Key Exchange Delegation Record for the DNS

Status of this Memo

Copyright Notice

ABSTRACT

   This note describes a mechanism whereby authorisation for one node to
   act as key exchanger for a second node is delegated and made
   available via the Secure DNS. This mechanism is intended to be used
   only with the Secure DNS. It can be used with several security
   services. For example, a system seeking to use IP Security [RFC-
   1825, RFC-1826, RFC-1827] to protect IP packets for a given
   destination can use this mechanism to determine the set of authorised
   remote key exchanger systems for that destination.

1. INTRODUCTION

   The Domain Name System (DNS) is the standard way that Internet nodes
   locate information about addresses, mail exchangers, and other data
   relating to remote Internet nodes. [RFC-1035, RFC-1034] More
   recently, Eastlake and Kaufman have defined standards-track security
   extensions to the DNS. [RFC-2065] These security extensions can be
   used to authenticate signed DNS data records and can also be used to
   store signed public keys in the DNS.

   The KX record is useful in providing an authenticatible method of
   delegating authorisation for one node to provide key exchange
   services on behalf of one or more, possibly different, nodes. This
   note specifies the syntax and semantics of the KX record, which is
   currently in limited deployment in certain IP-based networks. The

reader is assumed to be familiar with the basics of DNS, including
familiarity with [RFC-1035, RFC-1034]. This document is not on the
IETF standards-track and does not specify any level of standard.
This document merely provides information for the Internet community.

1.1 Identity Terminology

This document relies upon the concept of "identity domination". This
concept might be new to the reader and so is explained in this
section. The subject of endpoint naming for security associations
has historically been somewhat contentious. This document takes no
position on what forms of identity should be used. In a network,
there are several forms of identity that are possible.

For example, IP Security has defined notions of identity that
include: IP Address, IP Address Range, Connection ID, Fully-Qualified
Domain Name (FQDN), and User with Fully Qualified Domain Name (USER
FQDN).

A USER FQDN identity dominates a FQDN identity. A FQDN identity in
turn dominates an IP Address identity. Similarly, a Connection ID
dominates an IP Address identity. An IP Address Range dominates each
IP Address identity for each IP address within that IP address range.
Also, for completeness, an IP Address identity is considered to
dominate itself.

2. APPROACH

This document specifies a new kind of DNS Resource Record (RR), known
as the Key Exchanger (KX) record. A Key Exchanger Record has the
mnemonic "KX" and the type code of 36. Each KX record is associated
with a fully-qualified domain name. The KX record is modeled on the
MX record described in [Part86]. Any given domain, subdomain, or host
entry in the DNS might have a KX record.

2.1 IPsec Examples

In these two examples, let S be the originating node and let D be the
destination node. S2 is another node on the same subnet as S. D2 is
another node on the same subnet as D. R1 and R2 are IPsec-capable
routers. The path from S to D goes via first R1 and later R2. The
return path from D to S goes via first R2 and later R1.

IETF-standard IP Security uses unidirectional Security Associations
[RFC-1825]. Therefore, a typical IP session will use a pair of
related Security Associations, one in each direction. The examples
below talk about how to setup an example Security Association, but in
practice a pair of matched Security Associations will normally be

used.

2.1.1 Subnet-to-Subnet Example

If neither S nor D implements IPsec, security can still be provided
between R1 and R2 by building a secure tunnel. This can use either
AH or ESP.

```
    S ---+                                            +----D
         |                                            |
         +- R1 -----[zero or more routers]-------R2-+
         |                                            |
    S2---+                                            +----D2
```
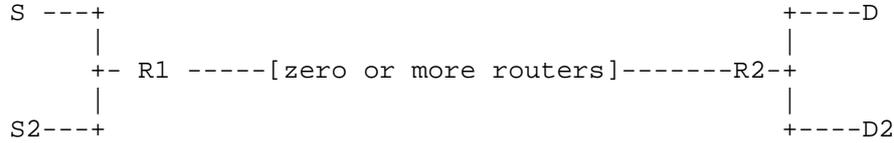
Figure 1: Network Diagram for Subnet-to-Subnet Example

In this example, R1 makes the policy decision to provide the IPsec
service for traffic from R1 destined for R2. Once R1 has decided
that the packet from S to D should be protected, it performs a secure
DNS lookup for the records associated with domain D. If R1 only
knows the IP address for D, then a secure reverse DNS lookup will be
necessary to determine the domain D, before that forward secure DNS
lookup for records associated with domain D. If these DNS records of
domain D include a KX record for the IPsec service, then R1 knows
which set of nodes are authorised key exchanger nodes for the
destination D.

In this example, let there be at least one KX record for D and let
the most preferred KX record for D point at R2. R1 then selects a
key exchanger (in this example, R2) for D from the list obtained from
the secure DNS. Then R1 initiates a key management session with that
key exchanger (in this example, R2) to setup an IPsec Security
Association between R1 and D. In this example, R1 knows (either by
seeing an outbound packet arriving from S destined to D or via other
methods) that S will be sending traffic to D. In this example R1's
policy requires that traffic from S to D should be segregated at
least on a host-to-host basis, so R1 desires an IPsec Security
Association with source identity that dominates S, proxy identity
that dominates R1, and destination identity that dominates R2.

In turn, R2 is able to authenticate the delegation of Key Exchanger
authorisation for target S to R1 by making an authenticated forward
DNS lookup for KX records associated with S and verifying that at
least one such record points to R1. The identity S is typically
given to R2 as part of the key management process between R1 and R2.

If D initially only knows the IP address of S, then it will need to
perform a secure reverse DNS lookup to obtain the fully-qualified
domain name for S prior to that secure forward DNS lookup.

If R2 does not receive an authenticated DNS response indicating that
R1 is an authorised key exchanger for S, then D will not accept the
SA negotiation from R1 on behalf of identity S.

If the proposed IPsec Security Association is acceptable to both R1
and R2, each of which might have separate policies, then they create
that IPsec Security Association via Key Management.

Note that for unicast traffic, Key Management will typically also
setup a separate (but related) IPsec Security Association for the
return traffic. That return IPsec Security Association will have
equivalent identities. In this example, that return IPsec Security
Association will have a source identity that dominates D, a proxy
identity that dominates R2, and a destination identity that dominates
R1.

Once the IPsec Security Association has been created, then R1 uses it
to protect traffic from S destined for D via a secure tunnel that
originates at R1 and terminates at R2. For the case of unicast, R2
will use the return IPsec Security Association to protect traffic
from D destined for S via a secure tunnel that originates at R2 and
terminates at R1.

2.1.2 Subnet-to-Host Example

Consider the case where D and R1 implement IPsec, but S does not
implement IPsec, which is an interesting variation on the previous
example. This example is shown in Figure 2 below.

```
    S ---+
         |
         +- R1 -----[zero or more routers]-------D
         |
    S2---+
```
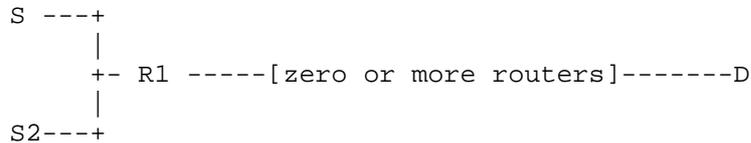
Figure 2: Network Diagram for Subnet-to-Host Example

In this example, R1 makes the policy decision that IP Security is
needed for the packet travelling from S to D. Then, R1 performs the
secure DNS lookup for D and determines that D is its own key
exchanger, either from the existence of a KX record for D pointing to
D or from an authenticated DNS response indicating that no KX record
exists for D. If R1 does not initially know the domain name of D,
then prior to the above forward secure DNS lookup, R1 performs a

secure reverse DNS lookup on the IP address of D to determine the
fully-qualified domain name for that IP address. R1 then initiates
key management with D to create an IPsec Security Association on
behalf of S.

In turn, D can verify that R1 is authorised to create an IPsec
Security Association on behalf of S by performing a DNS KX record
lookup for target S. R1 usually provides identity S to D via key
management. If D only has the IP address of S, then D will need to
perform a secure reverse lookup on the IP address of S to determine
domain name S prior to the secure forward DNS lookup on S to locate
the KX records for S.

If D does not receive an authenticated DNS response indicating that
R1 is an authorised key exchanger for S, then D will not accept the
SA negotiation from R1 on behalf of identity S.

If the IPsec Security Association is successfully established between
R1 and D, that IPsec Security Association has a source identity that
dominates S's IP address, a proxy identity that dominates R1's IP
address, and a destination identity that dominates D's IP address.

Finally, R1 begins providing the security service for packets from S
that transit R1 destined for D. When D receives such packets, D
examines the SA information during IPsec input processing and sees
that R1's address is listed as valid proxy address for that SA and
that S is the source address for that SA. Hence, D knows at input
processing time that R1 is authorised to provide security on behalf
of S. Therefore packets coming from R1 with valid IP security that
claim to be from S are trusted by D to have really come from S.

2.1.3 Host to Subnet Example

   Now consider the above case from D's perspective (i.e. where D is
   sending IP packets to S). This variant is sometimes known as the
   Mobile Host or "roadwarrior" case. The same basic concepts apply, but
   the details are covered here in hope of improved clarity.

```
        S ---+
             |
             +- R1 -----[zero or more routers]-------D
             |
        S2---+
```
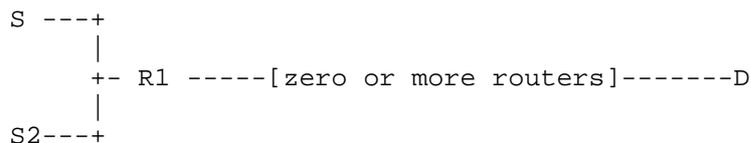
   Figure 3: Network Diagram for Host-to-Subnet Example

   In this example, D makes the policy decision that IP Security is
   needed for the packets from D to S. Then D performs the secure DNS
   lookup for S and discovers that a KX record for S exists and points
   at R1. If D only has the IP address of S, then it performs a secure
   reverse DNS lookup on the IP address of S prior to the forward secure
   DNS lookup for S.

   D then initiates key management with R1, where R1 is acting on behalf
   of S, to create an appropriate Security Association. Because D is
   acting as its own key exchanger, R1 does not need to perform a secure
   DNS lookup for KX records associated with D.

   D and R1 then create an appropriate IPsec Security Security
   Association. This IPsec Security Association is setup as a secure
   tunnel with a source identity that dominates D's IP Address and a
   destination identity that dominates R1's IP Address. Because D
   performs IPsec for itself, no proxy identity is needed in this IPsec
   Security Association. If the proxy identity is non-null in this
   situation, then the proxy identity must dominate D's IP Address.

   Finally, D sends secured IP packets to R1. R1 receives those
   packets, provides IPsec input processing (including appropriate
   inner/outer IP address validation), and forwards valid packets along
   to S.

2.2 Other Examples

   This mechanism can be extended for use with other services as well.
   To give some insight into other possible uses, this section discusses
   use of KX records in environments using a Key Distribution Center
   (KDC), such as Kerberos [KN93], and a possible use of KX records in
   conjunction with mobile nodes accessing the network via a dialup
   service.

2.2.1 KDC Examples

   This example considers the situation of a destination node
   implementing IPsec that can only obtain its Security Association
   information from a Key Distribution Center (KDC). Let the KDC
   implement both the KDC protocol and also a non-KDC key management
   protocol (e.g. ISAKMP). In such a case, each client node of the KDC
   might have its own KX record pointing at the KDC so that nodes not
   implementing the KDC protocol can still create Security Associations
   with each of the client nodes of the KDC.

   In the event the session initiator were not using the KDC but the
   session target was an IPsec node that only used the KDC, the
   initiator would find the KX record for the target pointing at the

KDC. Then, the external key management exchange (e.g. ISAKMP) would
be between the initiator and the KDC. Then the KDC would distribute
the IPsec SA to the KDC-only IPsec node using the KDC. The IPsec
traffic itself could travel directly between the initiator and the
destination node.

In the event the initiator node could only use the KDC and the target
were not using the KDC, the initiator would send its request for a
key to the KDC. The KDC would then initiate an external key
management exchange (e.g. ISAKMP) with a node that the target's KX
record(s) pointed to, on behalf of the initiator node.

The target node could verify that the KDC were allowed to proxy for
the initiator node by looking up the KX records for the initiator
node and finding a KX record for the initiator that listed the KDC.

Then the external key exchange would be performed between the KDC and
the target node. Then the KDC would distribute the resulting IPsec
Security Association to the initiator. Again, IPsec traffic itself
could travel directly between the initiator and the destination.

2.2.2 Dial-Up Host Example

   This example outlines a possible use of KX records with mobile hosts
   that dial into the network via PPP and are dynamically assigned an IP
   address and domain-name at dial-in time.

   Consider the situation where each mobile node is dynamically assigned
   both a domain name and an IP address at the time that node dials into
   the network. Let the policy require that each mobile node act as its
   own Key Exchanger. In this case, it is important that dial-in nodes
   use addresses from one or more well known IP subnets or address pools
   dedicated to dial-in access. If that is true, then no KX record or
   other action is needed to ensure that each node will act as its own
   Key Exchanger because lack of a KX record indicates that the node is
   its own Key Exchanger.

   Consider the situation where the mobile node's domain name remains
   constant but its IP address changes. Let the policy require that
   each mobile node act as its own Key Exchanger. In this case, there
   might be operational problems when another node attempts to perform a
   secure reverse DNS lookup on the IP address to determine the
   corresponding domain name. The authenticated DNS binding (in the
   form of a PTR record) between the mobile node's currently assigned IP
   address and its permanent domain name will need to be securely
   updated each time the node is assigned a new IP address. There are
   no mechanisms for accomplishing this that are both IETF-standard and
   widely deployed as of the time this note was written. Use of Dynamic

   DNS Update without authentication is a significant security risk and
   hence is not recommended for this situation.

3. SYNTAX OF KX RECORD

   A KX record has the DNS TYPE of "KX" and a numeric value of 36. A KX
   record is a member of the Internet ("IN") CLASS in the DNS. Each KX
   record is associated with a <domain-name> entry in the DNS. A KX
   record has the following textual syntax:

        <domain-name> IN KX <preference> <domain-name>

   For this description, let the <domain-name> item to the left of the
   "KX" string be called <domain-name 1> and the <domain-name> item to
   the right of the "KX" string be called <domain-name 2>. <preference>
   is a non-negative integer.

   Internet nodes about to initiate a key exchange with <domain-name 1>
   should instead contact <domain-name 2> to initiate the key exchange
   for a security service between the initiator and <domain-name 2>. If
   more than one KX record exists for <domain-name 1>, then the
   <preference> field is used to indicate preference among the systems
   delegated to. Lower values are preferred over higher values. The
   <domain-name 2> is authorised to provide key exchange services on
   behalf of <domain-name 1>. The <domain-name 2> MUST have a CNAME
   record, an A record, or an AAAA record associated with it.

3.1 KX RDATA format

   The KX DNS record has the following RDATA format:

      +--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
      | PREFERENCE |
      +--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
      /   EXCHANGER   /
      /   /
      +--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+

   where:

   PREFERENCE   A 16 bit non-negative integer which specifies the
                   preference given to this RR among other KX records
                   at the same owner. Lower values are preferred.

   EXCHANGER   A <domain-name> which specifies a host willing to
                   act as a mail exchange for the owner name.

   KX records MUST cause type A additional section processing for the
   host specified by EXCHANGER. In the event that the host processing
   the DNS transaction supports IPv6, KX records MUST also cause type
   AAAA additional section processing.

   The KX RDATA field MUST NOT be compressed.

4. SECURITY CONSIDERATIONS

   KX records MUST always be signed using the method(s) defined by the
   DNS Security extensions specified in [RFC-2065]. All unsigned KX
   records MUST be ignored because of the security vulnerability caused
   by assuming that unsigned records are valid. All signed KX records
   whose signatures do not correctly validate MUST be ignored because of
   the potential security vulnerability in trusting an invalid KX
   record.

   KX records MUST be ignored by systems not implementing Secure DNS
   because such systems have no mechanism to authenticate the KX record.

   If a node does not have a permanent DNS entry and some form of
   Dynamic DNS Update is in use, then those dynamic DNS updates MUST be
   fully authenticated to prevent an adversary from injecting false DNS
   records (especially the KX, A, and PTR records) into the Domain Name
   System. If false records were inserted into the DNS without being
   signed by the Secure DNS mechanisms, then a denial-of-service attack
   results. If false records were inserted into the DNS and were
   (erroneously) signed by the signing authority, then an active attack
   results.

   Myriad serious security vulnerabilities can arise if the restrictions
   throuhout this document are not strictly adhered to. Implementers
   should carefully consider the openly published issues relating to DNS
   security [Bell95,Vixie95] as they build their implementations.
   Readers should also consider the security considerations discussed in
   the DNS Security Extensions document [RFC-2065].

5. REFERENCES

   [RFC-1825] Atkinson, R., "IP Authentication Header", RFC 1826,
               August 1995.

   [RFC-1827] Atkinson, R., "IP Encapsulating Security Payload",
               RFC 1827, August 1995.

   [Bell95] Bellovin, S., "Using the Domain Name System for System
            Break-ins", Proceedings of 5th USENIX UNIX Security
            Symposium, USENIX Association, Berkeley, CA, June 1995.
            ftp://ftp.research.att.com/dist/smb/dnshack.ps

   [RFC-2065] Eastlake, D., and C. Kaufman, "Domain Name System
               Security Extensions", RFC 2065, January 1997.

   [RFC-1510] Kohl J., and C. Neuman, "The Kerberos Network
               Authentication Service", RFC 1510, September 1993.

   [RFC-1035] Mockapetris, P., "Domain names - implementation and
               specification", STD 13, RFC 1035, November 1987.

   [RFC-1034] Mockapetris, P., "Domain names - concepts and
               facilities", STD 13, RFC 1034, November 1987.

   [Vixie95] P. Vixie, "DNS and BIND Security Issues", Proceedings of
             the 5th USENIX UNIX Security Symposium, USENIX
             Association, Berkeley, CA, June 1995.
             ftp://ftp.vix.com/pri/vixie/bindsec.psf

ACKNOWLEDGEMENTS

AUTHOR'S ADDRESS

   Randall Atkinson
   Code 5544
   Naval Research Laboratory
   4555 Overlook Avenue, SW
   Washington, DC 20375-5337

   Phone: (DSN) 354-8590
   EMail: atkinson@itd.nrl.navy.mil

Full Copyright Statement