Network Working Group
Internet Draft
draft-rfced-info-atkinson-00.txt

Randall Atkinson
NRL
June 1997

Key Exchange Delegation Record for the DNS
<draft-rfced-info-atkinson-00.txt>

STATUS OF THIS MEMO

This document is an Internet Draft. 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 6 months. Internet Drafts may be updated, replaced, or obsoleted by other documents at any time. It is not appropriate to use Internet Drafts as reference material or to cite them other than as "work in progress".

This particular Internet Draft describes an extension to the Domain Name System that is in limited deployment in certain IP-based networks. It does not specify any level of standard and is not intended for the IETF standards-track.

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 [Atk95a, Atk95b, Atk95c] 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. [Mock87a, Mock87b] More recently, Eastlake and Kaufman have defined standards-track security extensions to the DNS. [EK97] 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 [Mock87a, Mock87b]. 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.

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 <to be assigned by IANA>. 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. 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 [Atk95a]. 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.

In this example, the decision to provide the IPsec service for traffic from R1 destined for R2 is made by R1. Once R1 has

decided that the packet to D should be protected, it performs a secure DNS lookup for the records associated with domain D. If these records include a KX record for the IPsec service, then R1 knows which set of nodes are possible 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 on behalf of S. R2 is able to authenticate the delegation of Key Exchanger authorisation for target S to R1 by making an authenticated DNS lookup for KX records associated with S and verifying that at least one such record points to R1.

If the key exchanger for D (in this example, R2) authentically informs R1 via the key management that the IPsec Security Association should have source address of S, proxy address of R1, and destination address of R2, then R1 sets up such an association with R2 to protect traffic from S to D. Otherwise, R1 creates an IPsec Security Association for a secure tunnel with source address of S, proxy address of R1, and destination address of D via negotiation with D's key exchanger. In each case, the Security Association has a source identity that is either (1) S or (2) an address range that includes S's address. Once the IPsec Security Association has been created, then R1 uses it to protect traffic from S destined for D. The destination identity is either (1) D or (2) an address range that includes the destination address.

2.1.2 Subnet-to-Host Example

If D implements IPsec but S does not implement IPsec, then things are more interesting. In this case, R1 determines that the security service is needed for the packet. 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 domain D pointing to domain D or from an authenticated DNS response indicating that no KX record exists for domain D. R1 then initiates key management with D to create an IPsec Security Association on behalf of S. 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. If there is no 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 accepted and established, it has a source address of S, a proxy address of R1, and a destination address of D. This IPsec Security Association has a source identity that is either (1) S or (2) an address range that includes S's address and a destination identity that is either (1) D or (2) an address range that includes D's 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). The same concept applies. However, in this case, D determines that the security service is needed for the packets to S. Then D performs the secure DNS lookup for S and discovers that a KX record for S exists and points at R1. D then initiates key management with R1, where R1 is acting on behalf of S, to create an appropriate Security Association.

If R1 indicates to D via key management that the IPsec Security Association should be between D and R1, then the IPsec Security Association is setup as a secure tunnel with a source address of D, a destination address of R1, source identity of either (1) D or (2) an address range including D, and a destination identity of either (1) S or (2) an address range including S.

Otherwise, the IPsec Security Association is setup with source address of D, destination address of S, source identity of either (1) D or (2) an address range including D, and a destination identity of either (1) S or (2) an address range including S.

Finally, D sends secured IP packets to the IPsec SA's destination. If the IPsec SA destination is R1, then R1 receives those packets, provides IPsec input processing, and forwards valid packets along to S. Again, authenticated DNS lookups for KX records is used to authenticate the delegation of Key Exchanger authority for a particular identity to a particular Key Exchanger node.

2.2 Other Examples

This mechanism can be extended for use with other services as well. For example, consider a destination node implementing IPsec that can only obtain its Security Association information from a key distribution center (for example, using Kerberos [KN93]). If that node's key distribution center implemented key management gateway capabilities that could negotiate security associations using a different key management protocol (e.g. ISAKMP), then that destination node might have a KX record pointing at its key distribution center.

In the event the initiator were not using the KDC but the 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 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 node that could only use the KDC. The target could verify that the KDC were allowed to proxy for the node only using the KDC by looking up the KX records for that node only using the KDC and finding a pointer to the KDC. The external key exchange would be performed between the KDC and the target. Then the KDC would distribute the IPsec SA to the initiator. Again, IPsec traffic itself travels directly between the initiator and the destination.

3. SYNTAX OF KX RECORD

A KX record has the DNS TYPE of "KX" and a numeric value of <to be assigned by IANA>. 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:

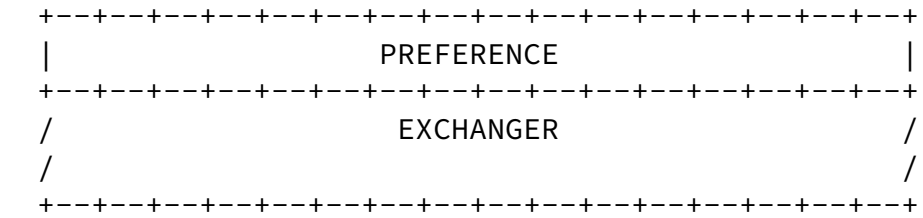
<domain-name> IN KX <preference> <domain-name>

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 be associated with either a Fully Qualified Domain Name, a CNAME record, an A record, or an AAAA record.

3.1 KX RDATA format

The KX DNS record has the following RDATA format:



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 cause type A additional section processing for the host specified by EXCHANGER.

4. SECURITY CONSIDERATIONS

KX records MUST always be signed using the method(s) defined by the DNS Security extensions specified in [EK97]. 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.

Myriad serious security vulnerabilities can arise if the above restrictions are not strictly adhered to.

5. REFERENCES

[Atk95a] R. Atkinson, "IP Security Architecture", RFC-1825, August 1995.

[Atk95b] R. Atkinson, "IP Authentication Header", RFC-1826, August 1995.

[Atk95c] R. Atkinson, "IP Encapsulating Security Payload", RFC-1827, August 1995.

[EK97] D. Eastlake, C. Kaufman, "Domain Name System Security Extensions", RFC-2065, 3 January 1997.

[KN93] J. Kohl & B. Neuman, "The Kerberos Network Authentication Service", RFC-1510, 10 September 1993.

[Mock87a] P. Mockapetris, "Domain names - implementation and specification", RFC-1035, 1 November 1987.

[Mock87b] P. Mockapetris, "Domain names - concepts and facilities", RFC-1036, 1 November 1987

ACKNOWLEDGEMENTS

Development of this DNS record was primarily performed during 1993 through 1995. The author's work on this was sponsored jointly by the Computing Systems Technology Office (CSTO) of the Advanced Research Projects Agency (ARPA) and by the Information Security Program Office (PD71E), Space & Naval Warface Systems Command (SPAWAR).

AUTHOR'S ADDRESS:

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

Email: rja@cs.nrl.navy.mil
Telephone: (DSN) 354-8590

--PART-BOUNDARY=.1970606161952.ZM10146.eos.home.net--