移動計算環境におけるユーザ認証に関する研究

氏名・(本籍)	田　窪　昭　夫 (神奈川県)
学位の種類	博　士　(工　学)
学位記番号	工博甲第　171　号
学位授与の日付	平成10年 3 月21日
学位授与の要件	学位規則第4条第1項該当
研究科・専攻の名称	電子科学研究科　電子応用工学
学位論文題目	**移動計算環境におけるユーザ認証に関する研究**
論文審査委員	(委員長) 教授　浅井秀樹　　教授　水野忠則 教授　福田　明　　教授　市川　朗 助教授　渡辺　尚

論文内容の要旨

ネットワーク、形態型端末の技術進歩の結果、従来の計算機が固定設置された固定計算環境(FCE)に加えて、計算機を携行して人の移動と共に計算環境が移動する移動計算環境(MCE)が可能になってきた。FCEでは、計算機の設置と共にネットワーク自体も固定されるが、MCEでは、無線を利用して何時でも誰でも誰とでも、利用者と利用する場所を特定しない環境になっている。従ってMCEでは新たな課題として、正当な利用者であることをネットワークに入る前に確認しなければならない。本論文は、MCEにおけるユーザ認証に関して、MCEモデル、ユーザ認証プロトコルGMAP、プロトコル検証シミュレータSS／AGを提案し考察した。

本論文は全6章から成っている。第1章では本研究の背景、目的を述べた。第2章では本研究に関連する従来の研究動向を述べた。最近のパソコンの小型軽量化、および、ネットワーク技術、とりわけ携帯電話、無線技術の進歩の結果として、MCE環境の考え方が一般的になってきた。従来からのFCE環境で研究されてきた課題は、そのままMCE環境に敷延することの可否については、まだまだ議論の残るところである。ユーザ認証については、従来からFCE環境を基本にしたUNIXベースのネットワークでの研究が活発に行われてきたが、常時ネットワーク接続された計算機を前提にしたFCEに代わって、必要に応じてネットワークに接続するMCE環境においては、ネットワークに入る時点において、正当なユーザであることが確認されなければならない。

第3章ではMCE環境におけるユーザ認証の観点から、従来のFCE環境の外挿として、MCE環境のモデルを提案した。FCE環境の場合、利用者はネットワーク接続され、かつ、常時ホストに補捉された

端末に赴き、ログイン操作によるホスト計算機にアクセスする。一方、モーバイルユーザが携行する移動端末は、通常はネットワークに接続されておらず、必要に応じて逐次移動端末に備えられた無線機能を利用してネットワークに接続する。更に直接目的のホストに接続するのではなく、まず最寄りのサーバに無線接続し、自分が登録された目的のホストに接続を託する。この場合ユーザは登録先の目的ホストを指定することなく、単にユーザ識別子をサーバに伝えるだけで、サーバがユーザ識別子から簡単に接続先のホストを割り出せるような、ユーザ識別子方式を提案した。

第4章では、MCE環境モデルの上で、ケルベロス方式を基本に、電子パスポートを用いた新たなユーザ認証プロトコルGMAPを提案した。このユーザ認証方式では、第三者からの攻撃を考慮して、認証に係わる情報を少なく抑えられている。本研究のモデルでは、モーバイルユーザは最寄りのサーバにシングルホッピングにより直接無線接続し、その後はマルチホッピングで一般的に固定ネットワーク上の複数のサーバを経由して、目的のホストに接続される。ケルベロス方式の考え方によれば、モーバイルユーザと最寄りのサーバの間で認証局、チケットセンタを利用した第三者認証が行われるが、ここではモーバイルユーザの電子パスポート方式を提案し、無線通信の間での情報量を少なく抑えている。固定ネットワーク上での各サーバ間では、ケルベロス方式により、サーバの認証が行われ、モーバイルユーザの電子パスポートが安全に中継されて、目的のホストに先送りされる。最終的にホストで電子パスポートによるモーバイルユーザの認証が行われる。メッセージの暗号化には公開鍵方式を使用し、モーバイルユーザの電子パスポートは、モーバイルユーザの秘密鍵で暗号化したものに、更にホスト公開鍵で暗号化を施すが、モーバイルユーザとホストとの特別な関係を考慮すれば、公開鍵方式による二重暗号化に伴う解読不能問題を回避できるように、予め両者の公開鍵と秘密鍵を設定することが可能である。

第5章では、外部からの第三者攻撃に対するユーザ認証プロトコルの安全性を確認するために、プロトコルシュミレータSS／AGを作成し、ユーザ認証プロトコルの耐攻撃性(ロバストネス)の評価を概括した。まず、プロトコルを構成する基本メッセージである、当事者同士で交信されるメッセージに着目し、メッセージの暗号化による静的な安全性の確認を行い、各メッセージの組み合わせによるプロトコルの動的な安全性について考察した。SS／AGは、プロトコルの構成するメッセージを1文ずつプロトコルバッファから取り出して解析するプロトコルアナライザ部と、第三者による攻撃をシミュレートするアタッカ部から構成される。

第6章では本研究成果の応用分野への展開、今後の研究課題を述べた。本研究によるプロトコルシミュレータの改良を重ね、プロトコルのロバストネスを定量的に把握するための指標を導出し、より安全なプロトコルを設計するための環境に供する。

論 文 審 査 結 果 の 要 旨

ネットワーク、携帯型端末の技術進歩の結果、従来の計算機が固定設置された固定計算環境(FCE)に加えて、計算機を携行して人の移動と共に計算環境が移動する移動計算環境(MCE)が可能になってきた。FCEでは計算機の設置と共にネットワーク自体も固定される。これに対し、MCEでは無線を利用するために、利用者と利用する場所が特定されない。従って、MCEでは正当な利用者であることをネットワークに入る前に確認するユーザ認証が重要な課題になる。本論文は、MCEにおけるユーザ認証に関して、MCEモデル、ユーザ認証プロトコルGMAPを提案し、その特性をプロトコル検証シミュレータSS／AGを作成して考察している。

本論文は全6章から成っている。第1章では本研究の背景、目的を記述している。第2章では本研究に関連する従来の研究動向を整理している。

第3章ではMCE環境におけるユーザ認証の観点から、従来のFCE環境を拡張して、MCE環境のモデルを提案している。モーバイルユーザは、必要に応じて逐次移動端末に備えられた無線機能を利用して、最寄りのサーバに接続し、自分が登録された目的のホストに接続を託する。本章では特に、ユーザが単にユーザ識別子をサーバに伝えるだけで、サーバがユーザ識別子から簡単に接続先のホストを割り出せるような、ユーザ識別子方式を提案している。

第4章では、MCE環境モデルの上で、ケルベロス方式と電子パスポートを用いた新たなユーザ認証プロトコルGMAPを提案している。モーバイルユーザは最寄りのサーバに直接接続し、その後は固定ネットワーク上の複数のサーバを経由して、最終的に目的のホストに接続する。固定ネットワーク上での各サーバでは、ケルベロス方式により、サーバの認証が行われ、モーバイルユーザの電子パスポートが中継されて、目的のホストに転送される。最終的にはホストで電子パスポートによりモーバイルユーザの認証が行われる。

第5章では、外部からの第三者攻撃に対するユーザ認証プロトコルの安全性を確認するために、プロトコルシュミレータSS／AGを作成し、ユーザ認証プロトコルの耐攻撃性の評価を行っている。メッセージの暗号化による静的な安全性の確認を行い、各メッセージの組み合わせによるプロトコルの動的な安全性について考察している。

第6章では本研究成果の応用分野への展開、今後の研究課題を総括している。

以上の成果は、今後も発展し続ける計算機ネットワークにおいて重要なユーザ認証分野を中心にした工学的分野に対して多大な価値を持ち、博士(工学)の学位を与えるものにふさわしいと認定する。