Network Working Group
Internet-Draft
Expires: September 2, 2005

F. Adrangi
V. Lortz
Intel
F. Bari
Cingular Wireless
P. Eronen
Nokia

March 2005

Identity selection hints for Extensible Authentication Protocol (EAP)
draft-adrangi-eap-network-discovery-12

Status of this Memo

Copyright Notice

Abstract

The Extensible Authentication Protocol (EAP) is defined in RFC 3748. This document defines a mechanism that allows an access network to

provide identity selection hints to an EAP peer. The purpose is to assist the EAP peer in selecting an appropriate Network Access Identifier (NAI) when there is no direct roaming relationship between the access network and the peer's home network. In this case, authentication is typically accomplished via a mediating network such as a roaming consortium or broker.

The mechanism defined in this document is limited in its scalability. It is intended for access networks that have a small to moderate number of direct roaming partners.

Table of Contents

1. Introduction

An EAP peer (hereafter, also referred to as the peer) can have several sets of credentials, and its home network may have roaming relationships with several mediating networks. In some cases, the peer may be uncertain which Network Access Identity (NAI) to include in an EAP-Response/Identity.

The Extensible Authentication Protocol (EAP) is defined in [RFC3748]. This document defines a mechanism that allows the access network to provide an EAP peer with identity selection hints, including information about its roaming relationships. This information is sent to the peer in an EAP-Request/Identity message by appending it after the displayable message and a NUL character.

One possible application for this mechanism is to help an EAP peer perform NAI decoration [rfc2486bis] to facilitate routing of AAA messages to the home AAA server. If there are several possible mediating networks, the peer can use this method to influence which one is used.

Exactly how the selection is made by the peer depends largely on the peer's local policy and configuration, and is outside the scope of this document. For example, the peer could decide to use one of its other identities, decide to switch to another access network, or attempt to reformat its NAI [rfc2486bis] to assist in proper AAA routing. The exact client behaviour is described by standard bodies using this specification such as 3GPP [TS 24.234].

Section 2 describes the required behavior of implementations of this Specification, including the packet format for structuring and presenting identity hint information to an EAP peer.

1.1 Applicability

The identity hints are typically useful only when there's too much ambiguity for an access network to determine how to route the AAA packet. This can happen, for instance, when access networks have contracts with multiple roaming consortiums but do not have a full list of home networks reachable through them.

In such scenarios, a limited number of identity hints (e.g., a list of roaming partners of the access network) can be provided by the mechanism to enable the EAP peer to influence routing of AAA packets. The immediate application of the proposed mechanism is in 3GPP systems interworking with WLANs [TS 23.234] and [TS 24.234].

The roaming partner information provided via this mechanism is limited by the link layer MTU size. For example, assuming an average of 20 octets per roaming partner / home network information and the link layer MTU size of 1096, the approximate number of roaming partners that can be advertised would be 50. The scalability limitation imposed by the link layer MTU size should be taken into consideration when deploying this solution.

This document is also related to the general network discovery and selection problem described in [netsel-problem]. The proposed mechanism described in this document solves only a part of the problem in [netsel-problem]. IEEE 802.11 is also looking into more comprehensive and long-term solutions for network discovery and selection.

1.2 Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

NAI — Network Address Identifier [rfc2486bis].

Decorated NAI — An NAI with additional information for influencing AAA routing. Please refer to section 2.7 of [rfc2486bis] for its construction.

NAI Realm — Realm portion of an NAI [rfc2486bis].

2. Implementation requirements

An EAP peer implementing this specification MUST be able to receive an identity hint in an initial EAP-Request/Identity, or in a subsequent EAP-Request/Identity.

The EAP authenticator MAY send an identity hint to the peer in the initial EAP-Request/Identity. If the identity hint is not sent initially (such as when the authenticator does not support this specification), then if the local EAP-aware AAA proxy/server implementing this specification receives an AAA Request packet with an unknown realm, it SHOULD reply with an EAP-Request/Identity containing an identity hint. For example, in case of RADIUS, if the EAP-aware RADIUS proxy/server [RFC3579] receives an Access-Request packet with an unknown realm in the UserName(1) attribute, then it can reply with an EAP-Request/Identity containing an identity hint within an Access-Challenge packet. See "option 3" in the appendix for the message flow diagram.

If the peer responds with an EAP-Response/Identity containing an unknown realm after the local AAA proxy/server sends an identity hint, then the local AAA proxy/server MUST respond with an EAP Failure packet. The local AAA proxy/server MAY also send an EAP-Notification message providing the reason for the failure prior to the EAP Failure packet.

When an Identity hint is sent by a AAA proxy/server, the AAA proxy/server MUST be able to determine if an identity hint had previously been sent by it to the EAP peer. When RADIUS is used, the State(24) attribute can be used to achieve this.

As noted in [RFC3748], Section 3.1, the minimum EAP MTU size is 1020 octets. EAP does not support fragmentation of EAP-Request/Identity messages, so the maximum length of the identity hint information is limited by the link MTU.

2.1 Packet format

The Identity hint information is placed after the displayable string and a NUL character in the EAP-Request/Identity. The following ABNF [RFC2234] defines an NAIRealms attribute for presenting the identity hint information. The attribute's value consists of a set of realm names separated by a semicolon.

```
identity-request-data = [ displayable-string ] "%x00" [ Network-Info ]

displayable-string    = *CHAR

Network-Info     =   "NAIRealms=" realm-list
Network-Info     =/  1*OCTET ",NAIRealms=" realm-list
Network-Info     =/  "NAIRealms=" realm-list "," 1*OCTET
Network-Info     =/  1*OCTET ",NAIRealms=" realm-list "," 1*OCTET

realm-list            = realm /
                        ( realm-list ";" realm )
```

The "OCTET" and "CHAR" rules are defined in [RFC2234] and the "realm" rule is defined in [rfc2486bis].

A sample hex dump of an EAP-Request/Identity packet is shown below.

```
01                        ; Code: Request
00                        ; Identifier: 0
00 43                     ; Length: 67 octets
01                        ; Type: Identity
48 65 6c 6c 6f 21 00 4e   ; "Hello!\0NAIRealms=example.com;mnc014.
41 49 52 65 61 6c 6d 73   ; mcc310.3gppnetwork.org"
3d 69 73 70 2e 65 78 61
6d 70 6c 65 2e 63 6f 6d
3b 6d 6e 63 30 31 34 2e
6d 63 63 33 31 30 2e 33
67 70 70 6e 65 74 77 6f
72 6b 2e 6f 72 67
```

The Network-Info can contain a NAIRealms list in addition to proprietary information. The proprietary information can be placed before or after NAIRealms list. To extract NAIRealms list, an implementation can either find the "NAIRealms=" immediately after the NUL or seek forward to find ",NAIRealms" somewhere in the string. The realms data ends either at the first "," or at the end of the string, whichever comes first.

3. IANA Considerations

This document does not define any new namespaces to be managed by IANA, and does not require any assignments in existing namespaces.

4. Security considerations

Identity hint information is delivered inside an EAP-Request/Identity before the authentication conversation begins. Therefore, it can be modified by an attacker. The NAIRealms attribute therefore MUST be treated as a hint by the peer.

Unauthenticated hints may result in peers inadvertently revealing additional identities, thus compromising privacy. Since the EAP-Response/Identity is sent in the clear, this vulnerability already exists. This vulnerability can be addressed via method-specific identity exchanges.

Similarly, in a situation where the peer has multiple identities to choose from, an attacker can use a forged hint to convince the peer to choose an identity bound to a weak EAP method. Requiring the use of strong EAP methods can protect against this. A similar issue already exists with respect to unprotected link layer advertisements such as 802.11 SSIDs.

If the identity hint is used to select a mediating network, existing EAP methods may not provide a way for the home AAA server to verify that the mediating network selected by the peer was actually used.

Any information revealed either from the network or client sides before authentication has occurred can be seen as a security risk. For instance, revealing the existence of a network that uses a weak authentication method can make it easier for attackers to discover that such network is accessible. Therefore, the consent of the network being advertised in the hints is required before such hints can be sent.

5. Acknowledgements

The authors would specially like to thank Jari Arkko, Bernard Aboba, and Glen Zorn for their help in scoping the problem, for reviewing the draft work in progress and for suggesting improvements to it.

The authors would also like to acknowledge and thank Adrian Buckley, Blair Bullock, Jose Puthenkulam, Johanna Wild, Joe Salowey, Marco Spini, Simone Ruffino, Mark Grayson, Mark Watson, and Avi Lior for their support, feedback and guidance during the various stages of this work.

6. Appendix - Delivery Options

Although the delivery options are described in the context of IEEE 802.11 access networks, they are also applicable to other access networks that use EAP [RFC3748] for authentication and use the NAI format [rfc2486bis] for identifying users.

The options assume that the AAA protocol in use is RADIUS [RFC2865]. However, Diameter [RFC3588] could also be used instead of RADIUS without introducing significant architectural differences.

The main difference amongst the options is which entity in the access network creates the EAP-Request/Identity. For example, the role of EAP server may be played by the EAP authenticator (where an initial EAP-Request/Identity is sent with an identity hint) or a RADIUS proxy/server (where the NAI Realm is used for forwarding).

The RADIUS proxy/server acts only on the RADIUS UserName(1) attribute and does not have to parse the EAP-Message attribute.

Option 1: Initial EAP-Request/Identity from access point

In typical IEEE 802.11 wireless LANs, the initial EAP-Request/Identity is sent by the access point (i.e., EAP authenticator). In the simplest case, the identity hint information is simply included in this request, as shown below.

```
     EAP          Access Point        local RADIUS          home RADIUS
     Peer                               proxy/server           server
     |     1. EAP        |                    |                    |
     |  Request/Identity |                    |                    |
     |   (NAIRealms)     |                    |                    |
     |<------------------|                    |                    |
     |     2. EAP        |                    |                    |
     |  Response/Identity|                    |                    |
     |------------------>|                    |                    |
     |                   | 3. Access-Request  |                    |
     |                   |      (EAP          |                    |
     |                   |  Response/Identity)|                    |
     |                   |------------------->|                    |
     |                   |                    | 4.Access-Request   |
     |                   |                    |      (EAP          |
     |                   |                    | Response/Identity) |
     |                   |                    |------------------->|
     |                   |                    |                    |
     |<-------------------EAP conversation ----------------------->|
```

Current access points do not support this mechanism, so other options may be preferable. This option can also require configuring the identity hint information in a potentially large number of access points, which may be problematic if the information changes often.

Option 2: Initial EAP-Request/Identity from local RADIUS proxy/server

This is similar to Option 1, but the initial EAP-Request/Identity is created by the local RADIUS proxy/server instead of the access point. Once a peer associates with an access network AP using IEEE 802.11 procedures, the AP sends an EAP-Start message [RFC3579] within a RADIUS Access-Request. The access network RADIUS server can then send the EAP-Request/Identity containing the identity hint information.

```
     EAP          Access Point          local RADIUS          home RADIUS
     Peer                                proxy/server           server
     |                   | 1. Access-Request  |                    |
     |                   |    (EAP-Start)     |                    |
     |                   |-------------------->|                    |
     |                   | 2.Access-Challenge |                    |
     |                   |       (EAP         |                    |
     |                   |  Request/Identity  |                    |
     |                   |   with NAIRealms)  |                    |
     |                   |<-------------------|                    |
     |     3. EAP        |                    |                    |
     | Request/Identity  |                    |                    |
     |   (NAIRealms)     |                    |                    |
     |<------------------|                    |                    |
     |     4. EAP        |                    |                    |
     | Response/Identity |                    |                    |
     |------------------>|                    |                    |
     |                   | 5. Access-Request  |                    |
     |                   |       (EAP         |                    |
     |                   | Response/Identity) |                    |
     |                   |------------------->|                    |
     |                   |                    | 6. Access-Request  |
     |                   |                    |        (EAP        |
     |                   |                    | Response/Identity) |
     |                   |                    |------------------->|
     |                   |                    |                    |
     |<------------------- EAP conversation ---------------------->|
```

This option can work with current access points if they support the EAP-Start message.

Option 3: Subsequent EAP-Request/Identity from local RADIUS proxy/server

In the third option, the access point sends the initial EAP-Request/Identity without any hint information. The peer then responds with an EAP-Response/Identity, which is forwarded to the local RADIUS proxy/server. If the RADIUS proxy/server cannot route the message based on the identity provided by the peer, it sends a second EAP-Request/Identity containing the identity hint information.

```
     EAP            Access Point       local RADIUS          home RADIUS
     Peer                              Proxy/Server            server
     |                   |                    |                    |
     |     1. EAP        |                    |                    |
     | Request/Identity  |                    |                    |
     | (w/o NAIRealms)   |                    |                    |
     |<------------------|                    |                    |
     |     2. EAP        |                    |                    |
     | Response/Identity |                    |                    |
     |------------------>|                    |                    |
     |                   | 3. Access-Request  |                    |
     |                   |      (EAP          |                    |
     |                   | Response/Identity) |                    |
     |                   |------------------->|                    |
     |                   | 4.Access-Challenge |                    |
     |                   |      (EAP          |                    |
     |                   |  Request/Identity  |                    |
     |                   |  with NAIRealms)   |                    |
     |                   |<-------------------|                    |
     |     5. EAP        |                    |                    |
     | Request/Identity  |                    |                    |
     |   (NAIRealms)     |                    |                    |
     |<------------------|                    |                    |
     |     6. EAP        |                    |                    |
     | Response/Identity |                    |                    |
     |------------------>|                    |                    |
     |                   | 7. Access-Request  |                    |
     |                   |      (EAP          |                    |
     |                   | Response/Identity) |                    |
     |                   |------------------->|                    |
     |                   |                    |                    |
     ======================Failure due to unknown realm=============
     |                   |                    |                    |
     |                   | 7a.Access-Reject   |                    |
     |                   |    (EAP-Failure)   |                    |
     |                   |<-------------------|                    |
     |    7b. EAP        |                    |                    |
     |     Failure       |                    |                    |
     |<------------------|                    |                    |
     =================================================================
     |                   |                    |                    |
     |                   |                    | 8. Access-Request  |
     |                   |                    |       (EAP         |
     |                   |                    | Response/Identity) |
     |                   |                    |------------------->|
     |                   |                    |                    |
     |<-------------------- EAP conversation --------------------->|
```

This option does not require changes to existing NASes, so it may be preferable in many environments.

7. References

7.1 Normative references

[rfc2486bis]
Aboba, B., Beadles, M., Arkko, J., and P. Eronen, "The Network Access Identifier", draft-ietf-radext-rfc2486bis-05 (work in progress), July 2004.

[RFC3748] Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J., and H. Levkowetz, "Extensible Authentication Protocol (EAP)", RFC 3748, June 2004.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2234] Crocker, D., Ed. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", RFC 2234, November 1997.

7.2 Informative references

[RFC3579] Aboba, B. and P. Calhoun, "RADIUS (Remote Authentication Dial In User Service) Support For Extensible Authentication Protocol (EAP)", RFC 3579, September 2003.

[netsel-problem]
Arkko, J. and B. Aboba, "Network Discovery and Selection Problem", draft-ietf-eap-netsel-problem-02 (work in progress), July 2004.

[TS 23.234]
"3GPP System to Wireless Local Area Network (WLAN) interworking. Stage 2. (www.3gpp.org)", Release 6 3GPP/ WLAN Stage 2 Specification TS 23.234.

[TS 24.234]
"3GPP System to Wireless Local Area Network (WLAN) interworking. Stage 3. (www.3gpp.org)", Release 6 3GPP/ WLAN Stage 2 Specification TS 24.234.

[RFC3588] Calhoun, P., Loughney, J., Guttman, E., Zorn, G., and J. Arkko, "Diameter Base Protocol", RFC 3588, September 2003.

[RFC2865] Rigney, C., Willens, S., Rubens, A., and W. Simpson,

"Remote Authentication Dial In User Service (RADIUS)",
RFC 2865, June 2000.

Authors' Addresses

Farid Adrangi
Intel Corporation
2111 N.E. 25th Avenue
Hillsboro, OR 97124
USA

Phone: +1 503-712-1791
Email: farid.adrangi@intel.com

Victor Lortz
Intel Corporation
2111 N.E. 25th Avenue
Hillsboro, OR 97124
USA

Phone: +1 503-264-3253
Email: victor.lortz@intel.com

Farooq Bari
Cingular Wireless
7277 164th Avenue N.E.
Redmond, WA 98052
USA

Phone: +1 425-580-5526
Email: farooq.bari@cingular.com

Pasi Eronen
Nokia Research Center
P.O. Box 407
FIN-00045 Nokia Group
Finland

Email: pasi.eronen@nokia.com

Intellectual Property Statement

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.