異なる環境間における安全な通信路の構築

Construction of Secure Network on Different Environment

藤田　憲正 [1)]　　鵜川　始陽 [2)]
松村　晋吾 [3)]
Norimasa FUJITA　　Tomoharu UGAWA
Shingo MATSUMURA

1) 京都大学工学部電気電子工学科（E-mail: nfu @ osk2.3web.ne.jp ）
2) 京都大学大学院情報学研究科（E-mail: foosen @ kuis.kyoto-u.ac.jp ）
3) 京都大学大学院情報学研究科（E-mail: @ ）

ABSTRACT. In these days, Wireless LAN is being popular. However, Wireless LAN is easy to intercept on the characteristic of media. On the other hand, the origin of the application protocol currently generally used is old, and the secrecy nature of data is not taken into consideration at all. As a means to solve this problem VPN is proposed. Although there is a means to realize VPN, mostly, but, finally, as a result of examining various plans, it decided to adopt "PPP over SSH VPN". And since there was no implementation of "PPP over SSH VPN" on Windows environment, we implement it.

1　背景

ここ数年のネットワーク環境の発達はめざましく、いつでも、どこでもネットワークに接続できるユビキタスな環境が構築されつつある。しかし、現在の標準的なアプリケーション層のプロトコルは、いわゆるインターネットの黎明期に作成されたものであり、ネットワークを通じて送受信されるデータの秘匿性は、全く考慮されていない。典型的な例が、POP3 や FTP などであり、これらは、認証情報を含む全てのデータを平文のまま、ネットワークを通じて送受信してしまう。同様に、トランスポート層やネットワーク層のプロトコルに関してもデータの秘匿性は全く考慮されていないと言ってよい。数少ない例外として、ネットワーク層における IPSec があるが、ネットワークの両端が共にこれに対応している必要がある。また、現在一般的な NAT や NAPT（いわゆる IP マスカレード）を越えての通信が困難であるなど、単体では非常に扱いにくいプロトコルである。

最近急激に利用されるようになった無線 LAN は、電波を使うという性質上、非常に盗聴が行いやすく、この上を保護されていないデータを流すことは、現在社会問題となっている重要な情報の漏洩の原因となったり、盗聴した情報を元にした不正アクセスを助長したりすることになりかねない。また、一方では、低価格なブロードバンド・ホームネットワーク環境の普及により、逆にインターネットサービスプロバイダのセキュリティ品質の低下を招き、偶然の事故とはいえ通信内容が他人に傍受されるような事態も起こっている。このような状況では、せっかくのユビキタスな環境を安心して使うことができない。

2　目的

1 章で述べた問題を解決するため、本プロジェクトは、異なる環境間（異なるオペレーティングシステム間、ハードウエアルータ及びパーソナルコンピュータ間等）で安全な通信路の構築を行う。

3　開発内容

（1）方針

1 章で述べた問題を解決するためのアプローチは、いくつか考えられる。例えば、新たに安全なプロトコルを作るというのは一つの方法である。また、既存の安全なプロトコルを安全でないプロトコルとうまく組み合わせることにより、解決できる場合もある。しかし、これらのアプローチではうまく行かないことがある。前者においては、新しいプロトコルが普及することはなかなか難しく、通信相手がそのプロトコルに対応しているとは限らないという問題が、後者においては、どうしても組み合わせることのできない状況が往々にして発生する。そこでこれらの問題を一挙に解決する手段として VPN というアプローチを提案することとする。

現在考えられる一般的なユビキタス環境を考えた場合、クライアントは、Windows 系が多く、サーバは、UNIX 系が多い。そのため、異なる環境間であっても、相互に安全な通信ができることは重要である。しかし、現状では、異なる環境間における VPN を考えた場合、安価に簡単にそれを実現する手段がない。その手段を提供することはユビキタスな環境をよりよくするために必要であると考える。

（2）構成

当初、VPN の実現方法として、次の 2 方式を検討対象としていた。

(a) Windows 系環境で一般的な L2TP/IPSec による方法

(b) UNIX 系環境で比較的用いられる PPP over SSH による方法

これらの長所、短所を総合的に判断した結果、より使え

る状況が多いと考えられる (b) の PPP over SSH による方法を今回の開発対象とした。したがって、サーバ側は、通常の UNIX 系環境で一般的な実装および設定をそのまま利用し、クライアント側は、Windows 用デバイスドライバ及びアプリケーションソフトウエアを実装した。各ソフトウエアの関係は図 1 の通りである。

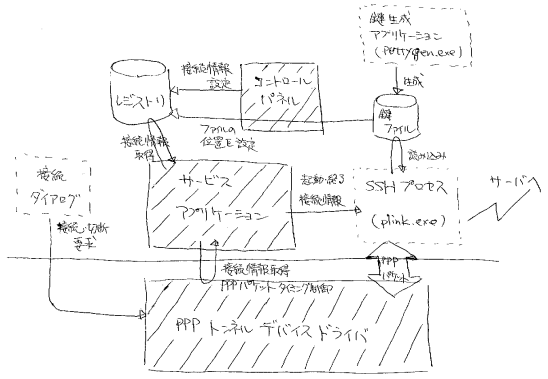

図 1: 成果物の構成 (斜線部が今回実装した物)

PPP トンネルデバイスドライバは、NDISWAN Miniport ドライバとして実装した。SSH サービスアプリケーション及び SSH プロセスとのインターフェイスはデバイスファイルとした。接続ダイアログとのインターフェイスは TAPI となっている。また、Windows の出力する同期 PPP パケットを非同期 PPP パケットに変換する機能をドライバ内に内蔵し、効率の良い動作が可能である。

SSH サービスアプリケーションは、起動時に自動的に実行される拡張サービスとして実装した。PPP トンネルデバイスドライバからの要求に応じて、レジストリから必要な接続情報を取得し、SSH プロセスを起動・終了・接続情報の受け渡し等を行う。また、SSH プロセスの挙動を監視し、必要に応じて PPP パケットの入出力タイミングを制御したり、通信路の切断を監視し PPP トンネルデバイスドライバに通知したりする機能を持つ。

また、接続情報を設定するツールとして、コントロールパネルを用意し、できるだけ簡単に接続の設定が出来るように配慮した。

SSH プロセス及び鍵生成アプリケーションは、既存のフリーな実装 (PuTTY, http://www.chiark.greenend.org.uk/ sgtatham/putty/) を利用している。

さらに、これらをできるだけ簡単に利用できるように、SSH サービスアプリケーション、コントロールパネル、SSH プロセス (plink.exe)、鍵生成アプリケーション (puttygen.exe) をまとめてインストールできるように、専用のインストーラを用意している。PPP トンネルデバイスドライバについては、現時点では、別途インストールする必要があるが、将来的には全てのソフトウエアが 1 度にインストールできるようにする予定である。

これらに関連して、一般に公開するため、現時点では最低限のドキュメントしか用意できていないが、これについても随時作成し、公開していく予定である。

4 評価

本プロジェクトでは以下のような特徴を持つソフトウエアを作成することが出来た。

- 今回作成したソフトウエアは Web Page (http://www.kmc.gr.jp/proj/vpn/) を通じて一般に無料で公開している。高価なセキュリティ関連の機材・ソフトウエアに頼ることなく手軽に安全な通信路を確保することができる。
- PPP トンネルデバイスドライバは、Windows の特徴をうまく生かし、また、極力不要な動作を行わないように設計しており、高速動作が可能である。UNIX マシン間の PPP over SSH に比べて、数分の一のレイテンシを実現できている。さらに、ユーザ空間のアプリケーションとのインターフェイスは、デバイスファイルという形になっており、組み合わせるアプリケーションを変更することにより、別の形態の VPN を実現することも可能である。

当初計画したスケジュールよりも設計・実装が遅れたため、リリースに関する部分ではまだまだ不十分であると認識している。また、一通りの実装は完成しているが、問題点も残されており、今後も適宜開発を続けていく予定である。特にユーザインターフェイスに関する部分は、多くの方に利用して頂くためには重要な部分であり、改善していきたいところである。

5 参加企業及び機関

なし

6 参考文献

なし