6K-6

ITRON 仕様 TCP/IP プロトコルスタックへの IPsec の実装

小野田　晃久†　　牛丸　真司‡

沼津工業高等専門学校　専攻科†　　沼津工業高等専門学校　電子制御工学科‡

1. 緒言

デジタル家電時代が到来したことにより、組込み機器をネットワークに接続することが多くなりつつあり、通信の安全性のため、セキュリティに関する問題は避けることができなくなった[1][2]。ネットワーク層で通信の暗号化を行う IPsec[3][4]を実装した TCP/IP プロトコルスタックは、既に市販製品が存在するが、ライセンス購入などを必要とするため、その分の製品単価の上昇は避けられない。このことがセキュアなユビキタスコンピューティング環境の普及を遅らせる要因となる可能性がある。

本研究では TOPPERS[5]プロジェクトの中で開発された、ITRON 仕様の TCP/IP プロトコルスタック[6]である TINET[5]に IPsec を実装し、それをオープンソースとして公開することで、組込みシステムにおける暗号化通信の実装モデルをオープンソースコミュニティに提供することを目的とする。

2. 作成したプロトコルスタックの仕様

非 PC 系デジタル機器の多くは、必要最小限のリソースしか持たないため IPsec をそのまま実装することは難しい。そこで、RFC2401 で規定されている IPsec の仕様に制限を設けた IPsec の最小セキュリティ仕様[1]で TINET に実装する。

- 手動鍵交換の機能を有すること。
- ESP 暗号化アルゴリズムと AH 認証アルゴリズムの両方を選択できるようにすること。
- トランスポートモードを実装していること。
- IPsec 無しでも通信できること。
- 自動鍵交換、ESP の認証機能などのオプション機能を追加実装しやすいプログラム構造とすること。
- オープンソースで提供できること。
- 開発プラットフォームは安価で入手しやすいこと。

3. 開発のためのプラットフォーム

3.1. ハードウェア

本研究では TINET がサポートしている AKI-H8/3069F をターゲットボードとした。その概観と主な仕様を、図 1 と表 1 にそれぞれ示す。

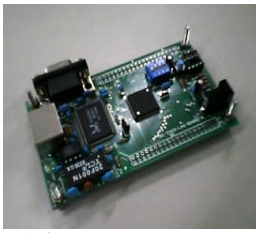

図 1 AKI-H8/3069F

表 1　AKI-H8/3069F

CPU	H8/3069F
メモリ	ROM／512kb RAM／16kb 外部 RAM／16Mb
NIC	RTL8019
システムクロック	20MHz

3.2. ソフトウェア

μITRON4.0 仕様に準拠しており、オープンソースとなっている TOPPERS/JSP カーネル 1.4.1 を搭載し、TINET をベースに IPsec に対応したプロトコルスタックを開発した。

4. 試験及び考察

図 2 のような通信試験環境を構築し、通信試験を行った。

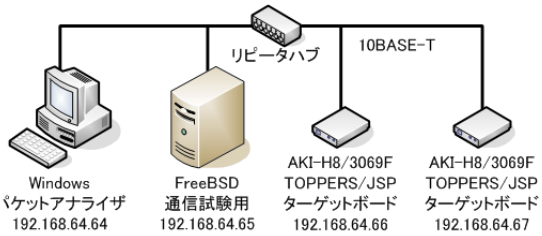

図 2 通信試験環境構成図

4.1. フラグメント化

1500 オクテットを超えた IP データグラムは IP 層でフラグメント化を行うことも可能だが、TINET と FreeBSD のプロトコルスタック間で通信実験を行ったところ、データグラムの再構成の際に分割したうちの後半のパケットが破棄されてしまった。その原因は、後半のデータグラムに IPsec のヘッダ情報が含まれないために IP 層でフラグメント化されたパケットが破棄されてしまったためである。

他のプロトコルスタックとの互換性を保つために、IP 層でフラグメント化を行わず、そのかわりとして、IPsec のヘッダを構成しても通信経路の MTU を超えないように、トランスポート層のセグメント長を調節することとした。

TINET では、config/<cpu_name>/tinet_cpu_config.h 内に MAX_TCP_SND_SEG としてトランスポート層のセグメント長がマクロ定義され

Implementation of IPsec on TCP/IP protocol stack based on ITRON specification.

†Akihisa ONODA: Advanced Engineering Course, Numazu College of Technology

‡Shinji USHIMARU: Department of Digital Engineering Numazu College of Technology

ている。静的に定義されているため、ipsec.h 内に IPsec に必要なオクテット数を IF_IPSEC として定義し、tinet_cpu_config.h に ipsec.h を include した上で、MAX_TCP_SND_SEG に定義されている値から減算するように変更した。伝送効率が若干落ちてしまうが数 10 オクテットのデータであるため、あまり影響は無いと考えてよい。

4.2. 遅延時間

表 2 に、IPsec を用いない通信、AH を用いた通信、ESP を用いた通信で 100 回 ping を用いた通信を行い、プログラムを H8 モニタプログラム上で動作させた場合と H8 上で直接動作させた場合の応答時間の平均値を算出した結果を示す。また、ESP に用いる暗号化アルゴリズムは DES-CBC を、AH に用いるハッシュ関数は MD5 をそれぞれ用いる。同時に、北海道立工業試験場にて TINET に暗号化アルゴリズムとして AES を用いた IPsec の実装が行われた際の試験結果[2]も示す。

表 2 通信の遅延時間

	H8		SH2[2]	H8S[2]
	モニタ上	ROM 、RAM 上		
IPsec 無し	5.9	3.9	1.5	3.8
AH	85.0	30.0		
ESP	134.0	39.2	6.7	22.4

単位：ミリ秒

ESP 化を行う場合と行わない場合で約 20 倍ほどの時間がかかっている。これはモニタを通して実装を行ったためと考えられたので、H8 上に直接プログラムを書き込むことで処理時間が約 2/7 になった。また、ESP による暗号化処理、AH による認証処理にかかる時間が大きい。モニタ上で検証を行っていた際、まれにタイムアウトをおこすこともあった。しかし H8 上に直接プログラムを書き込むことで大幅に通信時間を短縮することができることが確認でき、タイムアウトすることもなくなった。

今回の試験結果と北海道立工業試験場の試験結果との ESP による暗号化にかかる時間の差は、暗号化アルゴリズムの違い、または、CPU の違いと考えられる。SH は H8 に比べ非常に高性能な CPU であるので検討を行わない。H8S は H8 が持っていない乗算器を持っているため、処理を高速に行うことができている可能性がある。

4.3. 自動鍵交換の追加実装

実際に機器に組込んで使用することを考えた場合には自動鍵交換の機能が無い場合、あらかじめ規定したネットワーク以外とは IPsec を用いた通信を行うことができない上、鍵が常に一定では安全性の面でも問題がある。したがって、実際に運用する上では自動鍵交換を実装し、鍵交換を動的に行うことが必要である。

今回の開発では自動鍵交換を行う IKE の実装は行わなかったが、将来的にその機能を組込むことを考慮した実装を行った。IKE は IPsec を利用するプログラムとは独立に動作する必要がある。本研究で開発したプロトコルスタックでは、データベースタスクとして SAD、SPD を管理する機能を独立なタスクとして実装した。このタスクに IKE の機能を実装することで自動鍵交換に対応することができる。

5. 結言

作成した仕様に従った ITRON 仕様の IPsec プロトコルスタックは完成した。現時点では開発ドキュメントのうち、試験関連のドキュメントが完備されていないため公開には至っていない。ドキュメントの作成が完了し次第、WEB サイトを立ち上げ、TINET の差分ファイルとして早急に公開する予定である。

実際に機器に組込み運用する場合、自動鍵交換の機能が必須となってくるため、IKE の実装を今後検討していきたい。

また、今回、機能に関する試験はすべて行ったが、実際に機器に組込み、運用するまでには運用レベルの試験が更に必要となると考えられる。このことについて、今後検討していく予定である。

参考文献

[1] 江崎浩, 井上淳, 岡部宣夫, 佐治木次郎, 宮田宏,神原顕文, 小島富彦：情報家電の相互接続安全技術仕様策定と検証に関する研究開発, 平成 13 年度成果報告集第二版, 情報処理振興事業協会(2001)

[2] 堤大祐, 堀武司, 長内研, 吉川毅, 山本寧：組込みシステム向け TCP/IP プロトコルスタックにおける IPsec, 情報処理学会第 68 回全国大会, 5A-8, (Mar. 2006), pp.1-61 - 1-62

[3] Kent, S., and R. Atkinson："Security Architecture for the Internet Protocol",RFC2401(Nov. 1998)

[4] 小早川智明(著), 西田晴彦(監修)：IPsec 徹底入門, 翔泳社(Aug.2002)

[5] TOPPERS Project：http://www.toppers.jp/

[6] 高田広章(編)：ITRON TCP/IP API 仕様 1.00.01, トロン協会(1998)