ユーザ属性情報にもとづいたアクセス制御方式

1S－3

宮崎 博　　鮫島 吉喜
日立ソフトウェアエンジニアリング(株)

1. はじめに

一般企業においてもLANの導入が進み、ネットワークを介したデータのやり取りが行われるようになった。しかしネットワーク上を流れるデータは通常、平文のままなので盗聴や改竄の恐れが常にある[1][2]。そのため機密性を必要とする情報の送信に用いるには問題がある。また、企業内での情報アクセスは個人名だけでなく所属部署や担当業務といった属性情報によって制限することが多い。従って一般的に使用されている個人・グループ名とパスワードの組み合わせによるアクセス制御では、異動があるたびにパスワードの変更が必要となるなどパスワード管理が繁雑になる。

そこで本研究では企業内LANを念頭に置き、ユーザがネットワーク上のアプリケーションサーバにアクセスしようとした時にユーザの個人名や属性情報を認証してアクセス制御を行い、要求した情報を暗号化して通信するシステムを提案する。これらの機能をネットワーク上で動作するアプリケーションに提供するため、トランスポート層へのインタフェースであるバークレーソケットに実装する。

2 アクセス制御

企業における情報アクセス管理は、人事情報であれば社員の上長や人事部の人間しか参照・更新ができないというように、個人に対してではなく所属部署や担当業務などの属性情報に対して行うのが一般的である。また、どのような属性を持つ者に対してアクセスの許可を与えるのかは、会社内や部・課内の規則で一元的に定めるのが普通である。従ってネットワークを介した情報のアクセスにおいてもこれらの方法を適用するのが好ましい。このような場合に適したアクセス制御ポリシーとしてRole-Based Policyがある[3][4]。本研究では役割に相当するものとして所属部署、役職、担当業務を考え、それぞれについてユーザをグループ化してグループ毎にアクセス権の設定を行う。この際、ユーザは複数のグループに属していても良いとする。

実際のアクセス制御は以下のように行う。アプリケーションサーバ(AS)ごとにアクセス権をACL(Access Control List)で記述し、それぞれのACLをアクセス制御サーバに持たせる。アクセス制御サーバを設けるのは、アクセス制御を一元的に行うためである。ユーザはASにアクセスを要求する際に自分の属性情報も一緒に送り、ASは受け取った属性情報をアクセス制御サーバに転送する。アクセス制御サーバは、後述する方法で認証したユーザとその属性情報、ASに対応するACLを参照してアクセスの可否を決定する。

3 通信データの暗号化と認証

本研究では、秘密鍵証明書と属性証明書を導入し、秘密鍵暗号方式による鍵交換、相互認証を実現する[5]。ユーザは自分の秘密鍵を含んだ秘密鍵証明書と属性情報を含んだ属性証明書を持ち、ASも自分の秘密鍵を含んだ秘密鍵証明書を持つ。秘密鍵証明書と属性証明書はKDC（Key Distribution Center）が発行し、改竄防止のためにKDCの秘密鍵で署名する。なお秘密鍵証明書

Access Control based on User Attribute
Hiroshi Miyazaki, Yoshiki Sameshima
Hitachi Software Engineering Co., Ltd.

に含まれるユーザやASの秘密鍵は漏洩防止のためにKDCの秘密鍵で暗号化しておく。KDCはユーザとASの認証を行い、またアクセス制御に伴うデータの送受信回数を増加させないためにアクセス制御サーバを兼ねるとする。

セッション確立後に用いる暗号鍵DEK (Data Encryption Key) の交換と相互認証はユーザがアクセス要求を発した時に同時に行う。以下に述べるプロトコルではリプレイアタックに対抗するためチャレンジデータを含める。

(1) ユーザはランダムに生成したDEKとアクセス要求をユーザの秘密鍵K_uで暗号化し、秘密鍵証明書と属性証明書を添えてASに送る。

(2) ASはユーザのアクセス要求を更に自身の秘密鍵K_{AS}で暗号化し、ユーザの秘密鍵・属性証明書と自分の秘密鍵証明書を添えてKDCに送る。

(3) KDCはK_uとK_{AS}を鍵証明書から取り出し、受信データの復号を行う。この際に両者およびユーザの属性情報を認証する。アクセス要求と認証した属性からアクセス制御を行い、その結果をユーザとAS用にそれぞれの秘密鍵で暗号化する。これらの暗号化データとDEKをK_{AS}で暗号化したものをASに送る。

(4) ASはアクセス制御の結果を確認し、ユーザへのアクセス制御の結果を更にDEKで暗号化する。

(5) ユーザはDEKとK_uで受信データを復号し、アクセス制御の結果を得る。

(6) アクセスが許可されていればその後のデータのやり取りはすべてDEKで暗号化して行う。

4 バークレーソケットへの実装

ソケットレベルで暗号化・認証を行うものとしてSSL (Secure Socket Layer) が提案されている[6]。SSLでは鍵管理方式に公開鍵暗号を用いることを前提にプロトコルが設計されている。独自の拡張を施して鍵管理方式に秘密鍵暗号を用いることもできるが、その場合にはKDCとAS間の通信を含めて認証やDEKの確立のために6回のデータのやり取りが必要になる。この点がオーバヘッドになる可能性があるため、本研究では独自のプロトコルで行うことにしている。

5 まとめ

本研究では企業内LANを前提とした、通信の暗号化・認証・アクセス制御を行うシステムの提案を行なった。企業内での情報管理方式を考慮し、認証をユーザの名前だけでなく所属部署や担当業務などの属性情報でも行い、アクセス制御に利用するようにした。また、ソケットレベルに実装することで、ネットワークアプリケーションに変更を加えずに暗号化・認証・アクセス制御を行なえるようにした。

6 参考文献

[1] CERT : Ongoing Network Monitoring Attacks : Computer Emergency Response Team Coordination Center (1994)

[2] CERT : IP Spoofing Attacks and Hijacked Terminal Connections: Computer Emergency Response Team Coordination Center (1995)

[3] W.Ford : Computer Communications Security : Prentice Hall (1994)

[4] R.Sandhu, P.Samarati : Access Control - Principles and Practice : IEEE Comunications Magagine, 32, 9, pp.40-48 (September 1994)

[5] 鮫島, 宮崎 : 秘密鍵証明書・属性証明書を利用した暗号電子メールシステム : マルチメディア通信と分散処理ワークショップ論文集, 情報処理学会, pp.85-92 (1995)

[6] A.O.Freier, P.Karlton, P.C.Kocher : The SSL Protocol Version 3.0 : Internet Draft, Internet Activities Board (1995)