

# ***GEOPRIV Challenges in RADIUS***

Emile van Bergen,  
E-Advies

[openradius@e-advies.nl](mailto:openradius@e-advies.nl)

## *What is the problem?*

- ◆ GEOPRIV specifies that network devices may only transmit location information with the user's consent
- ◆ Therefore, if a NAS does not have prior knowledge about its users – and RADIUS clients generally don't – then it is not allowed to put location information in its initial Access-Request
- ◆ Yet, RADIUS server policies may wish to make their authorizations dependent on location information

# *Consequences*

- ◆ If the following conditions apply:
  - ◆ 1. a NAS does not know the user's privacy policy a priori,
  - ◆ 2. a NAS is not able to obtain permission to transmit location information directly from the user, and
  - ◆ 3. the RADIUS server's policy requires location information to make its authorization decisions,
- ◆ then, the NAS need to make an inquiry somewhere before it can send an Access-Request to the RADIUS server

# *Observations*

- ◆ It makes no sense to develop yet another protocol to link NASes to user profiles
- ◆ If RADIUS is used for AAA, then the user's profile at the RADIUS server is a likely place to store the user's location privacy policy too
- ◆ Some RADIUS server policies may not need location information at authorization time, but may need it at accounting time, or it may be purely optional

## *Solutions are possible: a first attempt*

- ◆ Let the NAS send a complete access request to the RADIUS server, lacking only location information governed by GEOPRIV
- ◆ If the RADIUS server's policy does not require location information to perform authorization, it can respond as normal
- ◆ It may include the user's privacy policy in the Access-Accept, to allow the NAS to include Location information in Accounting

## *If location information is required in accounting*

- ◆ Let the NAS make a promise in its Access-Request...
- ◆ ... saying that if the RADIUS server indicates in its Access-Accept that the user allows certain location information to be sent, the NAS will send it
- ◆ E.g. by including an A/V pair  
Will-Send-Location-\* = If-Allowed-By-Server
- ◆ \*) All supported types of location information should probably be listed separately

## *If location information is required for authorization*

- ◆ If a RADIUS server requires location information for proper authorization,
- ◆ ... and there is insufficient location information in the access request,
- ◆ ... and the user's profile indicates that the user allows the required location information to be transmitted,
- ◆ ... and the NAS has promised to send the required location information when asked
- ◆ ... It sends an Access-Challenge to the NAS

# *The server challenges the NAS*

- ◆ The server's Access-Challenge effectively contains the following information:
  - ◆ 1. It tells the NAS that the server requires certain pieces of location information before it can provide an Access-Accept or Access-Reject
  - ◆ 2. Implicitly, it tells the NAS that the server has verified that the user's profile allows that information to be sent, otherwise it would put the NAS in an impossible position
  - ◆ 3. It must also tell the NAS not to challenge the user in case of PAP and CHAP authentications

# *Accepting the challenge*

- ◆ However, before a RADIUS server can send an Access-Challenge to the NAS, it needs to know that the NAS will properly act upon the challenge
- ◆ The reason is that RFC 2865 requires NASes that don't understand an Access-Challenge to reject the user...
- ◆ ... which is premature if the server has a policy to offer limited access when location information is lacking

## *... in the proper way*

- ◆ Properly acting upon the challenge for location information also means not to ask the user for a second password...
- ◆ ... which is normal NAS behaviour for challenges to PAP and CHAP requests.

# *Two issues, two approaches*

- ◆ So, there are two issues on the table:
  - ◆ 1. The NAS must be able to tell the RADIUS server that it will not reject the user when challenged
  - ◆ 2. The RADIUS server must be able to tell the NAS in a non-EAP challenge that it should not prompt the user for a one time password, but resend the same access request (only this time with location information included)

## *The minimalistic approach*

- ◆ The minimalistic approach is to make it all implicit:
- ◆ The NAS' promise to send location information when permitted by an access accept, can be interpreted as a promise not to reject challenges either
- ◆ The server's inclusion of a list of required location attributes in the challenge, can be interpreted as a request not to prompt the user for another password

# *The generic approach*

- ◆ We can also decouple the challenge issue from GEOPRIV, because:
- ◆ there may be other cases where a NAS is required to withhold information from its initial access request (although I can't think of many), or
- ◆ there may be other cases where a challenge is required not to be misunderstood, or
- ◆ because overloading the meaning of the promises and demands is undesirable.

# *A generic challenge protocol*

- ◆ A protocol to get more certainty and flexibility for RADIUS challenges could be done as follows.
- ◆ The NAS promises using a Challenge-Support = Yes in its access request that:
  - ◆ it will not reject the user when challenged
  - ◆ if a challenge contains a Challenge-Cause attribute, it will act upon its value
  - ◆ if it doesn't know how, it will resend the access request as it was (with an echoed State as per RFC 2865), and without prompting the user

## *... gives certainty to the server*

- ◆ This challenge protocol provides the server with the following assurances:
  - ◆ that it can safely send the challenge to an unknown NAS, without worrying that the user will be rejected or inappropriately prompted
  - ◆ when the second access request comes in, the server knows that it contains all the information the NAS is able to provide
- ◆ It also removes some of the need for the NAS to advertise the list of withheld pieces of information

## *But is it worth the trouble?*

- ◆ That's the question
- ◆ It's either creating a considerable (but manageable) protocol for GEOPRIV alone,
- ◆ or doing something more future-proof that may never be really needed.

## *What we do need*

- ◆ Regardless of how we tell the server about challenge support or the NAS what the challenge is all about:
- ◆ allowing NASes to make certain promises about how it will act upon certain RADIUS responses is needed here – and for other situations as well:
- ◆ the most prominent example being session limiting attributes, such as filters, bandwidth controls, volume caps and the like.

# *Work to be done and things to think about*

- ◆ If we want a NAS' promise to act upon certain response attributes stay valid when response attributes are filtered by proxies,
- ◆ the proxy will have to be required to modify the promise to reflect its filtering policy
- ◆ How to encode the promises?
  - ◆ as A/V pairs – the trusted 'hints' mechanism?
  - ◆ as bitmaps referring to complete feature sets?
  - ◆ as a bitmap containing response attributes?

***Thanks***

for your time, attention and input!