KAME プロジェクトにおける IPsec の実装

坂根昌一
横河ディジタルコンピュータ株式会社 情報通信技術センター

1 はじめに

産学共同の KAME プロジェクト (以降 KAME と略す) では、次世代 IP プロトコルである IPv6 と、IP 層でセキュリティを施す IPsec を 4 つの OS 上で開発している。本発表では、KAME における IPsec スタックの実装状況を述べる。

2 実装対象の OS

KAME の IPsec スタックは、現在 BSD/OS3, FreeBSD2.2.8, FreeBSD3.3, NetBSD1.4.1 に実装されている。また BSD/OS4 には別のスタックが組み込まれているが、これを入れ換える形で現在進行中である。OpenBSD2.5 にも IPv4 用のスタックが既に組み込まれている。こちらは今の所 KAME のスタックを組み込む予定は無い。

3 実装の状況

IPsec スタックは、プロトコル制御部、鍵管理部ポリシ管理部、の 3 つの部分に分けられる。

プロトコル制御部は、SA のパラメータに従ってパケットにセキュリティプロトコルを適用する。セキュリティプロトコルは ESP, AH の新旧それぞれを実装済。IPv4,IPv6 ともにトランスポートモード, トンネルモードを実装済である。トンネルモードに関しては、ECN に関する配慮がされている。暗号アルゴリズムは 3DES や HMAC-SHA1 はもちろん、その他多くのアルゴリズムを実装している。MTU の計算や、IPv4 の Fragment bit に関しては実装しているもののテストが必要である。

鍵管理は SA のパラメータを定義する。ユーザ空間から SA のパラメータを設定、削除し、カーネルから SA の要求を受けつける。KAME のスタックでは PF_KEY 第 2 版を実装しているが、一意な SA を定義する部分と、SA の起因者の情報を受渡しする部分に独自の拡張を施している。また、ユーザ空間から PF_KEY を利用するためのライブラリを独自に用意している。SA の粒度はネットワーク単位、ホスト単位、ソケット単位を定義できる。SA を自動設定するためにユーザ空間に IKE の基本的な機能を実装している。

カーネルはパケットを出す時、どのパケットをプロトコル制御部へ渡すか、どの SA を使用するか判断する事ができない。また、パケットが入って来た時に、どの SA が使用されているべきかを検査することができない。ポリシ管理部は、任意のパケットに対するカーネルの挙動を定義し、どの SA をどの順序で使用するか、また使用されているべきかを定義する。ポリシ管理部は独自の実装であり、実験的要素が特に強い部分である。

4 おわりに

本発表では、標準化が進んでいる IPsec の実装状況 IPsec は基本仕様こそ固まりつつあるが、IKE や運用面において、仕様が固まっていないので、今後も開発は継続していく。