C-P34

IPsec を用いた組込み系暗号通信プログラムの研究

苫小牧工業高等専門学校　○岡　　宙，　　阿部　司，　　吉村　斎，　　大橋智志

要　旨

本研究では，LAN で接続されたマイコンボードの通信を保護するため，IPsec を用いた組込み系暗号通信プログラムの研究を行った．通信を暗号化することにより，組込みシステムの通信セキュリティを高めることが出来る．IPv4 用と IPv6 用の 2 種類の IPsec を実装する．さらに，実装した IPsec の IPv6/IPv4 デュアルスタック化を行う．暗号通信を解析した結果，IPv4・IPv6 共に暗号通信に成功した．また，IPv6/IPv4 デュアルスタック化を完了したため，研究成果について報告する．

1. はじめに

現在，ネットワーク接続機能を標準搭載しマイコンを内蔵した製品である ATM，工場の制御装置のような組込みシステムは，種類および量ともに増加し，世界全体に普及している．このような組込みシステムに対する，通信データの盗聴，改竄，なりすましなどの影響は，大きくなっている[1].

これに対応するためのセキュリティプロトコルの一つが，IPsec(Security Architecture for Internet Protocol)である．IPsec は，ネットワーク層のプロトコルであるため，ネットワーク層より上位層で動作する TCP などのプロトコルをまとめて保護することができる．

本研究では，IPsec を用いた組込み系暗号通信プログラムと IPv6/IPv4 混在環境[2]への対応のため，IPv6/ IPv4 デュアルスタックの研究を行う．

2. 研究概要

2.1 開発および実行環境

本研究の開発環境を図-2.1 に示す.

①PC の GDB(The GNU Project Debugger)で動作確認用アプリケーションプログラム(以降，実装プログラム)の転送およびデバッグを行う.

②PC の TeraTerm からマイコンボードの実装プログラムに対して命令コマンドの送信を行う.

③ネットワーク通信は，PC の通信用仮想マシンの FreeBSD とマイコンボード間で通信を行う.

④FreeBSD の setkey コマンドと実装プログラムによって，ネットワーク通信を IPsec で保護する.

⑤PC の解析用仮想マシンの FreeBSD で tcpdump コマンドを用いて，通信用仮想マシン-マイコンボード間の通信解析を行う.

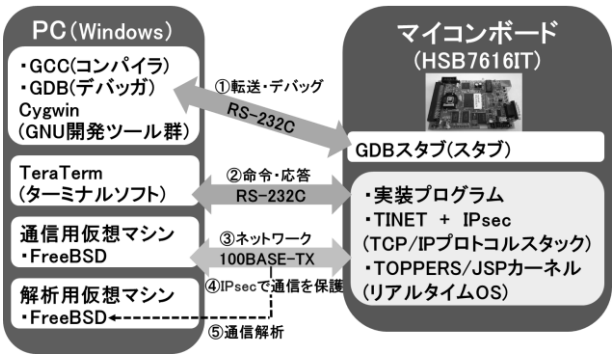

図-2.1 開発・実行環境

TINET と IPsec についての説明を以下に示す.

(1) TINET

TINET[3]は，リアルタイム OS である TOPPERS/JSP カーネルに対応した TCP/IP プロトコルスタックである．また，TINET の利点は，TCP/IP を利用する API が豊富に用意されており，オープンソースである点である．さらに，IPsec のフックが導入されているため，IPsec を TINET に組込み可能である.

(2) IPsec

IPsec は，AH(Authentication Header)，ESP(Encapsulated Security Payload)および IKE(Internet Key Exchange protocol)の 3 つのプロトコルから構成される．本研究では，主にデータの暗号化を行うプロトコルである ESP について研究を行う。また，ESP は，北海道立総合研究機構(以降，道総研)により開発された一部未実装の IPv4 用 ESP モジュール(2.2 より後述)を使用する.

2.2 研究内容

道総研が開発した IPv4 用 ESP モジュールでは，以下のように実装されている.

・暗号化・復号化機能は，実装済みである.

・送信部が，一部未実装である.

・受信部が，未実装である.

このため本研究では，以下を行った.

①IPv4 用 ESP モジュールの送信部･受信部を実装する.

②IPv6 用 ESP モジュールを実装する.

③IPv6/IPv4 デュアルスタック化を行う.

3. 動作確認

3.1 暗号通信の動作確認方法

暗号通信の動作確認方法を図-3.1 に示す.

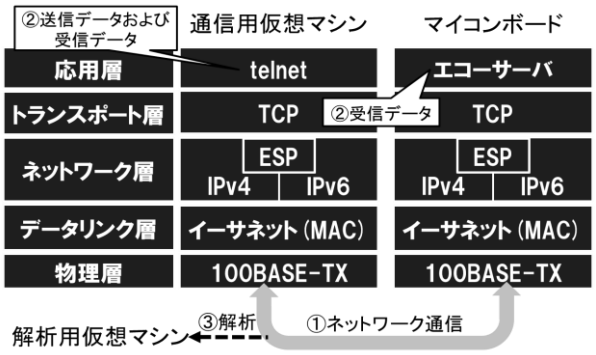

図-3.1 暗号通信の動作確認方法

本稿の解析では，以下の順に動作確認行った.

①通信用仮想マシンからマイコンボードのエコーサーバ(ポート番号 7)に対して telnet 接続を行う.

②telnet 接続後に通信用仮想マシンからマイコンボードへデータを送信し，マイコンボードからの応答を受信する.

③解析用仮想マシンの tcpdump コマンドによって通信結

果を解析する．

※エコーサーバを使用しているため，通信用仮想マシンは，送信したデータと同じデータを受信する．

※ネットワーク通信は，TCP によりコネクション接続を行い，ESP によりパケットの暗号化を行う．

※通信結果の動作確認は，IPv4 による暗号通信と IPv6 による暗号通信について行った．

また，暗号通信時のデータの流れを図-3.2 を示す．

図-3.2 より IPv4 による暗号通信のパケットは，順に IPv4 ヘッダ，ESP ヘッダ，TCP ヘッダおよびデータで構成されている．同様に，図-3.2 より IPv6 による暗号通信のパケットは，順に IPv6 ヘッダ，ESP ヘッダ，TCP ヘッダおよびデータで構成されている．また，TCP ヘッダおよびデータは，IPv4 と IPv6 どちらのパケットも ESP により暗号化される．

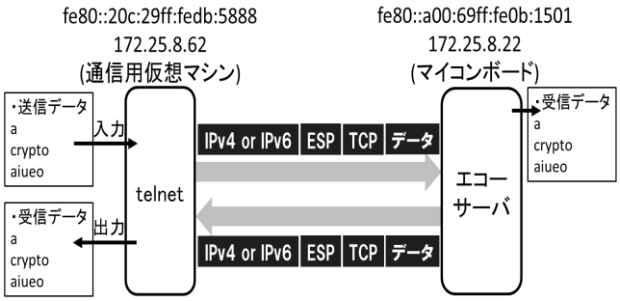

図-3.2 データの流れ

3.2 IPv4 による暗号通信の確認

図-3.2 より telnet 接続後に通信用仮想マシンからマイコンボードへ送信したデータは，「a」，「crypto」，「aiueo」である．マイコンボードの受信したデータは，通信用仮想マシンの送信したデータと一致しており，正しくデータを受信できていることが確認できる． 同様に，図-3.2 より通信用仮想マシンの受信したデータは，マイコンボードの受信したデータと一致しており，正しくデータを受信できていることが確認できる．

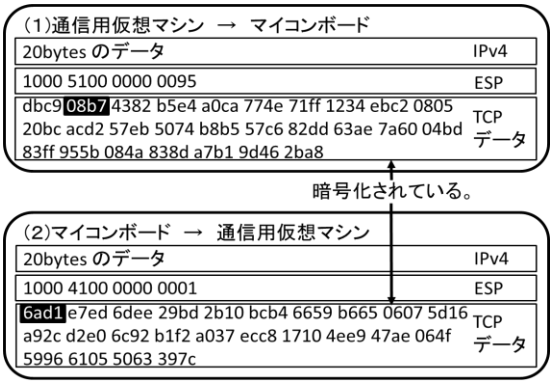

図-3.3 暗号通信の解析結果(IPv4)

また，IPv4 による暗号通信の解析結果を図-3.3 に示す．

図-3.3 より(1)の通信と(2)の通信ともにパケット内に ESP ヘッダの内容が記述されていることがわかる．さらに，(1)と(2)の 2 つの白抜き文字は，マイコンボード内のエコーサーバのポート番号の記述される箇所である．エコーサーバのポート番号は，「0007」である．しかし，(1)と(2)の 2 つの白抜き文字の値は，ランダムな値になっており，暗号化していることが確認できる．

3.3 IPv6 による暗号通信の確認

図-3.2 よりデータの流れは IPv4 による暗号通信と同様であり，正しく通信できていることが確認できる．

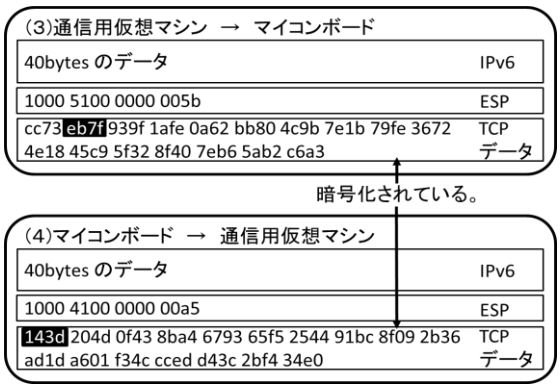

図-3.4 暗号通信の解析結果(IPv6)

また，IPv6 による暗号通信の解析結果を図-3.4 に示す．

図-3.4 よりパケットは IPv4 による暗号通信と同様であり，暗号化していることが確認できる．

3.4 IPv6/IPv4 デュアルスタック化

IPv6/IPv4 デュアルスタック化への対応の確認のため，マイコンボードのネットワークインタフェース情報を確認した．確認した内容を図-3.1 に示す．

図-3.5 より IPv6 アドレスと IPv4 アドレスの両方が割り振られており，IPv6/IPv4 デュアルスタック化へ対応できていることが確認できる．

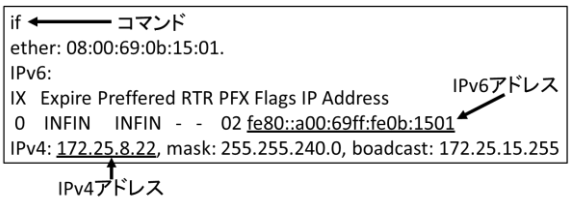

図-3.5 ネットワークインターフェース情報

4. おわりに

現在の本研究の成果を以下に示す．

- マイコンボードと PC 間の IPv4 通信を IPsec(ESP)にて暗号化し，通信を保護するプログラムを実装した．
- マイコンボードと PC 間の IPv6 通信を IPsec(ESP)にて暗号化し，通信を保護するプログラムを実装した．
- 本研究プログラムの IPv6/ IPv4 デュアルスタック化を行った．
- 以上成果の動作確認を完了した．

今後の研究課題を以下に示す．

- 本研究プログラムのソース整理を行う．
- IKE(鍵交換プロトコル)の導入の検討を行う．

5. 研究助成について

本研究は，「総務省北海道総合通信局」様より委託を受けた「ユビキタスサービスプラットフォームに対応した組み込みシステム用 TCP/IP プロトコルスタックとサポートシステムの研究開発」の成果と，貸与されている装置を利用しております．また，「株式会社 I ・TEC ソリューションズ」様からの寄付金の一部を活用しております．

参考文献

[1] 2014 年版 情報セキュリティ 10 大脅威 (pp.37-38，独立行政法人情報処理推進機構セキュリティセンター)

[2] 「IPv6/IPv4 デュアルスタック対応のプロトコルアナライザの研究」(pp. 157-158, 佐々木健一郎, 阿部司, 吉村斎, 大橋智志，情報処理北海道シンポジウム 2013)

[3] TOPPERS プロジェクト TINET とは https://www.toppers.jp/tinet.html