IP アドレスと MAC アドレスで偽造を行うだけで攻撃側端末と同様に接続性を確保することに成功した。

5 B 社のサービス例

5.1 認証方式

B 社の無線ホットスポットサービスにおけるユーザ認証には MAC アドレスと PPPoE が用いられている。正規ユーザはユーザ登録時に無線 LAN カードの MAC アドレスを登録しユーザ ID、パスワード、 ESS-ID を得る。ユーザ ID とパスワードはユーザ固有のものだが、 ESS-ID は全ユーザが共通で用いる値である。利用時には指定された ESS-ID を用いて AP にアクセス、そのそのうえで PPPoE を用いてサーバにアクセスし認証を行ってから利用する。

5.2 PPPoE [2]

PPPoE は PPP[3] をイーサネット上で行うものである。イーサネットのフレームを図 1 に示す。ク

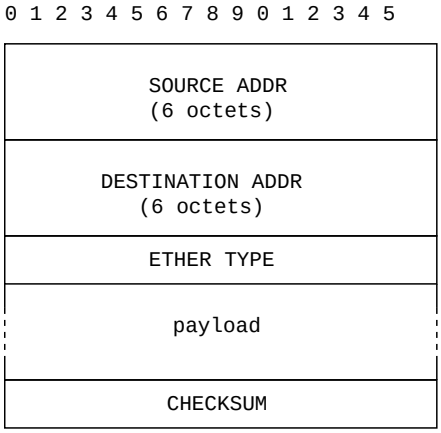

図 1: イーサネットフレーム

ライアントはまず PPPoE の開始を求めるパケットをブロードキャストする。サーバがこれに応えると PPPoE のセッションが確立される。ここで SessionID というそのセッション固有の値が与えられる。これは送信元 MAC アドレス、宛先 MAC アドレスとともにセッションを識別するものであり、これらが異なるパケットは無視される。 PPPoE のフォーマットを図 2 に示す。 ETHERTYPE には

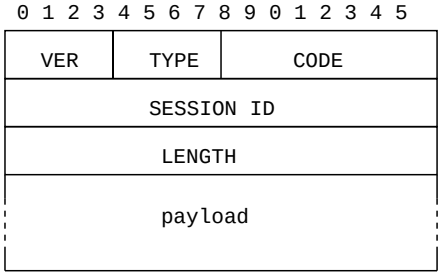

図 2: PPPoE フォーマット

PPPoE セッション確立前には 0x8863、確立後には 0x8864 が入る。

PPPoE のセッションが確立されると PPP の通信が始まる。 PPP はパケットサイズやオプションの利用の交渉、ユーザ ID とパスワードの認証、 IP アドレスや DNS サーバの通知を行い、それらが無事に終わると実際の通信が始まる。 PPP のヘッダはプロトコルタイプのみであり、 IP パケットの場合は 0x21 が入る。つまり PPP の通信が確立し IP パケットが送られる際は、イーサネットヘッダ、 PPPoE ヘッダ、 PPP ヘッダ、 IP パケットの順で送られる。

5.3 セキュリティ問題

B 社の方式では PPP の通信が確立した後、 PPPoE サーバが通信相手を識別するために用いる情報は IP アドレス、 MAC アドレス、 SessionID の 3 つであり、これらの値によってサーバ側は通信相手を識別する。しかし、無線 LAN 上ではチャンネル (周波数) が判明すれば、他の情報を解析し通信中の全端末の全ての通信内容を受信することができるので、これら 3 つの情報を得ることは難しくない。

つまりデータ送信においては送信元 IP アドレス・送信元 MAC アドレス・ SessionID、受信においては宛先 MAC アドレスを被攻撃側端末と同じ値を設定すれば誰でも正規クライアントになりすましてサービスを利用することができる。

5.4 実証実験

実験は A 社の場合と同様に 2 台の PC を用いて行った。 2 台とも正規のアカウントとして登録されたものである。被攻撃側端末は Windows XP Home Edition、攻撃側端末は FreeBSD 4.4–Release を用いた。

まず被攻撃側端末が通常通り認証し、通信する。攻撃側端末は tcpdump を用いて被攻撃側端末の通信を解析し被攻撃側端末と AP の MAC アドレスと IP アドレス、 SessionID を得る。それらを用いて送信データの送信元 IP アドレス、 MAC アドレス、 SessionID を偽装し、宛先 MAC アドレスが AP になるように設定する。受信データは宛先が偽装した MAC アドレス (被攻撃側端末の MAC アドレス) のものだけ受信するようにする。その結果攻撃側端末が通信コネクションを確立することに成功した。

6 まとめ

無線 LAN システムのセキュリティには多くの問題があげられている。従来の技術に他の技術を組み合わせることによって、認証時のセキュリティ問題は克服されている。しかし無線 LAN 上では認証後のパケット情報が第三者に読みとられてしまうため、通信中にセキュリティ問題があることが確認された。これらは全ての通信が傍受できる、という無線 LAN 特有の事情により起こるものであり、無線 LAN では有線のような接続開始時のみの認証ではなりすましを防ぐことは困難である。ユーザ認証を強化した新規格 IEEE802.1X にも既存のコネクションの乗っ取りや認証プロセスに割り込んでの設定中のアクセス情報の取得が可能であるという問題点が指摘されている [4]。無線ホットスポットサービスでセキュリティを確保するためには個々のパケット単位での認証をする必要があると考える。

参考文献

[1] http://airsnort.sourceforge.net/

[2] L. Mamakos, K. Lidl, J. Evarts, D. Carrel, D. Simone, R. Wheeler, “A Method for Transmitting PPP Over Ethernet (PPPoE)”, RFC2516, 1999.

[3] W. Simpson, “The Point-to-Point Protocol (PPP) ”, RFC1661, 1994.

[4] Aruesh Mishra, Wiiliam A. Arbough, “An Initial Security Analysis of the IEEE802.1X Standard”, http://www.cs.umd.edu/˜ waa/1x.pdf, 2002.