Network Working Group
Request for Comments: 4284
Category: Informational

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

January 2006

Identity Selection Hints for the Extensible Authentication Protocol (EAP)

Status of This Memo

Copyright Notice

IESG Note:

EAP Identity Selection was developed by 3GPP. Documentation is provided as information to the Internet community. The EAP WG has verified that this specification is compatible with EAP as defined in RFC 3748. Required 3GPP client behavior is described in 3GPP TS 24.234.

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 end of the link that responds to the authenticator. The purpose is to assist the EAP peer in selecting an appropriate Network Access Identifier (NAI). This is useful in situations where the peer does not receive a lower-layer indication of what network it is connecting to, or when there is no direct roaming relationship between the access network and the peer's home network. In the latter 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

The Extensible Authentication Protocol (EAP) is defined in [RFC3748]. An EAP peer (hereafter, also referred to as the peer) may have multiple credentials. Where the lower layer does not provide an indication of which network it is connecting to, or where its home network may have roaming relationships with several mediating networks, the peer may be uncertain of which Network Access Identifier (NAI) to include in an EAP-Response/Identity.

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.

This mechanism may assist the peer in selecting a credential and associated NAI, or in formatting the NAI [RFC4282] to facilitate routing of Authentication, Authorization, and Accounting (AAA) messages to the home AAA server. If there are several mediating networks available, the peer can 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 [RFC4282] to assist in proper AAA routing. The exact client behavior is described by standard bodies using this specification such as 3GPP [TS-24.234].

Section 2 describes the required behavior of implementations, including the format for identity hints.

1.1. Relationship with Other Specifications

This document specifies behavior of Remote Authentication Dial-In User Service (RADIUS) proxies that handle EAP messages. This includes the specification of the behavior of proxies in response to an unknown realm within the User-Name(1) attribute of an Access-Request containing one or more EAP-Message attributes. This document, if used in a scenario requiring NAI "decoration" as specified in [RFC4282], assumes a source-routing model for determination of the roaming relationship path, and therefore affects the behavior of RADIUS proxies in roaming situations.

1.2. Applicability

Identity hints are useful in situations where the peer cannot determine which credentials to use, or where there may be multiple alternative routes by which an access network can reach a home network. This can occur when access networks support multiple roaming consortiums but do not have a full list of the home networks reachable through them.

In such scenarios, identity hints (e.g., a list of roaming partners of the access network) can be provided to enable the EAP peer to influence route selection, using the NAI [RFC4282] to specify the desired source route. The immediate application of the proposed mechanism is in 3GPP systems interworking with WLANs [TS-23.234] and [TS-24.234].

The number of hints that can be provided by this mechanism is limited by the EAP MTU. For example, assuming 20 octets per hint and an EAP MTU of 1096, a maximum of 50 roaming partners can be advertised. Scaling limitations imposed by the EAP MTU should be taken into account when deploying this solution.

Since this mechanism relies on information provided in the EAP-Request/Identity packet, it is necessary for the peer to select a point of attachment prior to obtaining identity hints. Where there are multiple points of attachment available, the mechanism defined in this specification does not allow the peer to utilize the identity hints in making a decision about which point of attachment to select. In roaming situations, this can require the peer to try multiple points of attachment before it finds a compatible one, increasing handoff latency.

This document is 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.

1.3. 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 Access Identifier [RFC4282].

Decorated NAI An NAI specifying a source route. See [RFC4282] Section 2.7 for more information.

NAI Realm Realm portion of an NAI [RFC4282].

2. Implementation Requirements

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 the EAP peer may select the wrong NAI. If the local AAA proxy does not have a default route configured, then it may find that the User-Name(1) attribute in the request contains a realm for which there is no corresponding route.

As noted in [RFC2607], Section 5.1:

"Proxies are frequently used to implement policy in roaming situations. Proxies implementing policy MAY reply directly to Access-Requests without forwarding the request. When replying directly to an Access-Request, the proxy MUST reply either with an Access-Reject or an Access-Challenge packet. A proxy MUST NOT reply directly with an Access-Accept."

Where no route is found, existing AAA proxies will typically send an Access-Reject. However, where the request contains an EAP-Message attribute, AAA proxies implementing this specification should instead reply with a challenge including an identity hint.

For example, if a RADIUS proxy receives an Access-Request with an EAP-Message attribute and a User-Name(1) attribute containing an unknown realm, it SHOULD reply with an Access-Challenge with an EAP-Message attribute encapsulating an EAP-Request/Identity packet containing an identity hint, rather than an Access-Reject. 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 sends an identity hint, then a local AAA proxy/server implementing this specification MUST eventually send an Access-Reject containing an EAP-Failure. Prior to doing so, it MAY send an Access-Challenge containing an EAP-Notification, in order to provide an explanation for the failure. In order to determine whether an identity hint had been previously sent, the State(24) attribute defined in [RFC2865] can be used.

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 [RFC4234] 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 [RFC4234] and the "realm" rule is defined in [RFC4282].

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

```
01                          ; Code: Request
00                          ; Identifier: 0
00 3f                       ; Length: 63 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 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 an NAIRealms list in addition to proprietary information. The proprietary information can be placed before or after the NAIRealms list. To extract the 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. 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. That is, the peer must treat the hint as an unreliable indication

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 a network is accessible. Therefore, the consent of the network being advertised in the hints is required before such hints can be sent.

4. Acknowledgements

The authors would especially like to thank Jari Arkko, Bernard Aboba, and Glen Zorn for their help in scoping the problem, and for reviewing the document in progress and 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.

5. 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 [RFC4282] 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 the 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 NAIRealm is used for forwarding).

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

Option 1: Initial EAP-Request/Identity from the 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 the 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.

6. References

6.1. Normative References

[RFC4282] Aboba, B., Beadles, M., Arkko, J., and P. Eronen, "The Network Access Identifier", RFC 4282, December 2005.

[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.

[RFC4234] Crocker, D. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", RFC 4234, October 2005.

[RFC2607] Aboba, B. and J. Vollbrecht, "Proxy Chaining and Policy Implementation in Roaming", RFC 2607, June 1999.

6.2. 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", Work in Progress, October 2005.

[TS-23.234] 3GPP TS 23.234 V6.6.0, "3GPP System to Wireless Local Area Network (WLAN) interworking; System description (Release 6)", September 2005.

[TS-24.234] 3GPP TS 24.234 V6.4.0, "3GPP System to Wireless Local Area Network (WLAN) interworking; User Equipment (UE) to network protocols; Stage 3 (Release 6)", September 2005.

[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

Acknowledgement

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).