WIDE Technical-Report in 2010

WIDE合宿における WPA 実験

wide-tr-two-wpa-eap-02.pdf

WIDE Project : http://www.wide.ad.jp/

If you have any comments on WIDE documents, please contact to board@wide.ad.jp

Title: WIDE 合宿における WPA 実験
Author(s): 関谷勇司 (sekiya@wide.ad.jp), 大江将史 (masa@fumi.org)
Date: 2010-03-22

WIDE合宿における WPA 実験

関谷勇司, 大江将史

2010 年 3 月 22 日

1　本実験の目的

本実験は、WPA-EAP(WPE Enterprise) と呼ばれる無線暗号化の仕組みを、IEEE802.1x の証明書認証である EAP-TLS と組み合わせて運用することができるかどうか検証するために行った。また、本実験では特別な機材を用いることなく、汎用的な機材のみで WPA-EAP を実現することを目指した。

2　本実験の概要

本実験は、2006 年 9 月に信州松代ロイヤルホテルにて行われた WIDE 研究会会場にて行った。この WIDE 研究会は、参加人数 200 名を超える規模で行われたため、多種の OS、サプリカント、ならびにデバイスを被験者とした実験を行うことができた。さらに、2009 年 3 月の WIDE 合宿、ならびに 2010 年 3 月の WIDE 合宿における経験をもとに、加筆修正した。

本実験で用いた証明書は、moCA WG の発行した個人証明書ならびにサーバ証明書を用いた。認証サーバ用として、radius.camp.wide.ad.jp のサーバ証明書を発行してもらい、これを RADIUS サーバに組み込むことで EAP-TLS に利用した。なお、個人証明書は、moCA WG から WIDE メンバー全員に定期的に配布されているものを利用した。したがって、被験者はこの実験のために新しい証明書を用意することは必要なく、サプリカントの設定のみで実験に参加することができた。

3　実験に用いた機材

本実験に用いた機材は以下の通りである。

無線アクセスポイント

- Cisco Aironet 1130AG シリーズ

認証サーバ

- Turbo Linux Desktop 11 (kernel 2.6.13)
- freeradius-1.1.3

クライアント

- Windows XP SP2
- MacOS 10.4
- NetBSD-current (4.99.1 dated on Sep. 6 2006)
- FreeBSD 6.1
- Linux 2.6 with WPA supplicant
- Nokia E-60 携帯電話

以上の機材にて実験を行った。

4 実験に用いた設定

実験に用いた設定を公開する。なお、各クライアントの設定に関しては、被験者からの報告をそのまま載せており、追加検証は行っていない。

4.1 無線アクセスポイント設定

Cisco Aironet 1130AG シリーズの設定例を、今回の実験に関係のある部分のみ抜粋して図 1 に示す。

```
aaa group server radius rad_eap
 server X.X.X.X auth-port 1812 acct-port 1813

aaa authentication login eap_methods group rad_eap

dot11 ssid twodot1x
   vlan XXX
   authentication open eap eap_methods
   authentication key-management wpa
   guest-mode

interface Dot11Radio0
 encryption vlan XXX mode ciphers aes-ccm tkip
 broadcast-key change 3600
 ssid twodot1x

ip radius source-interface FastEthernetXXX

radius-server attribute 32 include-in-access-req format %h
radius-server host X.X.X.X auth-port 1812 acct-port 1813 key 7 XXXXXXXXXXXX
radius-server vsa send accounting
```

図 1: 無線アクセスポイント設定例

4.2 認証サーバ設定例

認証サーバとして、フリーの実装である freeradius の Version 1.1.3 を用いた。本実験の認証に必要であった radiusd.conf を図 2 に、eap.conf を 3 に示す。

```
$INCLUDE ${confdir}/eap.conf

authorize {
        eap
}

authenticate {
        eap
}

post-proxy {
        eap
}
```

図 2: radiusd.conf 設定例

```
eap {
     default_eap_type = tls
     timer_expire     = 60
     ignore_unknown_eap_types = no
     cisco_accounting_username_bug = no

     tls {
         private_key_password = "XXXXXXX"
         private_key_file = /usr/local/etc/1x/radius.camp.wide.ad.jp.pem

         certificate_file = /usr/local/etc/1x/radius.camp.wide.ad.jp.cert
         CA_file = /usr/local/etc/1x/wide.pem
         dh_file = /usr/local/etc/1x/dh2048.pem
         random_file = /usr/local/etc/1x/random

         fragment_size = 1024
         include_length = yes
         check_crl = no

         check_cert_issuer = "/C=JP/O=WIDE Project/"
     }
}
```

図 3: eap.conf 設定例

4.3 Windows XP(SP2) による設定例

クライアントとして Windows XP(SP2) を用いた場合の設定例を示す。なお、ネットワークカードならびにドライバが WPA2 に対応していない場合には、WPA-EAP ができ

ない場合がある。その場合には、

http://support.microsoft.com/default.aspx?scid=kb;ja;893357

にあるアップデートファイルを用いると WPA-EAP が可能となる場合がある。
以下の手順にて WPA-EAP を設定することができる。

1. ワイヤレスネットワーク接続の状態のウインドウからプロパティを選択
2. WPA2 AES の ESSID のプロパティを選択
3. アソシエーションの欄でネットワーク認証を WPA2、データの暗号化を AES に変更
4. 認証の欄で EAP の種類をスマートカードまたはその他の証明書を選択。他のチェック欄にはチェックを入れない。
5. プロパティでこのコンピュータの証明書を使うを選択。サーバの証明書を有効化するにチェック。他にはチェックを入れない。
6. 該当 ESSID を選んで接続する
7. 無線マークのところにポップアップが現れるのでクリック。正しく証明書が入っていれば、証明書選択のウインドウに移るので、証明書を選択。
8. NIC、ドライバが対応していれば WPA2 AES で接続。対応していなければ対応している暗号化で接続。

4.4 MacOS X による設定例

次に示すページに詳しく書かれている。

http://www.uic.edu/depts/accc/network/wireless/macx.html

4.5 NetBSD による設定例

NetBSD-current (4.99.1) を用いて接続に成功した設定例を示す。なお、機材は ThinkPad X32 であり、内蔵の mini-PCI Intel 2915ABG 無線 LAN カードを用いた。

1. 証明書を取り出す

```
# openssl pkcs12 -cacerts < 証明書 > /etc/cert/ca.pem
# openssl pkcs12 -clcerts < 証明書 > /etc/cert/client.pem
```

2. /etc/wpa_supplicant.conf を作る

```
network={
        ssid="XXXXXX"
        scan_ssid=1
        key_mgmt=WPA-EAP
        pairwise=CCMP TKIP
        group=CCMP TKIP
        eap=TLS
        identity="XXXXXXXXXXXXX"
        ca_cert="/etc/cert/ca.pem"
        client_cert="/etc/cert/client.pem"
        private_key="/etc/cert/client.pem"
        private_key_passwd="XXXXXX"
}

identity : Client Cert の CN を明記
```

3. wpa_supplicant を起動する

```
   # wpa_supplicant -i iwi0 -c /etc/wpa_supplicant.conf
```

4. 接続完了

4.6 Linux による設定例 (2009 年 6 月加筆)

Linux において以下の環境で wpa_supplicant による接続確認を行なうことができたので追記する。

- Kernel: Linux 2.6.26.1 (Debian の linux-image-2.6.26-1-686)
- Driver: ipw2200 (kernel 標準)
- wpa_supplicant v0.6.4

1. moCA 証明書を ca_cert, client_cert, private_key 用に書き出す

```
% openssl pkcs12 -cacerts -nokeys < 20080609-moca.p12 > widemoca.crt
% openssl pkcs12 -clcerts -nokeys < 20080609-moca.p12 > client.crt
```

2. クライアント鍵を書き出す

```
% openssl pkcs12 -clcerts -nocerts < 20080609-moca.p12 > client.key
```

ここではクライアント鍵を捻るためのパスフレーズを聞かれる。Enter PEM pass phrase: で private_key_passwd=”XXXX” に設定するものを入力。

3. wpa_supplicant.conf を設定する

```
network={
        ssid="wide-wpa2-enterprise"
        proto=WPA2 WPA
        scan_ssid=1
        key_mgmt=WPA-EAP
        pairwise=CCMP TKIP
        group=CCMP TKIP
        eap=TLS
        identity="XXXXXXXXXXXXX"
        ca_cert="/home/XXX/cert/widemoca.crt"
        client_cert="/home/XXX/cert/client.crt"
        private_key="/home/kXXX/cert/client.key"
        private_key_passwd="XXXX"
        priority=95
}

identity : Client Cert の CN を明記
```

4. wpa_supplicant を起動する

```
# wpa_supplicant -i iwi0 -c /etc/wpa_supplicant.conf
```

5. 接続完了

5 実験結果

本実験を通じて、各種フリー OS や商用 OS にて利用可能な WPA-EAP のシステムが構築可能であることがわかった。しかし、利用するサプリカントによっては、暗号化方式として AES を用いることができず、TKIP のみの接続となってしまう場合があった。現時点では、AES と TKIP の両方をサポートするよう無線基地局にて設定しておいた方が無難であると考えられる。