Blog Name:

802.1X clients and RADIUS server supporting bigger Diffie-Hellman (DH) keys

Group:
Log in to request membership [1]

TLDR: clients will move to not supporting Diffie-Hellman keys of less than 1024 bit - upgrade your RADIUS server configuration or release to ensure its providing bigger Diffie-Hellman parameters in the EAP session

overview

On the back of the recent wave of further SSL attacks and weakness identitication, several vendors are now making moves to stop SSL clients from negotiating connections where the parameters have weak Diffie-Hellman (DH) keys. In the world of web browsers , Chrome and Firefox have already started to refuse connections (unless configuration/preferences are overridden!) where the DH key is weak (less than 768bits) and are looking to at least 1024bit as an interim - recommendations are 2048bit.

OpenSSL itself (latest versions) will now generate 2048bit DH keys when invoked to do so.

In the world of 802.1X clients, I have seen wpa_supplicant eapol_test through a RADIATOR system exhibit this behaviour and today I've seen that the latest beta for the next OSX release 'El Capitan' is now also rejecting weak DH keys - see this page for info about DH keys less than 512 bit in that release - https://developer.apple.com/library/prerelease/mac/releasenotes/General/... [2] . Changes to mobile/tablet devices will be more problematic to diagnose as accessing any form of debug log can be problematic

verification/fixing the issue

to verify what DH keysize you are using on FreeRADIUS, check your EAP configuration (eap.conf on FreeRADIUS 2, modules-enabled/eap on FreeRADIUS 3) , locate the DH file and then perform the following test

```
openssl dhparam -in $dh -text -noout
```

(where $dh is the name of the file)

to change a FreeRADIUS configuration to use the new DH key

```
cd /etc/raddb/certs
```

(or wherever your DH file is kept as per the eap.conf file)

```
cp dh dh.old
```

(backup old file just in case..)

```
openssl dhparam -out dh 2048
```

(generate a 2048bit DH file....will take time!)

ensure that the DH file has the same permissions as the old one..and as required by the server

```
service radiusd restart
```

(restart the service...this would be on eg Redhat/CentOS etc, your distribution may vary)

PS whilst doing this, ensure your random file is using /dev/urandom and not just a file

for RADIATOR, the parameter is

```
EAPTLS_DHFile %D/certificates/cert/dh
```

in the configuration file. That key/file can be changed to a 2048 bit one in the same process as documentated above for FreeRADIUS

For NPS and ACS/ISE - vendor patches are expected to be released to update how they operate or to update the key size. Havent seen too much movement in the RADIUS world at the time of writing - they need to do something on when the next OSX..and possibly IOS releases come out, your RADIUS servers wont be able to authenticate those clients.

Default group content privacy:
Log in to request membership [1]

Links
[1] https://community-stg.jisc.ac.uk/
[2] https://developer.apple.com/library/prerelease/mac/releasenotes/General/rn-osx-10.11/