IPSECKEY WG
Internet-Draft
Expires: March 4, 2004

M. Richardson
SSW

September 4, 2003

A method for storing IPsec keying material in DNS.
draft-ietf-ipseckey-rr-07.txt

Status of this Memo

Copyright Notice

Abstract

This document describes a new resource record for DNS. This record may be used to store public keys for use in IPsec systems.

This record replaces the functionality of the sub-type #1 of the KEY Resource Record, which has been obsoleted by RFC3445.

Table of Contents

1. Introduction 3
1.1 Overview 3
1.2 Usage Criteria 3
2. Storage formats 4
2.1 IPSECKEY RDATA format 4
2.2 RDATA format - precedence 4
2.3 RDATA format - algorithm type 4
2.4 RDATA format - gateway type 4
2.5 RDATA format - gateway 5
2.6 RDATA format - public keys 5
3. Presentation formats 7
3.1 Representation of IPSECKEY RRs 7
3.2 Examples 7
4. Security Considerations 9
4.1 Active attacks against unsecured IPSECKEY resource records . . 9
5. IANA Considerations 11
6. Acknowledgments 12
Normative references 13
Non-normative references 14
Author's Address 14
Full Copyright Statement 15

1. Introduction

The type number for the IPSECKEY RR is TBD.

1.1 Overview

The IPSECKEY resource record (RR) is used to publish a public key that is to be associated with a Domain Name System (DNS) name for use with the IPsec protocol suite. This can be the public key of a host, network, or application (in the case of per-port keying).

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 [8].

1.2 Usage Criteria

An IPSECKEY resource record SHOULD be used in combination with DNSSEC unless some other means of authenticating the IPSECKEY resource record is available.

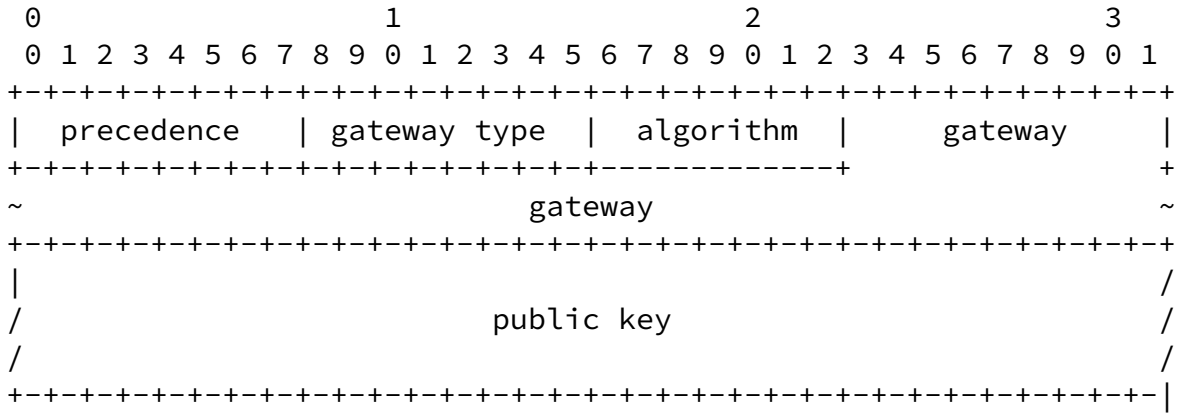
It is expected that there will often be multiple IPSECKEY resource records at the same name. This will be due to the presence of multiple gateways and the need to rollover keys.

This resource record is class independent.

2. Storage formats

2.1 IPSECKEY RDATA format

The RDATA for an IPSECKEY RR consists of a precedence value, a public key, algorithm type, and an optional gateway address.



2.2 RDATA format - precedence

This is an 8-bit precedence for this record. This is interpreted in the same way as the PREFERENCE field described in section 3.3.9 of RFC1035 [2].

Gateways listed in IPSECKEY records with lower precedence are to be attempted first. Where there is a tie in precedence, the order

should be non-deterministic.

2.3 RDATA format - algorithm type

The algorithm type field identifies the public key's cryptographic algorithm and determines the format of the public key field.

A value of 0 indicates that no key is present.

The following values are defined:

1 A DSA key is present, in the format defined in RFC2536 [11]

2 A RSA key is present, in the format defined in RFC3110 [12]

2.4 RDATA format - gateway type

The gateway type field indicates the format of the information that is stored in the gateway field.

The following values are defined:

0 No gateway is present

1 A 4-byte IPv4 address is present

2 A 16-byte IPv6 address is present

3 A wire-encoded domain name is present. The wire-encoded format is self-describing, so the length is implicit. The domain name MUST NOT be compressed.

2.5 RDATA format - gateway

The gateway field indicates a gateway to which an IPsec tunnel may be created in order to reach the entity named by this resource record.

There are three formats:

A 32-bit IPv4 address is present in the gateway field. The data

portion is an IPv4 address as described in section 3.4.1 of RFC1035 [2]. This is a 32-bit number in network byte order.

A 128-bit IPv6 address is present in the gateway field. The data portion is an IPv6 address as described in section 2.2 of RFC1886 [7]. This is a 128-bit number in network byte order.

The gateway field is a normal wire-encoded domain name, as described in section 3.3 of RFC1035 [2]. Compression MUST NOT be used.

2.6 RDATA format - public keys

Both of the public key types defined in this document (RSA and DSA) inherit their public key formats from the corresponding KEY RR formats. Specifically, the public key field contains the algorithm-specific portion of the KEY RR RDATA, which is all of the KEY RR DATA after the first four octets. This is the same portion of the KEY RR that must be specified by documents that define a DNSSEC algorithm. Those documents also specify a message digest to be used for generation of SIG RRs; that specification is not relevant for IPSECKEY RR.

Future algorithms, if they are to be used by both DNSSEC (in the KEY RR) and IPSECKEY, are likely to use the same public key encodings in both records. Unless otherwise specified, the IPSECKEY public key field will contain the algorithm-specific portion of the KEY RR RDATA for the corresponding algorithm. The algorithm must still be

designated for use by IPSECKEY, and an IPSECKEY algorithm type number (which might be different than the DNSSEC algorithm number) must be assigned to it.

The DSA key format is defined in RFC2536 [11]

The RSA key format is defined in RFC3110 [12], with the following changes:

The earlier definition of RSA/MD5 in RFC2065 limited the exponent and modulus to 2552 bits in length. RFC3110 extended that limit to 4096 bits for RSA/SHA1 keys. The IPSECKEY RR imposes no length limit on RSA public keys, other than the 65535 octet limit imposed by the two-octet length encoding. This length extension is applicable only to

IPSECKEY and not to KEY RRs.

3. Presentation formats

3.1 Representation of IPSECKEY RRs

IPSECKEY RRs may appear in a zone data master file. The precedence, gateway type and algorithm and gateway fields are REQUIRED. The base64 encoded public key block is OPTIONAL; if not present, then the

public key field of the resource record MUST be construed as being zero octets in length.

The algorithm field is an unsigned integer. No mnemonics are defined.

If no gateway is to be indicated, then the gateway type field MUST be zero, and the gateway field MUST be "."

The Public Key field is represented as a Base64 encoding of the Public Key. Whitespace is allowed within the Base64 text. For a definition of Base64 encoding, see RFC1521 [3] Section 5.2.

The general presentation for the record as as follows:

```
IN     IPSECKEY ( precedence gateway-type algorithm
                  gateway base64-encoded-public-key )
```

3.2 Examples

An example of a node 192.0.2.38 that will accept IPsec tunnels on its own behalf.

```
38.2.0.192.in-addr.arpa. 7200 IN     IPSECKEY ( 10 1 2
                 192.0.2.38
                 AQNRU3mG7TVTO2BkR47usntb102uFJtugbo6BSGvgqt4AQ== )
```

An example of a node, 192.0.2.38 that has published its key only.

```
38.2.0.192.in-addr.arpa. 7200 IN     IPSECKEY ( 10 0 2
                 .
                 AQNRU3mG7TVTO2BkR47usntb102uFJtugbo6BSGvgqt4AQ== )
```

An example of a node, 192.0.2.38 that has delegated authority to the node 192.0.2.3.

```
38.2.0.192.in-addr.arpa. 7200 IN     IPSECKEY ( 10 1 2
                 192.0.2.3
                 AQNRU3mG7TVTO2BkR47usntb102uFJtugbo6BSGvgqt4AQ== )
```

An example of a node, 192.0.1.38 that has delegated authority to the node with the identity "mygateway.example.com".

```
38.1.0.192.in-addr.arpa. 7200 IN     IPSECKEY ( 10 3 2
                 mygateway.example.com.
                 AQNRU3mG7TVTO2BkR47usntb102uFJtugbo6BSGvgqt4AQ== )
```

An example of a node, 2001:0DB8:0200:1:210:f3ff:fe03:4d0 that has delegated authority to the node 2001:0DB8:c000:0200:2::1

```
$ORIGIN 1.0.0.0.0.0.2.8.B.D.0.1.0.0.2.ip6.int.
0.d.4.0.3.0.e.f.f.f.3.f.0.1.2.0 7200 IN     IPSECKEY ( 10 2 2
                 2001:0DB8:0:8002::2000:1
                 AQNRU3mG7TVTO2BkR47usntb102uFJtugbo6BSGvgqt4AQ== )
```

4. Security Considerations

This entire memo pertains to the provision of public keying material for use by key management protocols such as ISAKMP/IKE (RFC2407) [9].

The IPSECKEY resource record contains information that SHOULD be communicated to the end client in an integral fashion - i.e. free from modification. The form of this channel is up to the consumer of the data - there must be a trust relationship between the end consumer of this resource record and the server. This relationship may be end-to-end DNSSEC validation, a TSIG or SIG(0) channel to another secure source, a secure local channel on the host, or some combination of the above.

The keying material provided by the IPSECKEY resource record is not sensitive to passive attacks. The keying material may be freely disclosed to any party without any impact on the security properties of the resulting IPsec session: IPsec and IKE provide for defense against both active and passive attacks.

Any user of this resource record MUST carefully document their trust model, and why the trust model of DNSSEC is appropriate, if that is the secure channel used.

4.1 Active attacks against unsecured IPSECKEY resource records

This section deals with active attacks against the DNS. These attacks require that DNS requests and responses be intercepted and changed. DNSSEC is designed to defend against attacks of this kind.

The first kind of active attack is when the attacker replaces the keying material with either a key under its control or with garbage.

If the attacker is not able to mount a subsequent man-in-the-middle attack on the IKE negotiation after replacing the public key, then this will result in a denial of service, as the authenticator used by IKE would fail.

If the attacker is able to both to mount active attacks against DNS and is also in a position to perform a man-in-the-middle attack on IKE and IPsec negotiations, then the attacker will be in a position to compromise the resulting IPsec channel. Note that an attacker must be able to perform active DNS attacks on both sides of the IKE

negotiation in order for this to succeed.

The second kind of active attack is one in which the attacker replaces the the gateway address to point to a node under the attacker's control. The attacker can then either replace the public

key or remove it, thus providing an IPSECKEY record of its own to match the gateway address.

This later form creates a simple man-in-the-middle since the attacker can then create a second tunnel to the real destination. Note that, as before, this requires that the attacker also mount an active attack against the responder.

Note that the man-in-the-middle can not just forward cleartext packets to the original destination. While the destination may be willing to speak in the clear, replying to the original sender, the sender will have already created a policy expecting ciphertext. Thus, the attacker will need to intercept traffic from both sides. In some cases, the attacker may be able to accomplish the full intercept by use of Network Addresss/Port Translation (NAT/NAPT) technology.

Note that the danger here only applies to cases where the gateway field of the IPSECKEY RR indicates a different entity than the owner name of the IPSECKEY RR. In cases where the end-to-end integrity of the IPSECKEY RR is suspect, the end client MUST restrict its use of the IPSECKEY RR to cases where the RR owner name matches the content of the gateway field.

5. IANA Considerations

This document updates the IANA Registry for DNS Resource Record Types by assigning type X to the IPSECKEY record.

This document creates an IANA registry for the algorithm type field.

Values 0, 1 and 2 are defined in Section 2.3. Algorithm numbers 3 through 255 can be assigned by IETF Consensus (see RFC2434 [6]).

This document creates an IANA registry for the gateway type field.

Values 0, 1, 2 and 3 are defined in Section 2.4. Algorithm numbers 4 through 255 can be assigned by Standards Action (see RFC2434 [6]).

6. Acknowledgments

My thanks to Paul Hoffman, Sam Weiler, Jean-Jacques Puig, Rob Austein, and Olafur Gurmundsson who reviewed this document carefully. Additional thanks to Olafur Gurmundsson for a reference implementation.

Normative references

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

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

[3] Borenstein, N. and N. Freed, "MIME (Multipurpose Internet Mail Extensions) Part One: Mechanisms for Specifying and Describing the Format of Internet Message Bodies", RFC 1521, September 1993.

[4] Bradner, S., "The Internet Standards Process -- Revision 3", BCP 9, RFC 2026, October 1996.

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

[6] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 2434, October 1998.

Non-normative references

[7] Thomson, S. and C. Huitema, "DNS Extensions to support IP version 6", RFC 1886, December 1995.

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

[9] Piper, D., "The Internet IP Security Domain of Interpretation for ISAKMP", RFC 2407, November 1998.

[10] Eastlake, D., "Domain Name System Security Extensions", RFC 2535, March 1999.

[11] Eastlake, D., "DSA KEYs and SIGs in the Domain Name System (DNS)", RFC 2536, March 1999.

[12] Eastlake, D., "RSA/SHA-1 SIGs and RSA KEYs in the Domain Name System (DNS)", RFC 3110, May 2001.

[13] Massey, D. and S. Rose, "Limiting the Scope of the KEY Resource Record (RR)", RFC 3445, December 2002.

Author's Address

Michael C. Richardson
Sandelman Software Works
470 Dawson Avenue
Ottawa, ON K1Z 5V7
CA

EMail: mcr@sandelman.ottawa.on.ca
URI: http://www.sandelman.ottawa.on.ca/

Full Copyright Statement

Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.