

Deploying EAP-FAST on FreeRADIUS

Maja Górecka-Wolniewicz
PIONIER

Handling EAP-FAST in FreeRADIUS

- An experimental `rlm_eap2` module has to be used
- The only documentation is in `raddb/experimental.conf` – only short comments
- The `libeap.so` from `hostap` distribution is needed to compile `rlm_eap2`
- This stuff was implemented and tested with version 1.1.4, the current version is 2.1.8

Hostap project

- <http://hostap.epitest.fi>
 - hostap version
 - neither latest stable version, nor latest development version can be used
 - only git version available from <http://hostap.epitest.fi/gitweb/gitweb.cgi> contains eap_example subdirectory code to build libeap.so
 - two git versions are developed:
 - **hostap-06.git** – requires less changes on FreeRADIUS side
 - hostap.git

Building libeap

- A patched version of OpenSSL is required
 - patches are available in the hostap distribution, from *patches* subdirectory
 - patches add support for session secret
 - OpenSSL has to be configured with `enable-tlsex` option
- Edit Makefile to
 - include EAP-FAST on server side
 - indicate appropriate OpenSSL library version
- make `CONFIG_SOLIB=yes`

FreeRADIUS - rlm_eap2

- rlm_eap2 module has to be adapted to work with hostap library
 - it doesn't provide configuration variables which are required by libeap
- Required extensions:
 - new general configuration items to pass
 - EAP-FAST authority identity, authority identifier information, PAC-key lifetime, PAC-key refresh time, PAC-Opaque values
 - in TLS configuration section DH file has to be provided - a Diffie-Hellman key is needed in Server Unauthenticated Provisioning mode

FreeRADIUS configuration

- Include eap2.conf with the same content as eap.conf plus subsection

```
fast {  
    pac_opaque_encr_key = ....  
    eap_fast_a_id = xxxxx  
    eap_fast_a_id_info = xxxxx  
}
```

- Inner-tunnel is not used by eap2 module
- eap2 has to be called instead of eap (sites-enabled/default)

Results

- eapol_test works for each EAP-FAST provisioning method, and PEAP, EAP-TTLS methods
- Only anonymous PAC provisioning works on the wireless network, because eap2 does not implement fragmentation
 - Alan deKok said:
”I think that's an issue with hostap library. Maybe there's an API for FreeRADIUS to set MTU for the library. (I haven't looked recently)”
- All changes were send as a patch to freeradius list