鍵管理不要な暗号化ファイル転送システム － Secure-ftp －

7K－4

中川　和美，岡本　隆司，桜井　幸一
三菱電機(株)情報システム研究所

1　はじめに

インターネットで標準的なファイル転送システムでは、送受信間で転送されるデータはすべて生のままであり、ネットワーク上の盗聴者が簡単にデータを盗聴することが可能であった。また、ユーザ認証においても、受信側にユーザのパスワードがそのまま転送されるため、ネットワーク上の盗聴者が不当にユーザのパスワードを入手して、ユーザに成り済ますことが可能であった。

これらの問題を解決するための一方法として、Kerberosシステム[1]が提案されており、徐々に利用され始めている。しかし、このシステムを利用するためには、安全な認証サーバの設定等の前提条件だけでなく、システムすべてのサービスを一括してKerberos対応化しなければならないという問題点があり、既存の環境にうまく溶け込めなかった。

そこで、

- 転送データの機密性を保つ
- 盗聴者による不正な成り済ましを防止する

と共に、

- 既存システムとの互換性を保つ

ことが可能な暗号化ファイル転送システムSecure-ftpを開発したので、ここに報告する。

2　Secure-ftpの特徴

本システムの特徴を以下に述べる。

- パスワード転送なしのユーザ認証
  零知識対話証明[2]を用いることにより、パスワードを転送することなく、ユーザ認証を行なう。これにより、ネットワーク上の盗聴者が、ユーザのパスワードを不正に入手し、ユーザに成り済ますことを防止する。
- 転送データの暗号化
  送受信間で転送するデータをすべて暗号化する。これにより、ネットワーク上の盗聴を防止する。
- データの暗号化／復号のための鍵管理不要
  送受信間で転送するデータを暗号化／復号するための鍵を共有鍵とし、二重暗号化方式[3]を用いて暗号化し、送信側から受信側に配布する。共有鍵は毎回ランダムに作成する。これにより、鍵管理を不要とする。
- Internet Draft準拠の暗号化データ転送プロトコル
  暗号化データの転送プロトコルは、ファイル転送プロトコルの標準規格であるRFC959[4]にセキュリティ機能を拡張したInternet Draft[5]に準拠している。これにより、既存のファイル転送システムとの互換性を保ち、オープンなシステムに対応する。即ち送信側或いは受信側が既存のファイル転送システムを用いている場合、鍵配布や転送データの暗号化／復号を行なわず、また、ユーザ認証には従来の方式を用いてファイル転送を行なう。これにより、既存システムとの互換性を保つことができる。

3　Secure-ftpの仕組み

3.1　構成

本システムの構成を図1に示す。

本システムを起動すると、まずデータの暗号化／復号のための共有鍵の作成および配布が行なわれ、次にユーザ認証が行なわれる。ユーザ認証に成功すると、ファイルの転送が行なわれる。ユーザ認証後に転送されるデータは、すべて共有鍵を用いて暗号化される。

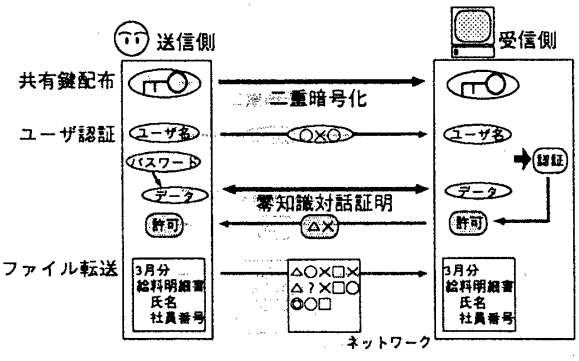

図1: システム構成

3.2　ユーザ認証

ユーザ認証は、零知識対話証明を用いている。零知識対話証明とは、証明者が秘密の情報を明かすこ

Encrypted File Transfer System without Key Management – Secure-ftp –
Kazumi NAKAGAWA, Takashi OKAMOTO, Kouichi SAKURAI
Mitsubishi Electric Corp.

となく、検証者と対話を行ないながらその秘密を知っていることを検証者に対して証明する方法である。

本システムでは、そのうち Fiat-Shamir 法を適用している。この認証手順は [2] と同様の方法を用いている。送信側と受信側での各種情報の交換は、すべて共有鍵により暗号化されて転送される。転送された情報は、受信側により共有鍵を使って復号される。

3.3 鍵配布

共有鍵の配布には、Shamir,Rivest,Adleman による二重暗号化方式 [3] を用いている。配布手順を図 2に示す。

まず、送信側は、共有鍵 K を乱数により作成する。次に、素数 p を用いて、

$$C_{rnd}C_{rec} \equiv 1 \pmod{p-1}$$

となるような乱数 C_{rnd} およびその逆元 C_{rec} を作成する。次に、

$$K_c \equiv K^{C_{rnd}} \pmod{p}$$

となる K_c を受信側に転送する。受信側は、

$$S_{rnd}S_{rec} \equiv 1 \pmod{p-1}$$

となるような乱数 S_{rnd} およびその逆元 S_{rec} を作成する。次に、

$$K_{cs} \equiv K_c^{S_{rnd}} [= (K^{C_{rnd}})^{S_{rnd}}] \pmod{p}$$

となる K_{cs} を送信側に転送する。送信側は、

$$K_s \equiv K_{cs}^{C_{rec}} [= ((K^{C_{rnd}})^{S_{rnd}})^{C_{rec}} = K^{S_{rnd}}] \pmod{p}$$

となる K_s を受信側に転送する。受信側は、

$$K \equiv K_s^{S_{rec}} [= (K^{S_{rnd}})^{S_{rec}}] \pmod{p}$$

より、共有鍵 K を受けとる。

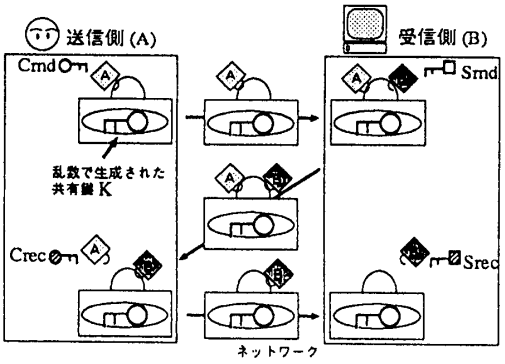

図 2: 鍵配布

3.4 ファイル転送

ファイルは共有鍵により、暗号化される。暗号化されたファイルは、Internet Draft に基づいて、base64 表記化されて転送される。受け取られたファイルは base64 表記から暗号文に戻された後、共有鍵によって復号される。

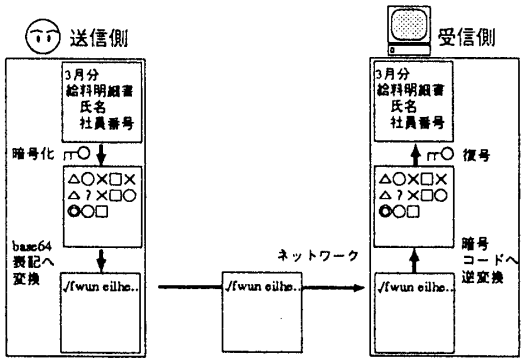

図 3: ファイル転送

4 おわりに

本稿では、今回開発を行なってきた暗号化ファイル転送システム Secure-ftp の特徴、構成および各種原理について述べた。今後は、暗号処理部分の高速化や、パスワードの初期設定および変更その他に対する処理の安全性について検討を加え、更にセキュリティ機能を向上したシステムを考えている。また、今回開発した技術を応用して、コンピュータネットワークサービス全般についての開発も進めていきたい所存である。

参考文献

[1] J.G.Steiner, C.Neuman, J.I.Schiller, "Kerberos: An Authentication Service for Open Network Systems," In Proceedings of the USENIX 1988 Winter Conference, pp.191-202

[2] 小林, 岡本, 桜井, " 零知識証明技術のコンピュータ間認証への適用," 情報処理学会第 44 回 (平成 4 年前期) 全国大会

[3] A.Shamir, R.L.Rivest, L.Adleman, "Mental Poker," MIT Laboratory for Computer Science, Report TM-125, 7 pages, (Feb. 1979)

[4] J.Postel, J.Reynolds, "FILE TRANSFER PROTOCOL (FTP)," RFC-959, (1985)

[5] S.J.Lunt, "FTP Security Extensions," Internet Draft, (1993)

[6] D.W.Davies, W.L.Price, (上園 忠弘 監訳), " ネットワーク・セキュリティ," 日経 BP 社, (1990)