7R-2

多機能 IC チップを利用した任意多地点間 VPN のための鍵交換手法に関する研究

Research of Key Exchange technique using IC chip for the On-Demand VPN

兵庫友一郎 [1]　鈴木裕之 [2]　小尾高史 [1]　谷内田益義 [2]　山口雅浩 [2]　大山永昭 [2]

Yuichiro HYOGO[1] Hiroyuki SUZUKI[2] Takashi OBI[1] Masuyoshi Yachida[2] Masahiro YAMAGUCHI[2] Nagaaki OHYAMA[3]

1. はじめに

近年、インターネットを専用線と同様に利用できる VPN サービスが大きな広がりを見せている。しかし、VPN の構築には利用者にネットワークの専門知識が必要なうえ、設定などを間違うと情報セキュリティ上多大な影響が発生する恐れがあるなど、誰もが容易に設置できる状況に至っていない。そのため、現在の VPN 利用方法としては、専門家が直接 VPN 接続機器を操作して VPN の設定をし、接続地点を固定しているのが一般的であり、多地点をダイナミックに接続する VPN の実現は困難な状況である。

このような背景の下、VPN の状態管理を行う VPN 管理機関と 2 階層 PKI に対応した IC チップが搭載された通信機器を用いて、利用者の要求に応じて認証鍵などの VPN 構築に必要な設定情報を、ネットワークを介して安全に配送し[1]、任意多地点間で直ちに VPN を構築するオンデマンド VPN(OD-VPN)技術の研究開発[2]が進められている。

現在の OD-VPN（図１）は、IPsec を利用した暗号通信を行っており、そのための鍵交換手法としては、Pre-Shared Key を利用した IKE（Internet Key Exchange）を用いている。しかし、Pre-Shared Key を用いる場合、同じ通信機器においても VPN 通信路毎に異なる鍵を設定する必要があり VPN 管理機関における鍵管理が煩雑になることや、通信機器が異なる VPN 管理機関に属していた場合の鍵生成・情報共有を実現する手法が明確になっていない等の課題がある。

本研究では、IKE プロトコルで用いられるデジタル署名認証方式をベースとし、機器に組み込まれた IC チップの利用と接続許可証を用いた接続権限管理とを組み合わせた鍵交換手法を提案する。さらに提案手法を用いて、異なる管理機関に属する機器間で容易に鍵交換が実現できることを示す。

所属：東京工業大学（Tokyo Institute of Technology）
1. 総合理工学研究科
Interdischiplinary Graduate School of Science and Engineering
2. 像情報工学研究施設
Imaging Science and Engineering Laboratory

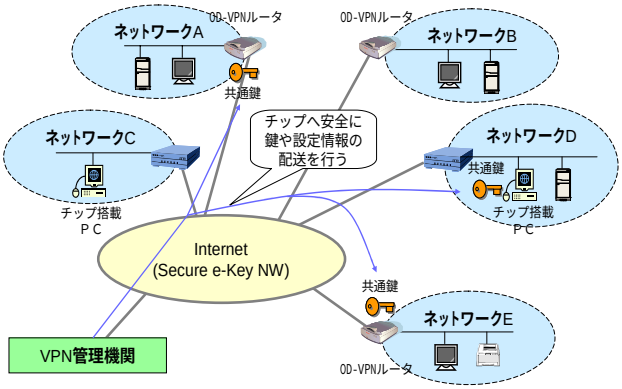

図１．　オンデマンド VPN

2. オンデマンド VPN における従来の鍵交換

ルータ間で IPsec による VPN を構築するためには、機器相互の ID や鍵情報などを用いて IPsec-SA を確立する必要があるので、現在 OD-VPN では、IKE を利用した鍵交換を採用している。また、接続の許可を判断するためのポリシー制御も同時に行う。

接続の際には、まず利用者が VPN 管理機関に対して VPN サービスの依頼を行う。VPN 管理機関は、ルータ等の機器所有者が設定したポリシーを確認し、接続可能な場合は、VPN 接続する二点間の機器の IC チップに対して、IKE のための Pre-Shared Key の配信を行う。この際、VPN 管理機関と IC チップは相互認証を行うとともに、暗号通信により鍵を安全に IC チップに格納する。その後二点間では、設定された情報を用いて IKE を実行する。

IC チップは、機器の認証による正当性保証と Pre-Shared Key の安全な配送にだけ関与し、VPN 構築自体には関与してない。また、Pre-Shared Key を利用した通信では、VPN 通信路毎に異なる鍵が必要となることや、複数の VPN 管理機関間で VPN 通信のローミングサービスを実施する場合の鍵漏洩の危険など、Pre-Shared Key をどのように管理、配送するかが新たな課題となる。

IKE には、公開鍵暗号技術を利用したデジタル署名認証方式があり、これを利用することでこれらの問題を解決することが可能であるが、現在の IC チップの性能や容量を考慮した場合、複数の認証局(CA)の公開鍵証明書の管理・検証を IC チップ上で行うことは困難である。

3. 接続許可証を利用したデジタル署名認証ベースのオンデマンド VPN 鍵交換手法

IKE のデジタル署名認証方式では、VPN ルータ間で IKE 認証を行うために秘密鍵およびそれに対応する VPN 管理機関が発行した公開鍵証明書が必要となる。現在の OD-VPN においては、VPN 接続の可否を VPN 管理機関が制御することになるため、提案手法でも IKE 時に必要となる公開鍵証明書の配送を VPN 管理機関が行うものとする。これにより、VPN 管理機関では鍵ではなく証明書を管理することになるので、安全性確保も容易になる。公開鍵証明書の検証は、各 VPN 管理機関が実施した上でセキュアチャネルを利用して IC チップに配送する。各 OD-VPN ルータ（以下、ルータ）は自らを管理している VPN 管理機関を信頼し、IC チップ上では公開鍵証明書の検証は行わない。その結果、IC チップ上で複数の管理機関の公開鍵証明書の検証を行う必要性はなくなる。

同時に、ルータを管理する VPN 管理機関 A は、ルータ A への接続許可証を発行し、VPN 管理機関 B へ送付し、VPN 管理機関 B から管理下にあるルータ B へ送付される(図２)。この接続許可証により接続許可の判断や異なる VPN 管理機関へのアクセス権限などを制御する。鍵交換時には、ルータ間でさきほどの接続許可証を交換し、接続許可証の内容のチェック及び署名検証を行う。ルータ A 及び B で VPN 管理機関が異なる場合でも、接続許可証の署名検証は自己が属する VPN 管理機関の公開鍵により行うため、それ以外の管理機関の存在を意識する必要はない。

本手法においては、接続許可証として公開鍵証明書に対応する属性証明書を用いる。IKE の Certificate ペイロードあるいは Certificate Request ペイロードを利用して属性証明書を送付すれば、IKE 通信で用いられる ISAKMP パケットの構成と機能をそのまま利用して接続許可証の配布が行えるためである。これにより、既存の鍵交換プロトコルを変更することなく、実現が可能となる。

すでに述べたように、本手法では VPN のための鍵管理を IC チップ上で安全に行うことができるので、VPN 通信全体の安全性向上が期待できる。

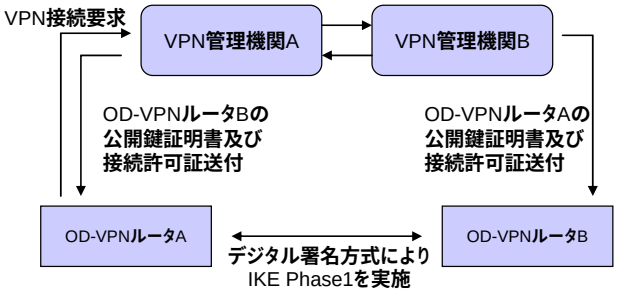

図２． 提案手法

4. 検証システムの構築

提案手法の有効性を確認するために、VPN 構成情報配送後からの IPsec 用の通信路暗号鍵交換部分までについて実装を行った。２台の機器(パソコン)にそれぞれ実際の IKE に則った機能を実装し、提案手法の検証システムを構築した。今回は実装の都合上、ルータ上ではなく機器上にデジタル署名認証機能・接続許可証の送付・検証・権限確認機能等を実現し、シミュレートソフトという形で鍵交換機能を実装した。

この検証システムにおいて接続許可証の検証および記載されている接続権限の確認、さらに VPN 接続で使用する通信路暗号鍵が共有されていることを確認した。

5. まとめ

オンデマンド VPN のための鍵交換手法として、デジタル署名方式による接続許可証を用いて、接続権限管理や異なる VPN 管理機関間での接続を制御する新たな鍵交換手法を提案し、検証した。今後の予定として、接続許可証の権限管理部分の詳細や異なる VPN 管理機関間の通信方法について検討が必要と考えている。なお、本研究の一部は，総務省の委託研究「高度ネットワーク認証基盤技術の研究開発」により行った。

参考文献

[1] 小尾高史　他：「オープンネットワーク環境で安全な鍵配送を実現するネットワーク基盤」,電子情報通信学会(2004)

[2] 釜仲　他：「機器の認証に基づく安全なＶＰＮ構築技術の提案」， 2004-CSEC-27，情報処理学会（2004）