       Definition of Master Key between PANA Client and Enforcement Point

Abstract

   This document defines a master key used between a client of the
   Protocol for carrying Authentication for Network Access (PANA) and an
   enforcement point, for bootstrapping lower-layer ciphering. The
   master key is derived from the Master Session Key of the Extensible
   Authentication Protocol as a result of successful PANA
   authentication. The master key guarantees cryptographic independence
   among enforcement points bootstrapped from PANA authentication across
   different address families.

Status of This Memo

   This is an Internet Standards Track document.

   This document is a product of the Internet Engineering Task Force
   (IETF). It represents the consensus of the IETF community. It has
   received public review and has been approved for publication by the
   Internet Engineering Steering Group (IESG). Further information on
   Internet Standards is available in Section 2 of RFC 5741.

   Information about the current status of this document, any errata,
   and how to provide feedback on it may be obtained at
   http://www.rfc-editor.org/info/rfc5807.

Copyright Notice

Table of Contents

1. Introduction

   The Protocol for carrying Authentication for Network Access (PANA)
   [RFC5191] is designed to facilitate network access authentication and
   authorization of clients in access networks. It carries Extensible
   Authentication Protocol (EAP) [RFC3748] between a PANA Client (PaC)
   and a PANA Authentication Agent (PAA) where the PAA functions as an
   authentication gateway to the Authentication Server (AS). The PANA
   framework [RFC5193] defines an another entity referred to as an
   Enforcement Point (EP), which resides in the access network and
   allows access (data traffic) of authorized PaCs while preventing
   access of others depending on the PANA authentication and
   authorization result (Figure 1). The EP and PAA may be implemented
   on the same device or separate devices.

```
                                           RADIUS,
                                           Diameter,
         +-----+       PANA          +-----+  LDAP, API, etc. +-----+
         | PaC |<------------------->| PAA |<--------------------->| AS  |
         +-----+                     +-----+                       +-----+
            ^                           ^
            |                           |
            |         +-----+           |
    IKE,    +-------->| EP  |<--------+ ANCP, API, etc.
    4-way handshake,  +-----+
    etc.                 .
                         .
                         .
                         v
                   Data traffic
```
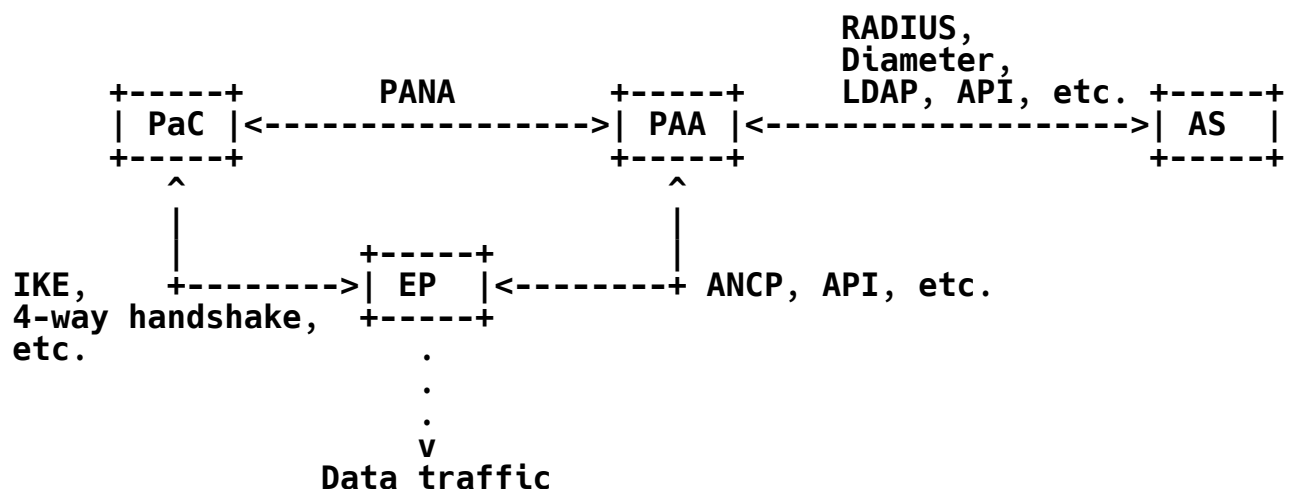
                   Figure 1: PANA Functional Model

   The EP uses non-cryptographic or cryptographic filters to selectively
   allow and discard data packets. These filters may be applied at the
   link-layer or the IP-layer [PANA-IPSEC]. When cryptographic access
   control is used, a secure association protocol [RFC3748] needs to run
   between the PaC and EP. After completion of the secure association
   protocol, link- or network-layer per-packet security (for example,
   IPsec ESP) is enabled for integrity protection, data origin
   authentication, replay protection, and optionally confidentiality
   protection.

   This document defines the PaC-EP Master Key (PEMK) that is used by a
   secure association protocol as the pre-shared secret between the PaC
   and EP to enable cryptographic filters in the access network. The
   PEMK is defined to guarantee cryptographic independence among EPs
   bootstrapped from PANA authentication across different address

families. This document also describes a guideline for distributing
PEMKs from the PAA to EP.

This document does not specify a mechanism for a PaC to know whether
the lower layer requires a secure association protocol or the pre-
shared secret for the secure association protocol needs to be
bootstrapped from PANA authentication. Such a mechanism may be
defined by each lower-layer protocol.

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

This document reuses the following terms defined in [RFC5191]: PaC
(PANA Client), PAA (PANA Authentication Agent), EP (Enforcement
Point), MSK (Master Session Key), PANA Session, and Session
Identifier.

3. PaC-EP Master Key

A PEMK (PaC-EP Master Key) is derived from an available MSK. The
PEMK is 64 octets in length and is calculated as follows:

PEMK = prf+(MSK, "IETF PEMK" | SID | KID | EPID)
        where | denotes concatenation.

o The prf+ function is defined in IKEv2 [RFC4306]. The pseudo-
   random function used for the prf+ function is specified in the
   PRF-Algorithm AVP carried in a PANA-Auth-Request message with 'S'
   (Start) bit set.

o "IETF PEMK" is the ASCII code representation of the non-NULL
   terminated string (excluding the double quotes around it).

o SID is a four-octet Session Identifier [RFC5191].

o KID is the content of the Key-ID AVP [RFC5191] associated with the
   MSK.

o EPID is the identifier of the EP. The first two octets represents
   the AddressType, which contains an Address Family defined in
   [IANAADFAM]. The remaining octets encode the address value. The

length of the address value is determined by the AddressType. The
AddressType is used to discriminate the content and format of the
remaining octets for the address value. The use of the
combination of address family and address value guarantees the
cryptographic independence of PEMKs among multiple EPs that are
bootstrapped from PANA authentication across multiple address
families. How a PaC discovers an EPID is out of the scope of this
document.

3.1. Key Name of PEMK

The key name of the PEMK is defined as follows.

PEMKname = SHA1(EPID | SID | KID), where SHA1 denotes the SHA-1
algorithm specified in [SHS]. Inclusion of the EPID, SID, and KID
provides uniqueness of PEMK names among multiple PaC-EP pairs under a
given PAA.

3.2. Scope of PEMK

One PEMK is used between one PaC and one EP. A PEMK MUST NOT be
shared among multiple PaCs or EPs.

3.3. Context of PEMK

A PEMK is used as the pre-shared key of the secure association
protocol in the scope of the PEMK. A PEMK MUST NOT be used for any
other usage.

3.4. Lifetime of PEMK

The lifetime of a PEMK MUST be less than or equal to the lifetime of
the MSK from which it is derived. At the end of the lifetime, the
PEMK and its associated states MUST be deleted.

4. Security Considerations

The following considerations are specifically made to follow the
Authentication, Authorization, and Accounting (AAA) key management
guidance [RFC4962]. Other AAA key management requirements such as
key lifetime, key scope, key context, and key name are described in
Section 3.

4.1. Channel Binding

Since the device identifier of the EP is involved in the key
derivation function, Channel Binding on a PEMK is made between the
PaC and PAA at the time when the PEMK is generated. If a malicious

EP advertises a different device identifier than that registered with
the PAA, the malicious attempt will not succeed since the secure
association protocol will fail due to the difference in the PEMK
values calculated by the PaC and the EP.

4.2. Guideline for Distributing PEMK from PAA to EP

When an EP is implemented on the same device as the PAA, no protocol
needs to be used for distributing a PEMK from the PAA to the EP.

In the case where the EP is implemented on a separate device from the
PAA, a protocol is needed to distribute a PEMK from the PAA to the
EP. Such a key distribution protocol may depend on the architecture
and deployment using PANA. A key distribution protocol for a PEMK
MUST ensure that the PEMK is encrypted as well as integrity and
replay protected, with a security association between the PAA and EP,
where the security association MUST be cryptographically bound to the
identities of the PAA and EP known to the PaC.

5. Acknowledgments

We would like to thank Jari Arkko, Basavaraj Patil, Pasi Eronen, Russ
Mundy, Alexey Melnikov, and all members of the PANA working group for
their valuable comments to this document.

6. References

6.1. Normative References

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

[RFC4306]   Kaufman, C., "Internet Key Exchange (IKEv2) Protocol",
               RFC 4306, December 2005.

[RFC5191]   Forsberg, D., Ohba, Y., Patil, B., Tschofenig, H., and
               A. Yegin, "Protocol for Carrying Authentication for
               Network Access (PANA)", RFC 5191, May 2008.

[SHS]   National Institute of Standards and Technology, U.S.
               Department of Commerce, "Secure Hash Standard", NIST
               FIPS PUB 180-2, August 2002.

[IANAADFAM]   IANA, "Address Family Numbers", http://www.iana.org.

6.2. Informative References

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

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

   [RFC5193]   Jayaraman, P., Lopez, R., Ohba, Y., Parthasarathy, M.,
                  and A. Yegin, "Protocol for Carrying Authentication for
                  Network Access (PANA) Framework", RFC 5193, May 2008.

   [PANA-IPSEC]   Parthasarathy, M., "PANA Enabling IPsec based Access
                  Control", Work in Progress, July 2005.

Authors' Addresses

   Yoshihiro Ohba
   Toshiba Corporate Research and Development Center
   1 Komukai-Toshiba-cho
   Saiwai-ku, Kawasaki, Kanagawa 212-8582
   Japan

   Phone: +81 44 549 2230
   EMail: yoshihiro.ohba@toshiba.co.jp

   Alper Yegin
   Samsung
   Istanbul
   Turkey

   EMail: alper.yegin@yegin.org