Use of EAP-GTC in eduroam infrastructure

(how to connect Nokia mobile phones to the eduroam infrastructure using EAP)

– DRAFT –

Dubravko Penezić, Miroslav Milinović,
University Computing Centre, University of Zagreb, Zagreb, Croatia
team@aaiedu.hr

Introduction

Nokia[1] mobile phones are popular devices used on GSM/GPRS/3G network. Some models have wireless adapter to connect to wireless network, and support a set of authentication protocols to authenticate user on the wireless network.

The eduroam[2] (EDUcation ROAMing) is the roaming infrastructure used by the international research and education community based on, among others, use of EAP[3] protocol(s).

Authentication issue

The eduroam infrastructure includes two provider types:

- SP – Service Provider
- IdP – Identity Provider.

IdPs mostly use data storage (typically directories) in such a way that stored identities may be used in different authentication scenarios. At the same time data storage is kept secure and with proper backup. A large number of IdPs in eduroam provide authentication via EAP protocol in the following combination: EAP-TTLS+PAP.

EAP authentication combination EAP-TTLS+PAP is based on creation of a secure communication channel using certificate (EAP-TTLS) and sending user name and password in clear text inside the established tunnel from the SP to the IdP (via PAP). Secure tunnel extends from the SP to the IdP (i.e. authentication server).

Although the EAP-TTLS-PAP authentication combination is a common solution, Nokia phones which are able to connect to the wireless network, use Symbian OS, which doesn't support EAP-TTLS+PAP (for more on this topic please check: Nokia Forum thread, EAP-TTLS/PAP support[4], started with initial post on 02.01.2007).

---

[1] Nokia, http://www.nokia.com/
[2] eduroam, http://www.eduroam.org/
[3] Extensible Authentication Protocol (EAP) RFC 3748, http://tools.ietf.org/html/rfc3748
[4] Nokia Forum thread EAP-TTLS / PAP support, http://discussion.forum.nokia.com/forum/showthread.php?p=622919#post622919

Confronted with the user demand we were forced to find a solution. Due to the nature of the IdP backend we have (LDAP directory, SHA1 hashed passwords) use of PEAP or similar solutions was not considered as a good approach. Therefore we tried with EAP-GTC authentication.

Solution

It is clear that the solution has to be found on the IdP's side, using supported EAP types on Nokia phone OS. Of course aim is also not to break security standards and eduroam policy requirements.

Therefore we've decided to try with the authentication combination EAP-TTLS+EAP-GTC.

EAP-GTC is the authentication protocol for Generic Token Card. It carries information about user and challenge-token in clear text. A small drawback of it, from the user point of view, is the fact that every authentication needs a user action (entering a challenge-token i.e. password).

EAP authentication combination EAP-TTLS+EAP-GTC is based on creation of a secure communication channel using certificate (EAP-TTLS) and sending user name and challenge-token in clear text inside that tunnel to the IdP (EAP-GTC). Again, like in a classical solution (EAP-TTSL+PAP), secure tunnel extends from the SP to the IdP (challenge-token is interpreted by the IdP's RADIUS server as the user's password). Of course, IdP needs to reconfigure authentication process in its RADIUS server and add EAP-GTC support to EAP-TTLS authentication mechanism for gathering user credentials.

We've done successful tests on our organisation's IdP (srce.hr) using the eduroam service points in Croatia.

Configuration examples

All examples require configuration support for EAP-TTLS+PAP authentication.

FreeRADIUS[5]

Add the following lines in eap.conf file under **eap** group :

```
gtc {
        challenge = "Password: "
        auth_type = LDAP
    }
```

Value of auth-type is connected with Auth-Type definition in the authentication group in the configuration (in this example it is ldap).

[5] FreeRADIUS, http://freeradius.org/

In the ttls group add:

```
ttls {

      default_eap_type = gtc
      ...
     }
```

It is required that EAP-TTLS is default EAP type and that default_eap_type variable in main eap block is set to ttls.

NavisRadius

Add the following plug-in in the policy flow :

```
CheckNewEAP     Method-Type=Compare Method-Next=<first_method> Method-
On-Fail=EAPGTC Method-Disabled=FALSE
        Compare-Input1 = "${packet.EAP-Identity}"
        Compare-Input2 = ""
        Compare-Operator = "=="

EAPGTC  Method-Type=AuthEapGtc Method-Next=<first_method> Method-On-
Fail=<first_method> Method-Disabled=FALSE
        AuthEapGtc-TunnelMethod = "GTCInfo"
        AuthEapGtc-TunnelWriteMap = <<
${request.*}:=${request.*};
DELETE ${request.EAP-Message};
${request.Password}:=${tunnel.Password};
>>
        AuthEapGtc-TunnelReadMap = "${request.*}:=${request.*};"
        AuthEapGtc-Message = "Upisite lozinku: "
        AuthEapGtc-UseReplyMessage = "TRUE"

GTCInfo Method-Type=WriteDebug Method-Disabled=FALSE
        WriteDebug-Map = <<
${Request Variable Group}=${request.*};
${Packet Variable Group}=${packet.*};
${User Variable Group}=${user.*};
${Check Variable Group}=${check.*};
${Reply Variable Group}=${reply.*};
>>
```

Check if the inner tunnel method in authEapTTLS is CheckNewEAP and change <first_method> with method that was selected as inner tunnel method in authEapTTLS before the change.

Setting Nokia mobile phone

To be able to connect to the eduroam Nokia phone must have support for wireless network and the proper root CA certificate (from the authority which provides RADIUS certificates for EAP-TTLS) in Nokia certificate store.

The exact procedure for configuring the Nokia phone may differ from phone to phone. Here is the generic one:

1. Define Access Point using eduroam SSID
2. Edit Access Point under Wlan Security Settings > EAP Plug-in Settings
3. Select EAP-TTLS and unselect all other EAP types
4. Edit EAP-TTLS and leave everything set by default except following
5. Change Authority Certificate to root CA which provides RADIUS certificate for EAP-TTLS on user's IdP server
6. Set Username in use to User define
7. For Username enter only uid part of the userid (e.g. for pero@srce.hr, enter only pero)
8. Set Realm in use to User define
9. For Realm enter only realm part of the userid (e.g. for pero@srce.hr, enter only srce.hr)
10. Select right arrow to edit inner protocol (upper right corner)
11. Select EAP-GTC and unselect all other EAP types
12. Edit EAP-GTC and write full userid (pero@srce.hr)

At every authentication request Nokia phone will ask for user challenge-token which is, in this case, the user's password.