モーバイル環境におけるユーザ認証とセキュリティシミュレータ*

2T－7

石川 睦　田窪 昭夫　渡辺 尚　水野 忠則†

静岡大学情報学部‡

1 はじめに

NotePC や PDA の普及によりモーバイルコンピューティング環境、つまり「いつでもどこでも」コンピュータが利用できるという環境が急速に整いつつある。しかし、このような環境では、既存のネットワークになかった様々な問題が生じる。

本研究では、モーバイルコンピューティング環境におけるユーザの認証に関する問題をとりあげ、認証モデルの提案を行う。また、ユーザ認証のプロトコルの評価を行うためのシミュレータについて説明する。

2 モーバイルコンピューティング環境

固定計算機環境では、計算機は常時ネットワークの管理下にあり、ユーザは登録されている計算機のある場所に出向いて計算機、ネットワークを利用する。また、そのサービスはそのネットワークに登録されているユーザのみが利用できる。

一方、モーバイルコンピューティング環境では、ユーザは計算機を持って移動し、モーバイル端末は一時的にネットワークからの切断が行われる。このことは、計算機、ユーザがネットワーク管理下から一度離れることを意味する。そこで、ユーザが再度ネットワークへの接続を行う場合、ユーザは自分の身元を示し、それが確認される必要がある。

このような接続をサポートするため、移動計算機からの接続要求を受け、ユーザの確認をする役割を果たすモーバイルサーバを本モデルでは導入する。

モーバイルユーザが移動してネットワークに接続する場合のパターンは二通り考えられる。

(1) 自分の登録されているネットワークへの接続
(2) 手近なネットワークのモーバイルサーバに接続し、そこを経由してネットワーク上の計算機を利用する場合

3 登録モーバイルサーバへの接続

この場合、ユーザはそのネットワークに登録されている。したがって、モーバイルサーバはユーザの情報、例えばパスワードなどを参照する事が出来る。従って、ユーザの認証を行うためには、通常と同様にユーザは自分の ID 、パスワードを示せば良い。

*Authentication of Mobile Computing Environment and Security Simulator

†Mutsumi Ishikawa, Akio takubo, Takashi Watanabe and Tadanori Mizuno

‡Faculty of Information, Shizuoka Univ.

4 非登録モーバイルサーバへの接続

移動計算機からネットワークへのアクセスには、移動性などの点から携帯電話のような無線通信が使われることを考えなくてはならない。この無線通信をネットワーク接続に用いる場合、通常の有線ネットワークと比べ、

(1) 低速でかつ低品質である
(2) 接続コストが高い
(3) 盗聴されやすい

などが問題になる。そこで、無線通信の利用を極力減らすため、モーバイルユーザが手近な自分が登録されていないモーバイルサーバに接続し、そこでユーザ認証を行いネットワークの利用を可能にする方法を考える。

この場合、接続されたモーバイルサーバはユーザ情報を参照することが出来ない、また、パスワードなどの情報を別のネットワークに流すべきではない [?]。

そこで、ID や パスワードの情報を転送せず、ユーザと接続先のモーバイルサーバ、ユーザが登録されているモーバイルサーバ間で何らかの情報をやりとりすることによりユーザ認証を行うプロトコルを提案する。

5 ユーザ認証のモデル

モーバイルユーザ (MU) は、出先のモーバイルサーバ (LMS) に対して自分の身元を明かさなければならない。また、LMS は MU の登録されているモーバイルサーバ (HMS) と通信を行い、その身元を確認する。

この時、ホストのなりすましなどを考えると、通信相手が目的の相手である事を確認することが必要になる。また、経路上でのデータの盗聴や改竄の危険性を考慮すると、重要な情報は通信相手にしかわからない形で暗号化などを行って送ることを考えねばならない。

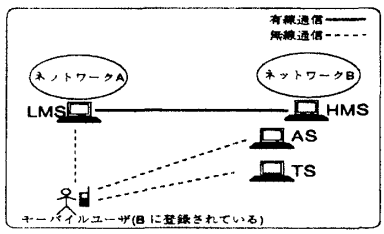

図 1: モーバイルユーザ認証モデル A

そこで、Kerberos [?] に見られるような第三者認証を行うための認証サーバ (AS)、チケットサーバ (TS) を導入する。MU は AS,TS と通信を行う事によって LMS との仮接続権を得てユーザ認証に関する情報を LMS を経由して HMS とやりとりする事で認証を行う。

しかし、このモデルの場合、無線通信を多用するため認証にかかる時間やコストの面で不利である。また、有

線通信に比べると無線通信はより盗聴しやすいことを考えると、セキュリティの面からの不安もあるそこで、ユーザ認証に無線通信を極力しないように次のようなモデルBを提案する。

このモデルでは、モーバイルユーザからのリクエストを受け、AS, TS への通信を LMS が代行する。これによって無線通信を減らす事ができる。

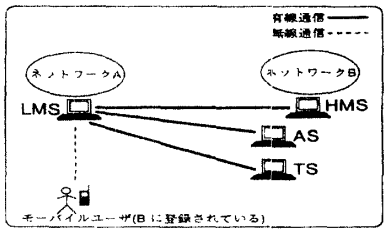

図 2: モーバイルユーザ認証モデル B

6 セキュリティシミュレータ

このようなモデルにおいて考えられるセキュリティの脅威は、(1) 情報の盗聴 (及び、リプレイアタック)、(2) 情報の改竄、(3) 情報の横取り (情報が届かないようにする)、(4) 各計算機自体の悪意、(5) 別の計算機によるなりすまし、などに分類できる。こういった攻撃に対して今回提案したプロトコルの問題点を調べるため、非形式的な検討は既に行った [?]。

しかし、このような方法では人間の思考に頼らざるを得ず、計算機で自動化することは難しい。また、完全に全てのセキュリティの脅威に対応できたことを検証できたかどうかも確かめることはできない。

そこで、BAN logic のように、数学的な手法でセキュリティの安全性を証明する方法がいくつか提案されている [?, ?]。このような方法の場合、プロトコルの完全性を数学的に証明でき、計算機による自動化も可能であるのでプロトコルの完全性を示すのには適している。

しかし、プロトコルのロバストネス、つまりそのプロトコルがどの程度の攻撃にまで耐えられるのか、どの部分が弱い点なのか、などプロトコルの強度を評価するのには適さない。

認証のプロトコルに関する攻撃としては、先に挙げたようにいくつかのパターンに分類することが出来る。

また、ユーザ認証のプロトコルで各計算機が行う動作は、受け取ったメッセージや既に自分が持っている情報などに対して暗号化 / 復号化、内容の確認などを行うことによってメッセージを作成し、それを送信するということである。これらの動作も一般化し、いくつかの基本動作に分けることができる。

そこで、プロトコルに従ってユーザ認証の動作をシミュレートするプログラムを作成し、そこに上であげたような攻撃を発生させるモジュールを組み込むことを考える。つまり、正常な動作に対して攻撃をシミュレートするわけである。

この場合、プロトコルの完全性は証明できないが、プロトコルに対して攻撃を加えた時にどのような動作をするのか、どのような問題が発生するのか記録し、プロトコルの強度、弱点などを検討することが可能になる。

一つの例として、

(1) A → S: A, B, N_A
(2) S → A: $\{N_A, B, K_{AB}, K_{AB}, A_{K_B}\}_{K_A}$
(3) A → B: $\{K_{AB}, A\}_{K_B}$
(4) B → A: $\{N_B\}_{K_{AB}}$
(5) A → B: $\{N_B - 1\}_{K_{AB}}$

というプロトコルをシミュレータに与えると、このプロトコルの動作とそれに対する攻撃をシミュレートし、どのような攻撃が生成され、認証プロトコルの動作がどのようになったかが出力される。

```
Attacker to B  :(Replay) {Kab[5],A}Kb    Success on B
B to A         :         {Nb[5]}Kab[5]   Success on A
A to B         :         {Nb[5]-1}Kab[5] Success on B
Auth Compleate : (Replay)
```

図 3: シミュレータの出力例

上のプロトコルの場合、例えば (3) で送られたメッセージが攻撃モジュールによって再送されても認証が成功してしまうという結果が得られる。この結果から、上のプロトコルではその部分を補強する必要がある事が判断できる。

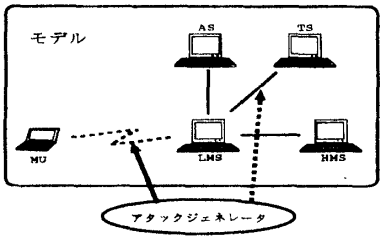

図 4: 認証プロトコル検査シミュレータ

参考文献

[1] R. Molva, D. Samfat and G. Tsudik "Authentication of Mobile Users" *IEEE Network*, March/April 1994

[2] J. Kohl, B. Neuman, "The Kerberos Network Authentication Service(V5)" rfc1510, Oct. 1993

[3] M. Burrows, M. Abadi and R. Needham "A Logic of Authentication." ACM Trans.Computing Systems, vol. 8,pp 18-36, February 1990

[4] J. Glasgow, G. MacEwan and P. Pananageden "A logic for Reasoning about Security." ACM Trans. Computing Systems. vol. 10, no. 3 pp. 265-310. 1992

[5] 石川 睦, 田窪 昭夫, 渡辺 尚, 水野 忠則: モーバイルコンピューテイング環境におけるユーザ認証方式とその評価, 情報処理学会研究報告, 情処研報 Vol.96, No.MBL-2, pp.13-18(1996.10)