7G−4

暗号化機能と認証機能を取り入れた遠隔会議システムの構築

高木和幸　中村秀紀　米沢千尋　岡田謙一　松下温
慶應義塾大学

1、はじめに

近年、ネットワークセキュリティに対する関心が高まっているがその実際的な応用面については、理論的なものにとどまっている傾向がある。暗号化の技法はネットワークセキュリティの中心となるもので、現在最も急速に発展している分野の一つでもある。メッセージを暗号化して複合鍵を持っていない者には解読できないようにするという機能は暗号の基本的機能であるが、そこから鍵の配送、相手の認証などの新たな研究課題が生まれており、特に認証に関する研究は活発に行われているのが現状である。

一方、ネットワーク網が発達するにつれて、それにともなう分散的処理に対する研究も現在活発に行われており、遠隔会議システムはその具体的な応用例の一つである。このような会議システムにおいては会議を円滑にすすめるためにはどのような環境を設定すれば良いのかという研究は行われていても、そのセキュリティに関する研究はほとんど行われていない状態である。そこで我々は、会議システムにおけるセキュリティ機能の必要性を議論し、実際の応用例としてＵＮＩＸ上に構築したシステムを提示する。

2、暗号技法

2．1　メッセージの暗号化

現在、基本的暗号法としては、秘密鍵暗号法と呼ばれる暗号鍵を秘密に管理する慣用的なものと、1976年にDiffieとHellmanが考案した公開鍵暗号法と呼ばれるものの二通りが存在する[1]。公開鍵暗号法では、暗号化鍵は公開され、各人は自分宛のメッセージに対する複合鍵のみを秘密に管理することになる。秘密鍵暗号法の代表的なものとしては、ＤＥＳ、ＦＥＡＬ−８などがあり、公開鍵暗号法では、ＲＳＡ、ＲＡＢＩＮ暗号などがある。

2．2　認証技法

メッセージの暗号化を基本機能とするなら、認証機能はもう一つ上位のレベルの機能といえる。通信相手が本当にその本人であるという証明や文章の改変が行われていないという証明が必要なときに使われる機能であるが、なりすましを防ぐためには、公開鍵暗号を応用したものや、ＩＤ情報を利用したものがあり[3]、最近では零知識証明の技法を利用した認証が有名である[2]。

3、会議システムにおけるセキュリティ

3．1　必要なセキュリティ機能

（1）暗号化機能

基本的にネットワークを通じた情報のやりとりは全て暗号化するべきであるので、会議を開くときはその参加者全員が共通に持っている鍵で暗号化を施す。

（2）認証機能

認証はどの方法を採用するにしても手間がかかるので、本当に必要な場合にしか採用しないようにするのが良い。具体的には、以下のような場合がある。

◎　会議を始めるときの参加者に対する本人確認
◎　新たに議題を議長に提案する場合
◎　決議を行う際の本人確認

3．2　高速性

会議システムでは意見の交換が頻繁でしかもリアルタイムに近いことが望まれるので、ネットワークが高速であればあるほど暗号化は迅速に行われなくてはいけない。従って、公開鍵暗号法よりもＤＥＳのような慣用暗号法の方が好ましいことになる。認証に関しても、参加人数が多い程オーバーヘッドが大きくなるので通信効率やの良いものや、計算の速いものが好ましい。ＲＳＡを使った認証では、高速性を満たすことができないので、調停者つきの慣用暗号を用いた認証か、もしくは零知識証明の技法を応用した拡張Ｆｉａｔ−Ｓｈａｍｉｒ法を用いるのが好ましい。

3．3　多重ウインドウ

暗号をかけるか否か、認証を使うか否かをユーザが常に意識するのは煩わしいことなので、目的別のウインドウを設定することにする。基本的には3つのウインドウが必要でそれは以下のようになる。

Implementation of Remote Conference System with Encryption And Authentification Functions
Kazuyuki Takagi, Hidenori Nakamura, Tihiro Yonezawa, Kenichi Okada, Yutaka Matusita
Keio University

（１）認証用ウインドウ
（２）暗号化ウインドウ（認証機能なし）
（３）個人用ウインドウ（暗号機能なし）

認証用ウインドウは議題を設定する役目も果たし、他のユーザとの画面の同一性を図るようになっている。つまり、実際の会議でのホワイトボードの役割を果たすことになる。このウインドウの画面を変えるには、議長もしくは他ユーザの承認が必要となる。暗号化ウインドウではメッセージは無条件に暗号化され、全ユーザに同報される。このウインドウのことをグループウインドウと呼ぶことにする。個人用ウインドウは個人が自分の好きなように情報を整理して参照できるところで、他のウインドウに入って来た情報はこの個人用ウインドウにも無条件に入ってくることにするが、そうしないように設定することも自由である。その場合は、ユーザーはグループウインドウから必要と思われる情報だけを選んで個人用ウインドウに持ってくることになる。その様子を図１に示す。

また、この方法では画面がせまくて困るようであれば、グループウインドウと個人用ウインドウを共用して個人用ウインドウにする方法も考えられる。この場合、個人用ウインドウから単純にメッセージを送ると、他ユーザの個人用ウインドウに暗号化されて送られるようになる。

3．4　メッセージ管理

送られて来たメッセージは文書化して管理することとなるが、実際の会議のように複数の文書をずらしながら見たい場合があると思われるので、同時に二つの文書までは参照できるようにする。理論的には文書のレイアウトはウインドウ内では自由であるべきだが、マシンのオーバーヘッドを減らすために、複数の文書をつなぎあわせて一つの長い文章のようにして管理することとする。ただし、文書と文書の切れ目は管理して、自分が何番目の文書を参照しているのか解るようにし、マウスでクリックすることによってすぐに別の文書に移れるようにする。また、文書の順番の並び換えも自由である。

４、システム構築

我々は以上のような機能を盛り込んだ会議システムの試作版をＵＮＩＸ上で実現した。開発言語はＣ言語でツールとしてはＸ－ＷＩＮＤＯＷ上でのＸ－ＶＩＥＷを使用した。実際の通信を行うプログラムについてはソケットベースの低次元言語でプログラミングを行った。また、ウインドウの数についてはとりあえず個人ウインドウとグループウインドウを共用させた２個のものを構成したが、この形態が使いにくいようであればウインドウの配置や数についてさらに検討を加える。

５、今後の展望

今後は試作システムの完成度を高め、新しい機能を盛り込んで評価を行う予定である。

参考文献

１、W.Diffie and M.E.Hellman:"New direction in cryptography",IEEE Trans. inform. Theory, Vol.IT-22,No6,1976.11.
２、A. Fiat and A. Shamir:"How to Prove Yourself: Pratical Solutions to Identification and Signature Problem", Proc. of Crypto'86,1986,5.
３、A. Shamir:"Identity-based cryptosystems and signature schemes", Proc. of Crypto'84, Lecture Notes in Computer Science 196, Springer Verlarg,1985

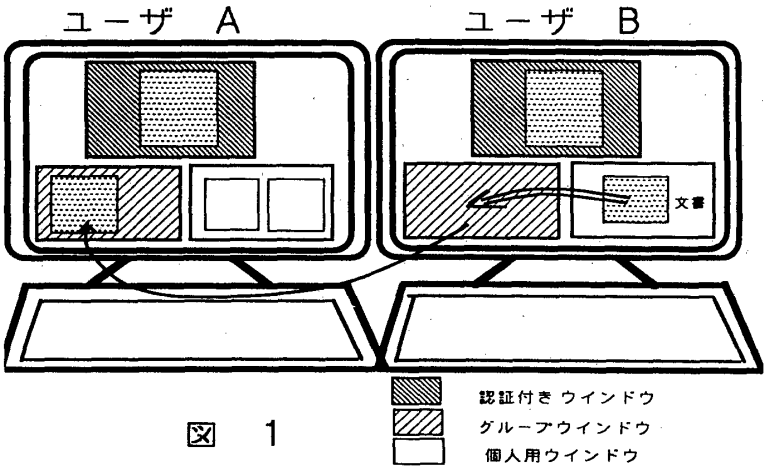

図　1