ダウンロード・データあります

ご購入はこちら

パケットづくりではじめる ネットワーク入門

第63回 簡易L2スイッチの認証機能をパスワードに対応させる

坂井 弘亮

本連載はネットワーク上を流れるパケットを直接扱うようなツールを自作しつつ，ネットワークの仕組みを勉強していきます．テーマは「自作」，「現物ベース」，「動く感動」の3つです．ネットワークはイーサネットとIPを想定しています．

今回やること

今回はパスワードをあらかじめ共有し，MD5（Message Digest algorithm 5）によるハッシュ値を利用した認証を行うことで，パスワードを知られることなく実現できる認証機能を実装します．

パスワード対応の認証機能の概要

● ハッシュ値を使って認証する

▶前回の簡易認証機能の問題点

前回実装した認証機能は，クライアント側から認証要求のパケットを送信する際に，パケット中にパスワードを格納し，簡易L2スイッチ側ではパスワードをチェックして認証を行うというものでした．

パスワードは暗号化などされずにそのまま格納されていたため，パケットがキャプチャされればそのパスワードは容易に知られてしまいます．

簡易L2スイッチとクライアントの間では，共通のパスワードを持っていますが，これをそのままパケットに格納するのでなく，なんらかのハッシュ値に変換してパケットに格納すれば，パケットをキャプチャしても，元のパスワードを知られることはありません．

しかし，単にハッシュ値に変換するだけでは，そのハッシュ値自体が使われてしまえばハッシュ値がパスワード代わりとなってしまい，同様の問題が起こります．

▶クライアント固有の値（MACアドレス）を使う

そこで，パスワードのみをハッシュ化するのではなく，パスワードにクライアント固有の何らかの値を付加してハッシュ値を計算することにします．このようにすれば，ハッシュ値自体が知られてしまっても，そのハッシュ値を使って別のクライアントから認証パケットを出したとしても，クライアント固有の値が異なるので，簡易L2スイッチ側ではハッシュ値のエラーを検出できます．

ここではクライアント固有の値に，そのクライアントのMACアドレスを利用します．これにより，ハッシュ値が知られたとしても，パスワードが分からなければ，MACアドレスから正しいハッシュ値を生成することはできません．

● ハッシュ（MD5）値の計算方法

今回はMD5値の計算には，OpenSSLのライブラリを使います．

FreeBSDでは標準でインストールされていますが，CentOS/Debian環境では次のコマンドを実行してパッケージをインストールします．

（CentOSの場合）

```
# yum install openssl-devel
```

（Debian/GNU Linuxの場合）

```
# apt-get install libssl-dev
```

これにより次のファイルがインストールされ，プログラム中でMD5値の計算用のサービス関数を使うことができるようになります．

- ヘッダ・ファイル：`md5.h`
- ライブラリ：`libcrypto.a / libcrypto.so`

リスト1に示すのは，OpenSSLのライブラリを使ったMD5値の計算のサンプル・プログラムです．OpenSSLのMD5ライブラリの使い方は次の通りです．

1. `md5.h`をインクルードする（4行目）
2. MD5_CTX という型で，計算用のコンテキストを確保する（8行目）
3. `MD5_Init()`でコンテキストを初期化する（14行目）
4. `MD5_Update()`でデータを入力する（20行目）
5. `MD5_Final()`で結果を採取する（25行目）

`MD5_Final()`を呼び出すことで，最終的に16バイトのMD5値が取得できます．

リスト1は，次のコマンドでコンパイルし，実行できます．

本連載のプログラムのソースコードは以下の筆者のホームページからダウンロードできます．ライセンスはKL-01というもので，組み込み機器などでも自由に利用できます．
http://kozos.jp/books/interface/ethernet2/