SSH の拡張による FTP のセキュリティ機能の向上

能登研究室　　瀧 智博 (36043)

1　はじめに

FTP(File Transfer Protocol) とは、UNIX マシン間でのファイルの転送を行うためのプロトコルと、またそのプロトコルを用いてファイル転送を行うプログラムのことである。ユーザは FTP を用いることにより、TELNET に基づいた対話的なインターフェースを利用して、ローカルマシンとリモートマシンの間でのファイル転送を行うことができる。

本研究ではそのプロトコルのセキュリティ上の問題点を指摘し、セキュリティ機能の改良について提案する。

2　FTP の仕様とそのセキュリティ

FTP は、ファイル転送の際、以下の 2 つのコネクションを確立する (図 1 参照)。

1. コントロールコネクション
   リモートシステムへのログインやログインに伴うユーザー認証、FTP コマンドやリプライなど、クライアントとサーバ間での制御に関するやり取りを行う。
2. データコネクション
   データが転送される経路になる。

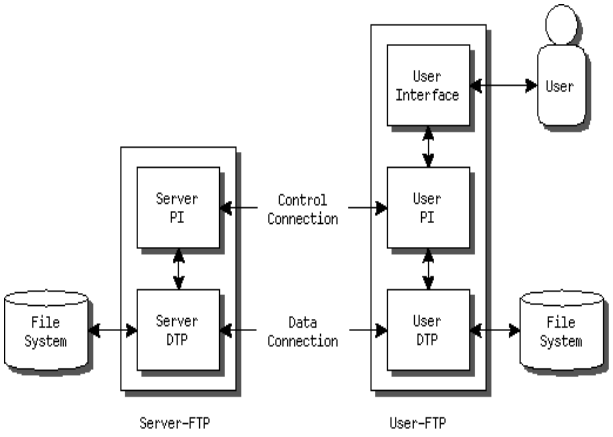

図 1: FTP モデル

現在実装されている FTP では、この 2 つのコネクションは暗号化されない平文でネットワーク上を流れているため、tcpdump 等のネットワークを流れるパケットを監視するツールを用いることにより、盗聴することが可能である。これは、攻撃者による FTP を利用するユーザのパスワードの暴露や、外部秘のデータの漏洩などが起こり得ることを意味する。

3　コネクションの暗号化

現在、ファイル転送の盗聴を防ぐ幾つかの方法が存在し、その中の一つに、SSH (Secure SHell) のポート転送機能を用いたコネクションの暗号化による方法がある。

この方法では、コントロールコネクションポートを暗号化することにより、FTP セッションを確立する際に行われるユーザ認証の為のパスワードや FTP セッションでユーザが入力したコマンド等のコントロールコネクション上を流れる情報の盗聴を防ぐことができる。

しかし、この方法によって暗号化されているのはコントロールコネクションポートのみであり、データコネクションポートは暗号化されていない。そのため、転送データが流れているデータコネクションの盗聴には依然として無力なままである。

本研究では、このデータコネクションの暗号化による FTP のセキュリティ機能の改良を提案する。

4　暗号化の方法

データコネクションにおいても、コントロールコネクションの時と同様に、SSH のポート転送機能を用いて暗号化を行う。しかし、データコネクションの確立はコントロールコネクションの確立よりも複雑な手順で行われているため、データコネクションの暗号化は、コントロールコネクションの暗号化とは異なる方法で行わなくてはならない。

今日利用されている多くの FTP では、一つの FTP セッション内において、複数のデータ転送を可能にするために、それぞれのデータの転送毎に、異なるポートに新しいデータコネクションを確立している。それに対応するため、データコネクションの暗号化は、データの転送毎に確立される異なるポート毎に暗号化を行う。

5　おわりに

FTP のセキュリティ面に関する改良・拡張を提案した。今後はこの仕様の詳細を設計し、その設計に基づいた FTP(Client/Server) を実装する予定である。この仕様が実装されれば、FTP を用いたファイル転送におけるセキュリティがさらに向上し、盗聴を完全に防止することができるようになるであろう。