             EAP Pre-authentication Problem Statement
                  draft-ietf-hokey-preauth-ps-04

Status of this Memo

   By submitting this Internet-Draft, each author represents that any
   applicable patent or other IPR claims of which he or she is aware
   have been or will be disclosed, and any of which he or she becomes
   aware will be disclosed, in accordance with Section 6 of BCP 79.

   Internet-Drafts are working documents of the Internet Engineering
   Task Force (IETF), its areas, and its working groups. Note that
   other groups may also distribute working documents as Internet-
   Drafts.

   Internet-Drafts are draft documents valid for a maximum of six months
   and may be updated, replaced, or obsoleted by other documents at any
   time. It is inappropriate to use Internet-Drafts as reference
   material or to cite them other than as "work in progress."

   The list of current Internet-Drafts can be accessed at
   http://www.ietf.org/ietf/1id-abstracts.txt.

   The list of Internet-Draft Shadow Directories can be accessed at
   http://www.ietf.org/shadow.html.

   This Internet-Draft will expire on March 13, 2009.

Abstract

   EAP (Extensible Authentication Protocol) pre-authentication is
   defined as the use of EAP to pre-establish EAP keying material on a
   target authenticator prior to arrival of the peer at the access
   network managed by that authenticator. This draft discusses EAP pre-
   authentication problems in detail.

Table of Contents

[1](#). Introduction

When a mobile device during an active communication session moves
from one access network to another access network and changes its
point of attachment, it is subjected to disruption in the continuity
of service because of the associated handover operation. The
performance requirement of a real-time application will vary based on
the type of application and its characteristics such as delay
tolerance and loss tolerance limit. ITU-T G.114 [ITU] recommends 150
ms as the upper limit for VoIP applications and 400 ms as generally
unacceptable delay. Similarly, a streaming application has a
tolerable packet (SDU) error rates ranging from 0.1 to 0.00001 and
the transfer delay of less than 300 ms. Thus, any optimized handoff
mechanism will need to take these factors into consideration in order
to be able to support a heterogeneous handover that is agnostic to
link-layer technologies.

As a mobile device goes through a handover process, it is subjected
to delay because of the rebinding of its association at several
layers of the protocol stack. Delays incurred within each of these
layers affect the ongoing multimedia application and data traffic
within the client [WCM].

Handover often requires authentication and authorization for
acquisition or modification of resources assigned to a mobile device
and the authentication and authorization needs interaction with a
central authority in a domain in most cases. In some cases the
central authority may be placed far away from the mobile device. The
delay introduced due to such an authentication and authorization
procedure adds to the handover latency and consequently affects
ongoing application sessions [MQ7]. We focus our discussion
highlighting the factors that affect the performance due to network
access authentication and authorization where EAP [RFC3748] is used
for network access authentication.

This draft discusses EAP pre-authentication problems in detail where
EAP pre-authentication is defined as the utilization of EAP to pre-
establish EAP keying material on an EAP authenticator prior to
arrival of the mobile device that acts as an EAP peer, at the access
network served by that authenticator.

[1.1](#). Specification of Requirements

In this document, several words are used to signify the requirements
of the specification. These words are often capitalized. 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].

[2](). Terminology

Peer

> See [RFC3748].

Authenticator

> See [RFC3748].

EAP Server

> See [RFC3748].

Serving Authenticator (SA)

> An authenticator that is currently serving the peer.

Target Authenticator (TA)

> An authenticator that has been chosen to be the new serving
> authenticator for a peer.

Candidate Authenticator (CA)

> An authenticator that can potentially become the target
> authenticator for a peer. There can be multiple candidate
> authenticators for the peer.

Master Session Key (MSK)

> See [RFC3748].

Access Point (AP)

> A network point of attachment in IEEE 802.11 wireless LAN
> [802.11].

Basic Service Set (BSS)

> The basic building block of an IEEE 802.11 wireless LAN [802.11].
> The BSS consists of a group of any number of 802.11 stations.

Extended Service Set (ESS)

> A set of infrastructure BSSs in IEEE 802.11 wireless LAN [802.11],
> where the access points communicate amongst themselves to forward
> traffic from one BSS to another to facilitate movement of stations

      between BSSs.

   Access Domain

      A set of access networks of a specific link layer technology among
      which a peer is allowed to change its network points of attachment
      without changing its serving authenticator. An IEEE 802.11r
      mobility domain [802.11r] is an access domain.

   Inter-Access-Domain Handover

      A handover across multiple access domains.

   Inter-ESS Handover

      An 802.11 handover across multiple ESSs.

   Intra-AAA-Domain Handover (Intra-Domain Handover)

      A handover within the same AAA domain.

   Inter-AAA-Domain Handover (Inter-Domain Handover)

      A handover across multiple AAA domains.

   Intra-Technology Handover

      A handover within the same link layer technology.

   Inter-Technology Handover

      A handover across different link layer technologies.

   Inter-Authenticator Handover

      A handover across multiple authenticators. An inter-authenticator
      handover includes an inter-access-domain handover, an inter-ESS
      handover, an inter-AAA-domain handover, an inter-technology
      handover, and any possible combination of them.

   ERP (EAP Extensions for EAP Re-authentication Protocol)

      Extensions to EAP and EAP keying hierarchy to support an EAP
      method-independent protocol for efficient re-authentication
      between the peer and an EAP re-authentication server defined in
      [RFC5296].

3. **Problem Statement**

   The basic mechanism of handover is a three-step procedure involving
   i) discovery of candidate network points of attachment and their
   authenticators, ii) network selection procedure to determine the
   appropriate candidate network point of attachment and iii) handover
   or setting up L2 and L3 connectivity to the target network point of
   attachment. Currently, as part of the third step, network access
   authentication and authorization are performed directly with the
   target network. For example, in IEEE 802.11 wireless LANs [802.11],
   the network access authentication and authorization involves
   performing a new IEEE 802.1X message exchange with the authenticator
   in the target AP to initiate an EAP exchange to the authentication
   server [WPA]. Following a successful EAP authentication, a secure
   association procedure is performed between the peer and the target
   authenticator to derive a new set of link-layer ciphering keys from
   EAP keying material such as the MSK. The third step may require full
   EAP authentication in the absence of any particular optimization for
   handover key management. The handover latency introduced by full EAP
   authentication has proven to be larger than that is acceptable for
   real-time applications scenarios as described in [MQ7]. Hence,
   improvement in the handover latency performance due to EAP is a
   necessary objective for such scenarios.

   There is relevant work undertaken by various standards organizations,
   but these efforts are scoped to a specific link layer technology.
   IEEE 802.11F [802.11f], a trial use document has defined context
   transfer and caching mechanism to transfer some IEEE 802.11 keying
   material between the neighboring APs. However, it has been
   administratively withdrawn since 2006. IEEE 802.11 [802.11] defines
   a pre-authentication mechanism for use in 802.11 wireless networks.
   This mechanism allows peers to pre-authenticate to one or more
   candidate authenticators over the wired medium, by way of the serving
   authenticator. IEEE 802.11r [802.11r] defines Fast BSS transition
   mechanisms involving a definition of a key management hierarchy and
   setup of session keys before the re-association to the target AP in
   the same 802.11r mobility domain. These mechanisms, as indicated
   before, are defined for IEEE 802.11 technologies and are only
   applicable for intra-access-domain handovers and fall short when it
   comes to inter-technology handovers. They also require L2 (e.g.,
   Ethernet) connectivity for transfer of key management signaling to
   the target AP. A solution is needed to enable EAP pre-authentication
   for inter-access-domain or inter-ESS handovers in IEEE 802.11.

   As various flavors of wireless technologies are increasingly
   available, there is a growing demand for seamless inter-technology
   mobility. This is particularly beneficial in the presence of high
   bandwidth, wireless technologies (e.g., IEEE 802.11) with only

hotspot-like coverage while the overlay licensed wireless/cellular
coverage is expensive and relatively low bandwidth. Hence, the
security optimization mechanisms for better handover performance must
be looked at from the IP level so as to make it a common method over
different access technologies.

Optimized solutions for secure inter-authenticator handovers can be
largely seen as security context transfer: ERP [RFC5296] or EAP pre-
authentication. Security context transfer involves transfer of
reusable key context to the new point of attachment. However, the
recent AAA key management requirements [RFC4962] do not recommend
horizontal context transfer of reusable key context because of the
domino effect in which the compromise of an authenticator will lead
to the compromise of another authenticator. ERP uses existing EAP
keying material for deriving a re-authentication key to be
distributed to an ERP server in a visited domain in order to reduce
the handover delay, which eliminates the need for running full EAP
authentication with the EAP server in the home domain for intra-
domain handovers. On the other hand, there are certain cases where
ERP is not applicable or an additional optimization mechanism is
needed to establish a key for the candidate authenticator:

o One case is an inter-domain handover with or without any trust
   relationship between the home and visited AAA domains. If there
   is no trust relationship between the two AAA domains, ERP cannot
   be used in the visited AAA domain, and the EAP server in the home
   AAA domain is the only entity that can authenticate the peer.
   Even if there is a trust relationship between the two AAA domains
   and the visited AAA domain supports ERP, full EAP authentication
   with the EAP server in the home AAA domain is still needed when
   entering the visited AAA domain unless the security policy of the
   home AAA domain allows the same re-authentication root key to be
   shared with the visited AAA domain.

o Another case is an intra-domain, inter-authenticator handover
   where the target authenticator or AAA domain do not support ERP,
   or ERP needs to be performed proactively before the peer arrives
   at the target authenticator.

EAP pre-authentication discussed in this document is mainly to deal
with these cases while a general solution for the EAP pre-
authentication problem can be used for other handover cases.

EAP pre-authentication has general applicability to various
deployment scenarios in which proactive signaling can take effect.
In other words, applicability of EAP pre-authentication is limited to
the scenarios where candidate authenticators can be discovered and an
accurate prediction of movement can be easily made. Also the

effectiveness of EAP pre-authentication may be less significant for
particular inter-technology handover scenarios where simultaneous use
of multiple technologies is not a major concern.

In EAP pre-authentication, AAA-based authentication and authorization
for a candidate authenticator is performed while ongoing data
communication is in progress via the serving network. The goal of
EAP pre-authentication is to avoid AAA signaling for EAP when or soon
after the peer moves. There are several AAA issues related to EAP
pre-authentication. The pre-authentication AAA issues are described
in Section 6.

Figure 1 shows the functional elements that are related to EAP pre-
authentication. These functional elements include a peer, a serving
authenticator, a candidate authenticator and an AAA/EAP server or
AAA/EAP servers. When the serving and candidate authenticators
belong to different AAA domains, the candidate authenticator may use
a different AAA server and user credentials than those were used by
the serving authenticator to authenticate the peer.

```
+------+           +-------------+     +------+
| Peer |---------|   Serving   |    /         \
|      |           |Authenticator|---/           \
+------+           +-------------+  /             \
   .                              /               \   +-----------------+
   . Move                        +    IP Network   +---|AAA/EAP Server(s)|
   .                              \               /    +-----------------+
   v                 +-------------+  \           /
                     |  Candidate  |---\         /
                     |Authenticator|    \       /
                     +-------------+     +------+
```
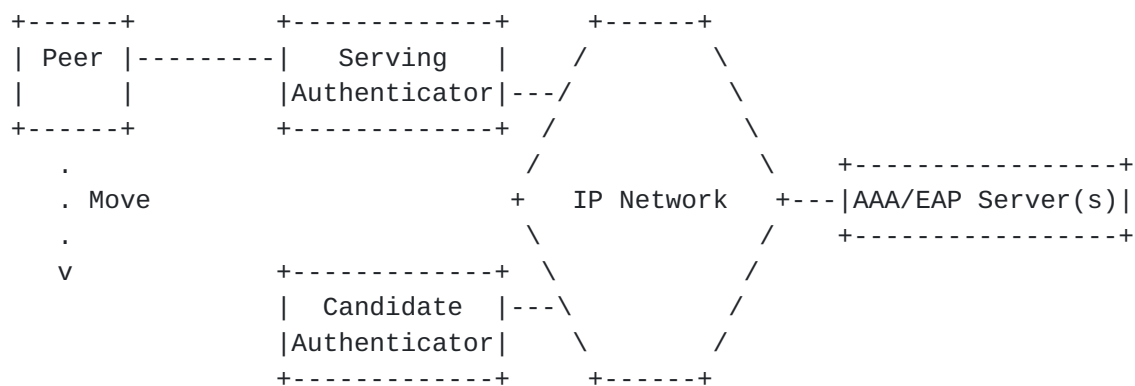
        Figure 1: EAP Pre-authentication Functional Elements

A peer is attached to the serving access network. Before the peer
performs handover from the serving access network to a candidate
access network, it performs EAP pre-authentication with a candidate
authenticator via the serving access network. The peer may perform
EAP pre-authentication with one or more candidate authenticators. It
is assumed that each authenticator has an IP address. It is assumed
that there is at least one candidate authenticator in each candidate
access network while the serving access network may or may not have a
serving authenticator. The serving and candidate access networks may
use different link layer technologies.

Each authenticator is either a standalone authenticator or pass-
through authenticator [RFC3748]. When an authenticator acts as a
standalone authenticator, it also has the functionality of an EAP

server. When an authenticator acts as a pass-through authenticator, it communicates with the EAP server typically implemented on a AAA server using a AAA transport protocol such as RADIUS [RFC2865] and Diameter [RFC3588].

If the candidate authenticator uses an MSK [RFC5247] for generating lower-layer ciphering keys, EAP pre-authentication is used for proactively generating an MSK for the candidate authenticator.

4. Usage Scenarios

There are two scenarios for how EAP pre-authentication signaling can happen among a peer, serving authenticator, candidate authenticator and AAA server, depending on how the serving authenticator is involved in the EAP pre-authentication signaling. It is assumed that in both scenarios there is no direct L2 connectivity between a peer and a candidate authenticator. No security association between the serving authenticator and the candidate authenticator is required for either pre-authentication scenario (see Section 7 for more detailed discussion).

4.1. Direct Pre-authentication

Direct pre-authentication signaling is shown in Figure 2.

```
   Peer                 Serving              Candidate            AAA/EAP
                      Authenticator        Authenticator          Server
                         (SA)                 (CA)
    |                     |                    |                   |
    |                     |                    |                   |
    |        Peer-CA Signaling (L3)            |       AAA         |
    |<-----------------+------------------>|<---------------->|
    |                     |                    |                   |
    |                     |                    |                   |
```
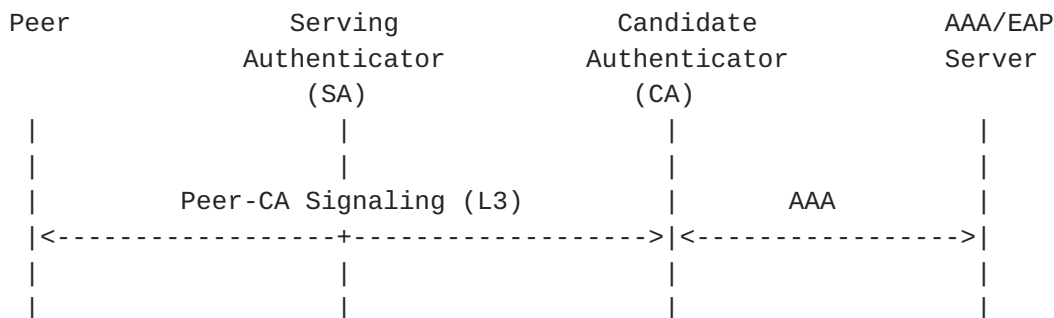
Figure 2: Direct Pre-authentication

In this type of pre-authentication, the serving authenticator forwards the EAP pre-authentication traffic as it would any other data traffic or there may be no serving authenticator at all in the serving access network.

[I-D.ietf-pana-preauth] is identified as a protocol to realize direct pre-authentication.

4.2. Indirect Pre-authentication

   In indirect pre-authentication, it is assumed that a trust
   relationship exists between the serving network (or serving AAA
   domain) and candidate network (or candidate AAA domain). Indirect
   pre-authentication signaling is shown in Figure 3.

```
      Peer                  Serving                 Candidate              AAA/EAP
                          Authenticator           Authenticator            Server
                              (SA)                     (CA)
         |                     |                        |                      |
         |                     |                        |                      |
         | Peer-SA Signaling | |   SA-CA Signaling    | |        AAA           |
         |     (L2 or L3)      |          (L3)          |                      |
         |<----------------->|<------------------->|<----------------->|
         |                     |                        |                      |
         |                     |                        |                      |
```
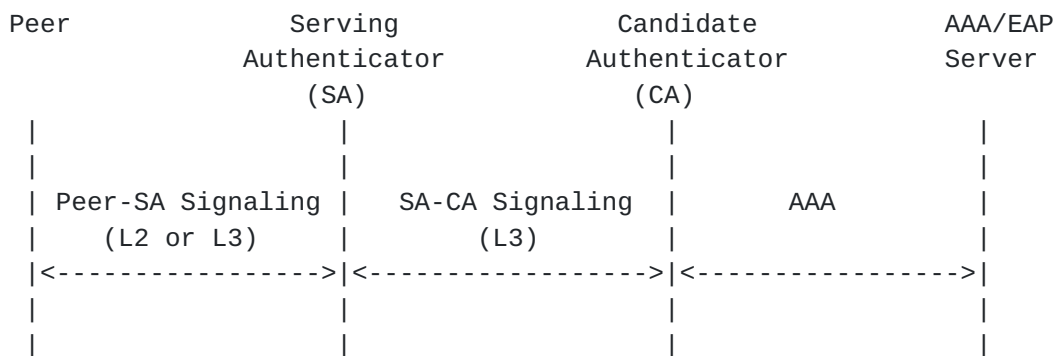
                    Figure 3: Indirect Pre-authentication

   With indirect pre-authentication, the serving authenticator is
   involved in EAP pre-authentication signaling. Indirect pre-
   authentication is needed if the peer cannot discover the candidate
   authenticator's IP address or if IP communication is not available
   due to security or network topology reasons.

   Indirect pre-authentication signaling between a peer and a candidate
   authenticator consists of peer to serving authenticator signaling
   (Peer-SA signaling) and serving authenticator to candidate
   authenticator signaling (SA-CA signaling).

   SA-CA signaling is performed over L3.

   Peer-SA signaling is performed over L2 or L3.

   The role of the serving authenticator in indirect pre-authentication
   is to forward EAP pre-authentication signaling between the peer and
   the candidate authenticator and not to act as an authenticator, while
   it acts as an authenticator for normal authentication signaling.
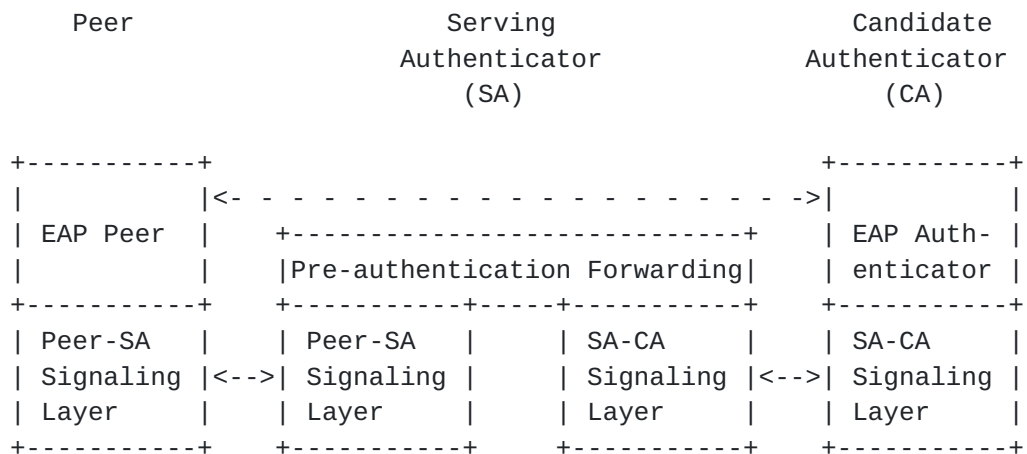   This is illustrated in Figure 4.

```
           Peer                      Serving                 Candidate
                                  Authenticator           Authenticator
                                      (SA)                     (CA)

      +-----------+                                     +-----------+
      |           |<- - - - - - - - - - - - - - - - ->|           |
      | EAP Peer  |     +------------------------------+    | EAP Auth- |
      |           |     |Pre-authentication Forwarding|    | enticator |
      +-----------+     +-----------+-----+-----------+    +-----------+
      | Peer-SA   |     | Peer-SA   |     | SA-CA     |    | SA-CA     |
      | Signaling |<-->| Signaling |     | Signaling |<-->| Signaling |
      | Layer     |     | Layer     |     | Layer     |    | Layer     |
      +-----------+     +-----------+     +-----------+    +-----------+
```

             Figure 4: Indirect Pre-authentication Layering Model

5. Architectural Considerations

   There are two architectural issues relating to pre-authentication:
   authenticator discovery and context binding.

5.1. Authenticator Discovery

   In general, pre-authentication requires an address of a candidate
   authenticator to be discovered either by a peer or by a serving
   authenticator prior to handover. An authenticator discovery protocol
   is typically defined as a separate protocol from a pre-authentication
   protocol. For both intra-domain and inter-domain handover, the IP
   address of a candidate authenticator must be reachable by the peer or
   the serving authenticator that is performing the pre-authentication.
   For example, IEEE 802.21 Information Service (IS) [802.21] provides a
   link layer independent mechanism for obtaining neighboring network
   information by defining a set of Information Elements (IEs), where
   one of the IEs is defined to contain an IP address of a point of
   attachment. IEEE 802.21 IS queries for such an IE may be used as a
   method for authenticator discovery.

   If IEEE 802.21 IS or a similar mechanism is used, an authenticator
   discovery requires a database on the neighboring network information.
   Provisioning of a server with such a database is another issue.

5.2. Context Binding

   When a candidate authenticator uses different EAP transport protocols
   for normal authentication and pre-authentication, a mechanism is
   needed to bind link layer independent context carried over pre-
   authentication signaling to the link layer specific context of the

link to be established between the peer and the candidate
authenticator. The link layer independent context includes the
identities of the peer and authenticator as well as the MSK. The
link layer specific context includes link layer addresses of the peer
and the candidate authenticator. Such context binding can happen
before or after the peer changes its point of attachment.

There are at least two possible approaches to address the context
binding issue. The first approach is based on communicating the link
layer context as opaque data via pre-authentication signaling. The
second approach is based on running EAP over the link layer of the
candidate authenticator after the peer arrives at the authenticator
using short-term credentials generated via pre-authentication. In
this case, the short-term credentials are shared between the peer and
the candidate authenticator, where the candidate authenticator is
also the EAP server for the EAP method execution performed after the
peer arrives at the target authenticator resides in the
authenticator. In both approaches, context binding needs to be
securely made between the peer and the candidate authenticator.
Also, the peer is not fully authorized by the candidate authenticator
until the peer completes the link layer specific secure association
procedure with the authenticator using the link layer signaling.

[6]. AAA Issues

Most of the AAA documents today do not distinguish between a normal
authentication and a pre-authentication and this creates a set of
open issues:

Pre-authentication authorization: Many users may not be allowed to
   have more than one logon session at the time. This means that
   when such users actively engage in an active session (as a result
   of a previously valid authentication), they will not be able to
   perform pre-authentication. The AAA server currently has no way
   of distinguishing between a normal authentication request and a
   pre-authentication request.

Pre-authentication lifetime: Currently AAA protocols define
   attributes carrying lifetime information for a normal
   authentication session. Even when a user profile and the AAA
   server supports pre-authentication, the lifetime for a pre-
   authentication session is typically valid only for a short amount
   of time because the peer has not completed its authentication at
   the target link layer. It is currently not possible for a AAA
   server to indicate to the AAA client or a peer the lifetime of the
   pre-authenticated session unless AAA protocols are extended to
   carry pre-authentication session lifetime information. In other

words, it is not clear to the peer or the authenticator when the
pre-authentication session will expire.

Pre-authentication retries: It is typically expected that shortly
    following the pre-authentication process, the peer moves to the
    new point of attachment and converts the pre-authentication state
    to a normal authentication state (the procedure for which is not
    the topic of this particular subsection). However, if the peer
    has not yet moved to the new location and realizes that the pre-
    authentication is expiring, it may perform another pre-
    authentication. Some limiting mechanism is needed to avoid
    unlimited number of pre-authentication tries.

Completion of network attachment: Once the peer has successfully
    attached to the new point of attachment, it needs to convert its
    authentication state from pre-authenticated to fully attached and
    authorized. There may need to be a mechanism within the AAA
    protocol to provide this indication to the AAA server if the AAA
    server needs to differentiate between pre-authentication and
    normal authentication. This is important from billing perspective
    where the billing policy does not charge for a pre-authenticated
    peer until the peer is fully attached to the target authenticator.

Session Resumption: In case the peer cycles between a network N1
    with which it has a normal authentication state to another network
    N2 and then back to N1, it should be possible to simply convert
    the full authentication state to a pre-authenticated state. The
    problems around handling session lifetime and keying material
    caching need to be dealt with.

Multiple candidate authenticators: There may be situations where
    the peer may need to make a selection between a number of
    candidate authenticators. In such cases, it is desirable for the
    peer to perform pre-authentication with multiple candidate
    authenticators. In such cases the AAA server may need to be aware
    of the situation.

Inter-technology support: Current specifications on pre-
    authentication mostly deal with homogeneous 802.11 networks. The
    AAA attributes such as Calling-Station-ID [I-D.aboba-radext-wlan]
    may need to be expanded to cover other access technologies.
    Furthermore, inter-technology handovers may require a change of
    the peer identifier as part of the handover. Investigation on the
    best type of identifiers for peers that support multiple access
    technologies is required.

7. Security Considerations

This section specifically covers threats introduced to the EAP model
by pre-authentication. Security issues on general EAP and handover
are described in other documents such as [RFC3748], [RFC4962],
[RFC5169] and [RFC5247].

Since pre-authentication described in this document needs to work
across multiple authenticators, any solution needs to consider the
following security threats.

First, a resource consumption denial of service attack is possible,
where an attacker that is not on the same IP link as the legitimate
peer or the candidate authenticator may send unprotected pre-
authentication messages to the legitimate peer or the candidate
authenticator. As a result, they may spend their computational and
bandwidth resources on processing pre-authentication messages sent by
the attacker. This attack is possible for both direct and indirect
pre-authentication scenarios. To mitigate this attack, the candidate
network or authenticator may apply non-cryptographic packet filtering
so that pre-authentication messages received from only a specific set
of serving networks or authenticators are processed. In addition, a
simple solution for the peer side would be to let the peer always
initiate EAP pre-authentication and not allow EAP pre-authentication
initiation from an authenticator.

Second, consideration for the Channel Binding problem described in
[RFC5247] is needed as lack of Channel Binding may enable an
authenticator to impersonate another authenticator or communicate
incorrect information via out-of-band mechanisms (such as via a AAA
or lower layer protocol) [RFC3748]. It should be noted that it is
relatively easier to launch such an impersonation attack for pre-
authentication than normal authentication because an attacker does
not need to be physically on the same link as the legitimate peer to
send a pre-authentication trigger to the peer.

8. IANA Considerations

This document has no actions for IANA.

9. Acknowledgments

The authors would like to thank Bernard Aboba, Jari Arkko, Ajay
Rajkumar, Maryna Komarova, Charles Clancy, Glen Zorn, Subir Das,
Shubhranshu Singh, Preetida Vinayakray and Rafa Marin Lopez for their
valuable input.

10. Contributors

   The following people contributed to this document.

        Yoshihiro Ohba (yohba@tari.toshiba.com)

        Ashutosh Dutta (adutta@research.telcordia.com)

        Srinivas Sreemanthula (srinivas.sreemanthula@nokia.com)

        Alper E. Yegin (alper.yegin@yegin.org)

        Madjid Nakhjiri (madjid.nakhjiri@motorola.com)

        Mahalingam Mani (mmani@avaya.com)

11. References

11.1. Normative References

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

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

   [RFC4962]   Housley, R. and B. Aboba, "Guidance for Authentication,
               Authorization, and Accounting (AAA) Key Management",
               BCP 132, RFC 4962, July 2007.

   [RFC5247]   Aboba, B., Simon, D., and P. Eronen, "Extensible
               Authentication Protocol (EAP) Key Management Framework",
               RFC 5247, August 2008.

11.2. Informative References

   [RFC2865]   Rigney, C., Willens, S., Rubens, A., and W. Simpson,
               "Remote Authentication Dial In User Service (RADIUS)",
               RFC 2865, June 2000.

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

   [RFC5169]   Clancy, T., Nakhjiri, M., Narayanan, V., and L. Dondeti,
               "Handover Key Management and Re-Authentication Problem
               Statement", RFC 5169, March 2008.

   [RFC5296] Narayanan, V. and L. Dondeti, "EAP Extensions for EAP Re-
              authentication Protocol (ERP)", RFC 5296, August 2008.

   [I-D.aboba-radext-wlan]
              Aboba, B., Malinen, J., Congdon, P., and J. Salowey,
              "RADIUS Attributes for IEEE 802 Networks",
              draft-aboba-radext-wlan-08 (work in progress), June 2008.

   [I-D.ietf-pana-preauth]
              Ohba, Y., "Pre-authentication Support for PANA",
              draft-ietf-pana-preauth-02 (work in progress),
              November 2007.

   [802.21]   IEEE, "Draft Standard for Local and Metropolitan Area
              Networks: Media Independent Handover Services", LAN MAN
              Standards Committee of the IEEE Computer Society 802.21
              D11 2008.

   [802.11]   IEEE, "IEEE Standard for Information technology -
              Telecommunications and information exchange between
              systems - Local and metropolitan area networks - Specific
              requirements Part 11: Wireless LAN Medium Access Control
              (MAC) and Physical Layer (PHY) Specifications", IEEE
              Computer Society 2007.

   [802.11r] IEEE, "Information technology - Telecommunications and
              information exchange between systems - Local and
              metropolitan area networks - Specific requirements - Part
              11: Wireless LAN Medium Access Control (MAC) and Physical
              Layer (PHY) specifications - Amendment 2: Fast BSS
              Transition", LAN MAN Standards Committee of the IEEE
              Computer Society 802.11r D9.0 2008.

   [802.11f] IEEE, "IEEE Trial-Use Recommended Practice for Multi-
              Vendor Access Point Interoperability via an Inter-Access
              Point Protocol Across Distribution Systems Supporting IEEE
              802.11 Operation", IEEE Computer Society 2003.

   [ITU]   ITU-T, "General Characteristics of International Telephone
              Connections and International Telephone Circuits: One-Way
              Transmission Time", ITU-T Recommendation G.114 1998.

   [ETSI]   ETSI, "Telecommunications and Internet Protocol
              Harmonization Over Networks (TIPHON) Release 3: End-to-end
              Quality of Service in TIPHON systems; Part 1: General
              aspects of Quality of Service.", ETSI TR 101 329-6 V2.1.1.

   [WPA]   The Wi-Fi Alliance, "WPA (Wi-Fi Protected Access)", Wi-

Fi WPA v3.1, 2004.

[MQ7]   Lopez, R., Dutta, A., Ohba, Y., Schulzrinne, H., and A.
            Skarmeta, "Network-layer Assisted Mechanism to Optimize
            Authentication Delay During Handoff in 802.11 Networks",
            ACM Mobiquitous 2007.

[WCM]   Dutta, A., Famorali, D., Das, S., Ohba, Y., and R. Lopez,
            "Media-Independent Pre-Authentication Supporting Secure
            Interdomain Handover Optimization Network-layer Assisted
            Mechanism to Optimize", IEEE Wireless Communications April
            2008.

Author's Address

   Yoshihiro Ohba
   Toshiba America Research, Inc.
   1 Telcordia Drive
   Piscataway, NJ 08854
   USA

   Phone: +1 732 699 5365
   Email: yohba@tari.toshiba.com