DANE
Internet-Draft
Intended status: Standards Track
Expires: January 7, 2016

E. Osterweil
G. Wiley
T. Okubo
R. Lavu
A. Mohaisen
VeriSign, Inc.
July 6, 2015

Opportunistic Encryption with DANE Semantics and IPsec: IPSECA
draft-osterweil-dane-ipsec-03

Abstract

This document defines a new Domain Name System (DNS) resource record type called the IPSECA RR that is used to associate an X.509 certificate or a public key to an Internet Protocol Security (IPsec) gateway in a similar manner TLSA RR is used in the DNS-based Authentication of Named Entities (DANE) protocol does that for Transport Layer Security (TLS) in order to make the credential discovery easier through DNS and to allow credential discovery to be performed in a secure manner leveraging DNS Security Extensions (DNSSEC). Among the issues addressed in this draft is the danger of IP address spoofing that can be a liability to IPsec endpoints. It is important to note that the "right destination" in this document is strictly defined by the response of the DNS and does not attest to the identity of the organization or the ownership of the IP address space. The identity of the organization shall be attested in an X.509 certificate issued by a certification authority if desired and the ownership of the IP address space shall be attested by other mechanisms such as Towards A Secure Routing System (TASRS) architecture or Resource Public Key Infrastructure (RPKI).

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

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."

This Internet-Draft will expire on January 7, 2016.

Copyright Notice

Table of Contents

1. Introduction

This document defines a new Domain Name System (DNS) [RFC1035] resource record type called the IPSECA RR that is used to associate an X.509 certificate or a public key to an Internet Protocol Security (IPsec) gateway in a similar manner TLSA RR is used in the DNS-based Authentication of Named Entities (DANE) protocol [RFC6698] does that for Transport Layer Security (TLS) [RFC5248]

The benefit of associating an X.509 certificate or a public key to an IPsec gateway is twofold. One is to make the credential discovery easier through DNS: a protocol that is widely adopted throughout the Internet and mechanism that is publicly available. The other is to allow credential discovery to be performed in a secure manner leveraging DNS Security Extensions (DNSSEC) [RFC4033], [RFC4034], [RFC4035]. DNSSEC protects the authenticity and integrity of the signed DNS response, which plays an instrumental role in assuring that the gateway is connecting to the right destination and is using the the appropriate Internet Key Exchange Protocol Version 2 (IKEv2) [RFC5996] credentials to establish the tunnel.

It is important to note that the "right destination" in this document is strictly defined by the response of the DNS and does not attest to the identity of the organization or the ownership of the IP address space. The identity of the organization shall be attested in a X.509 certificate issued by a certification authority if desired and the ownership of the IP address space shall be attested by other mechanisms such as Towards A Secure Routing System (TASRS) [TASRS] architecture or Resource Public Key Infrastructure (RPKI) [RFC6810].

In addition to the fact that the combination of DNS and DNSSEC will provide a secure and robust foundation for IPsec to perform opportunistic encryption, it also provides an alternative for those who wish to deploy opportunistic encryption for IPsec but have difficulty getting the sub-delegation for the reverse DNS. By removing the obstacle, this mechanism will allow more entities to effectively and efficiently enable opportunistic encryption for their IPsec facilities. In other words, IPSECA RR will maximize the "Fax Effect" for IPsec opportunistic encryption.

This document details the motivation for, the synergy from, and a protocol to advertise and verify security credentials that can be used to verify Opportunistic Encryption (OE) IPsec [RFC4301], [RFC6071] tunnels for DNS transactions. Securing DNS transactions in this way is both necessary and sufficient for providing confidentiality of many types of DNS-transaction meta data, which can betray user privacy. This document details a new DANE-like [RFC6698] DNS Resource Record (RR) type called IPSECA, and explains how to use

it to bootstrap entries in IPsec Security Policy Databases (SPDs) and to subsequently verify Security Associations (SAs) for OE IPsec tunnels.

1.1. What IPSECA Adds to DNSSEC Transactions

DNSSEC's focus on object level security leaves the types of protections offered by IPsec unaddressed. Specifically, the way (or ways) to associate certificate(s) used by IPsec with a DNSSEC-aware name server need to be codified. This can be especially complicated if different IPsec certificates need to be discovered for different services that are running on the same IP address. This can become complicated if certificates are learned solely by the IP addresses of networked-services. This gap is inherently overcome during certificate discovery in DANE protocols by the concept of "Service Address Records," [I-D.draft-ogud-dane-vocabulary]. These Security Associations are defined by, and discovered by, domain names rather than just IP addresses. [RFC6698] standardizes a way for security associations of certificates to be made with service domains for TLS, rather than just IP addresses. As one of the underlying facilities of DANE's approach to certificate verification, this adds a necessary enhancement to certificate learning in IPsec, over approaches that

are based solely on IP addresses in DNS (such as described in [RFC4025] and [RFC4322]).

The advantages of using DANE for IPsec OE also include other simplifications that the DANE protocol inherently offers all of its protocols. Such as, the automatic de-authorization of certificates that happens when they are removed from a DNS zone, which may (under many circumstances) obviate the need for extensive use of revocation mechanisms (OCSP [RFC6960] or CRL [RFC5280]). Details of these relative trade offs is described in more detail in [DANE_SATIN12]. Once a certificate is learned from DANE, it should be periodically rechecked, but without out-of-band maintenance, the association will remain valid until its X.509 signature (if certain Usage Types that include PKIX validation are used) expires.

It is also noteworthy that DANE offers flexibility that is not available in IP-centric certificate discovery and IP-centric OE [RFC4322], while still being backwards compatible with them. That is, while users can use IPSECA records to map OE IPsec tunnels to service names, they can also use IPSECA records in their reverse DNS zone in a similar fashion to the IPSECKEY [RFC4025] record used in [RFC4322]. However, while this document illustrates an example usage of DANE with IPsec OE, any specification for how the IPSECA resource record MUST get used with OE is beyond the scope of this document.

1.2. IP-Centric IPsec Tunnel Discovery Using IPSECKEY

In contrast to a DANE-centric discovery, [RFC4025] specifies a DNS resource record called IPSECKEY. The IPsec certificate learning described therein prescribes that relying parties learn the intended usage of IPsec certificates after they locate them in DNS and retrieve them. The types of information that relying parties learn from IPSECKEY responses include: precedence, gateway type, algorithm, gateway, and possibly the public key. After learning the key and creating the Security Association, the relying party can use techniques like [RFC4322] to initialize an OE IPsec tunnel.

The inherent key learning and verification technique in [RFC4322] is based on learning tunnels from IP addresses only (IP-centric). Because of this technique's focus on IP-centric learning, operational

entities running services on a specific IP address may not have access to annotate the reverse DNS zone for their services (especially if they are shared environments). So, this type of OE may often be a non-starter. One example would be when zones are hosted and/or served by cloud service providers. In this case, customers are almost certainly not allowed to annotate the reverse DNS zone for their providers.

1.3. Service-Centric IPsec Tunnel Discovery Using IPSECA and DANE

The suggested usage of this document is to aid in discovering where OE IPsec tunnels exist, and to act as an out of band verification substrate that can validate the certificates received during IPsec key exchange. For example, if a DNS caching recursive resolver is configured to attempt OE IPsec tunnels to DNS name servers (using a specific key exchange protocol, like [RFC5996], etc.), then when it receives a referral it SHOULD query name servers for corresponding IPSECA resource records. (we discuss the format of the resource record and domain names below in Section 2). When an IPSECA record is discovered by a resolver, that resolver SHOULD follow its configurations and setup an SPD entry, in order to signal its IPsec layer to attempt to attempt to establish an SA. Note, this document does not specify a new, or any modifications to any existing, IPsec key exchange protocols. Rather, after adding an SPD and a successful tunnel establishment, the credentials used for the Security Association with the name server SHOULD be cross-checked with the IPSECA resource record(s).

We note that simply adding PAD entries with the IPSECA keys and identifying them with IP addresses so that the traditional IPSEC implementations work would result in several security issues. In particular, each zone answering a forward A and IPSEC lookups could give their keys for an arbitrary IP address that they are bound to,

allowing to intercept some else's tunnel. To address this issue, we require that a resource certification mechanisms (such as Towards A Secure Routing System (TASRS) [TASRS] architecture or Resource Public Key Infrastructure (RPKI) [RFC6810]) be used. In particular, a verifiable certification of the association of a resource with an A record would limit the ability of an adversary from publishing such answers to an IPSEC lookup. We note that this does not only address this security issue, but also marginalizes other issues associated

with the many-to-one mapping from DNS domain names to IP addresses.

When using IPSECA resource records to verify OE tunnels, clients MUST perform full DNSSEC validation of the DNSSEC chain of trust that leads to IPSECA RRs. As specified in [RFC6698]:

> "A [IPSECA] RRSet whose DNSSEC validation state is secure MUST be used as a certificate association for [IPsec] unless a local policy would prohibit the use of the specific certificate association in the secure TLSA RRSet.
>
> If the DNSSEC validation state on the response to the request for the [IPSECA] RRSet is bogus, this MUST cause IPsec not to be started or, if the IPsec negotiation is already in progress, MUST cause the connection to be aborted.
>
> A [IPSECA] RRSet whose DNSSEC validation state is indeterminate or insecure cannot be used for [IPsec] and MUST be considered unusable."

This is to ensure that the SPD entries and SA(s) used for tunnels are fully verified. This verification MAY include local trust anchor processing, such that local DNSKEY resource records can be used to verify corresponding RRSIGs. Trust anchors (which may be distributed during dynamic host configuration) may be useful for bootstrapping. For example, consider the case where private address space [RFC1918] is used for internal recursive resolvers. Here, the locally provisioned DNS names for the private address space (in the reverse tree) that are secured using DNSSEC MAY use local trust anchors. That is, if an [RFC1918] address is used internally, the corresponding domain name MUST also resolve and be verifiable through DNS and DNSSEC, but a local trust anchor MAY be used to verify covered RRSIGs. This shifts the onus of securing DNS transactions to the initial configuration step. The intuition behind this reasons that if the first (configuration) step was already where the local resolver was configured, then the security of the DNS transactions already hinged on learning the valid resolver this way. So, this step is already used to convey trusted configurations (bootstrapping). Adversaries attempting to subvert an end host have only the narrow attack window that is associated with learning

configurations. In contrast, an insecure DNS resolver offers an

attack window every time it issues or responds to a query. We discuss this further in Section 5.2.

2. The IPSECA Resource Record

The IPSECA resource record is modeled heavily off of the IPSECKEY RR [RFC4025], but it differs in significant ways. The format of IPSECA is harmonized with the architectural direction set by other DANE work [RFC6698], [I-D.draft-ogud-dane-vocabulary].

2.1. IPSECA RDATA Wire Format

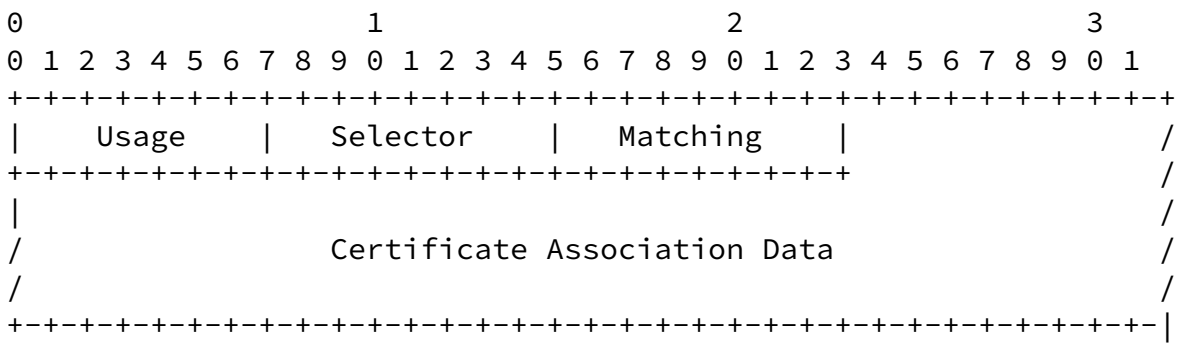

Figure 1

2.1.1. The Usage Field

The meaning, semantics, and interpretation of the Usage field of the IPSECA resource record follow the specification described in Section 2.1 of [RFC7218]:

Value	Acronym	Short Description	Reference
0	PKIX-TA	CA constraint	[RFC6698]
1	PKIX-EE	Service certificate constraint	[RFC6698]
2	DANE-TA	Trust anchor assertion	[RFC6698]
3	DANE-EE	Domain-issued certificate	[RFC6698]
4-254		Unassigned	
255	PrivCert	Reserved for Private Use	[RFC6698]

Table 1: TLSA Certificate Usages

2.1.2. The Selector Field

The meaning, semantics, and interpretation of the Selector field of the IPSECA resource record follow the specification described in Section 2.2 of [RFC7218]:

Value	Acronym	Short Description	Reference
0	Cert	Full certificate	[RFC6698]
1	SPKI	SubjectPublicKeyInfo	[RFC6698]
2-254		Unassigned	
255	PrivSel	Reserved for Private Use	[RFC6698]

Table 2: TLSA Selectors

2.1.3. The Matching Field

The meaning, semantics, and interpretation of the Matching field of the IPSECA resource record follow the specification described in Section 2.3 of [RFC7218]:

Value	Acronym	Short Description	Reference
0	Full	No hash used	[RFC6698]
1	SHA2-256	256 bit hash by SHA2	[RFC6698]
2	SHA2-512	512 bit hash by SHA2	[RFC6698]
3-254		Unassigned	
255	PrivMatch	Reserved for Private Use	[RFC6698]

Table 3: TLSA Matching Types

2.1.4. The Certificate Association Data Field

The meaning, semantics, and interpretation of the Certificate Association Data field of the IPSECA resource record follow the specification of the same field in the TLSA resource record, described in Section 2.1.4 of [RFC6698]:

"This field specifies the 'certificate association data' to be matched. These bytes are either raw data (that is, the full

certificate or its SubjectPublicKeyInfo, depending on the selector) for matching type 0, or the hash of the raw data for matching types 1 and 2. The data refers to the certificate in the association, not to the TLS ASN.1 Certificate object."

2.2. IPSECA RR Presentation Format

</STUBBED OUT SECTION>

2.3. Domain Names used for IPSEC Records

The IPSECA resource record SHOULD be mapped to a domain name that is intuitive when discovering OE IPsec tunnels for specific services. The expected procedure for constructing the domain names for IPSECA records that enable OE for DNS (port 53) are:

1. The left-most label begins with an underscore character (_), followed by the decimal representation of the port number that corresponds to the service that should be conducted over IPsec. For example, the DNS transactions discussed in this document would result in "_53".

2. Next, the fully qualified domain name [RFC1035] of the service is appended to the right side. In the case of a DNS name server, that is its domain name. In the case of a service that is locate using an IP address, the service address records MUST be its full reverse octet name (including the appropriate suffix, such as .in-addr.arpa. for IPv4 addresses and .ip6.arpa for IPv6 addresses).

Any custom configured tunnels and port mappings may result local policies that use their own domain name format. Such custom OE tunnels are non-standard, and may not be discoverable by other relying parties.

2.4. IPSECA RR Examples

Because the IPSECA record is intended to be associated with a Service Address Records, it can (implicitly) also be associated with an IP

address through the reverse DNS. A few illustrative mappings are presented here as examples. Note that these domain name / resource record mappings are not necessarily intended to update the processing of protocols like IKEv1 [RFC2409], IKEv2 [RFC5996], etc. or other OE protocols [RFC4322]. Rather, these mappings are intended to serve as examples of IPsec tunnels, and their proper configuration. Those mappings MAY be used in verifying Security Associations. However, we note that a specific protocol to do the verification is beyond the scope of this document.

We note that there are several issues associated with using forward DNS in the following examples. In particular, a malicious actor may intercept a tunnel by showing a key for an association with an A record to an arbitrary initiator. We note that this is more of a foundational problem addressed by Internet Number Resource Certification. Systems proposed to address this include the Resource Public Key Infrastructure (RPKI), and others.

2.4.1. OE to a DNS Name Server Example

Suppose a DNS zone example.com is served by the name servers ns1.example.com and ns2.example.com. If the zone operators want to advertise their willingness to offer OE to their name servers using IKEv2 [RFC5996], then the following domain names MUST be placed under the example.com zone (the contents of the resource records, below, are exemplary only and MAY have whatever values a zone operator chooses):

```
_53.ns1.example.com. IN IPSECA (
    0 1 1 edeff39034cd2ee83446633a9fba
          d815a579134ecd7636e51af92ec7
          207fd490 ) ; Verify IPsec for DNS txns

_53.ns2.example.com. IN IPSECA (
    0 1 1 edeff39034cd2ee83446633a9fba
          d815a579134ecd7636e51af92ec7
          207fd490 ) ; Verify IPsec for DNS txns
```

This example illustrates how a zone MAY indicate where an SPD entry and SA establishment endpoints exist for its name servers (note, they are not required to be the name servers themselves). Here, each name

server is a tunnel end point, and these two name servers are mapped to service ports for DNS (port 53). The IPSECA records above indicate that they verify the CA who must have issued the IPsec certificate used and they represent a SHA256 hash of that certificate's SPKI.

Alternately, suppose an enterprise wants to configure OE for DNS transactions between its desktop clients and its recursive resolver. In this case, if the enterprise has configured their desktop clients (perhaps through DHCP) to forward their DNS queries to a caching recursive resolver at the IP address 192.168.1.2, then the following IPSECA mapping should be placed in an internally managed DNS reverse zone:


```
_53.2.1.168.192.in-addr.arpa. IN IPSECA (
    3 0 2 8f6ea3c50b5c488bef74c7c4a17a
          24e8b0f4777d13c211a29223b69a
          ea7a89184ac4d272a2e3d9760966
          fb3f220b39f7fdfb325998289e50
          311ce0748f13c1ed ) ; Verify data in IKEv2 SA
```

This example illustrates how a caching recursive resolver MAY indicate where it will accept IPsec tunnel establishment and what the certificate used for a SA should be. Here the DNS service port and the IPSECA records describe the nature of the authentic certificate that SHOULD be used in an SA with this endpoint. In this example, the IPSECA records both specify that a DANE-EE cert should be expected in an SA with this resolver, and the SHA-512 hash of that full certificate should match the encoded value in the IPSECA resource record.

Of note here is that since SAs MAY be identified by domain names (which map to IP addresses), some IP addresses may host services that offer IPsec, and some that do not. The IPSECA record allows hosts to advertise these nuanced configurations in the same way that these services are discovered (through the DNS itself).

3. Operational Considerations

Scaling IPsec connections to the full capacity that large recursive resolvers or large authoritative name servers operate at could be cause for concern. The additional overhead required to establish and maintain SAs could exceed the provisioning capacity of deployed systems. However, there are several relevant observations:

1. If a resolver enables OE, but no (or relatively few) name servers provision IPSECA records, then no IPsec tunnels will be established, and the load will remain static (or marginally increase).

2. If an authoritative name server provisions IPSECA record, it will only result in additional load if querying resolvers are configured to attempt OE.

3. Using white-listing techniques (such as those used during pilot deployments of AAAA records) would allow authoritative name servers to only return IPSECA responses to clients that have been white-listed. This would allow name servers to control the amount of IPsec overhead they incur. For the same reason, resolvers can be configured to only query for IPSECA records from white-listed name servers.

4. IANA Considerations

This document uses a new DNS resource record type, called IPSECA. This resource record will need to have a new value assigned to it. Current implementations are advised to use a type number TYPE65347.

This document uses the same semantics and values as the TLSA resource record [RFC6698] for its Usage, Selector, and Matching fields. Any future use or modification of an IANA registry for that resource record will have similar effects on this resource record.

5. Security Considerations

This document details some of the benefits of using IPsec OE for DNS transactions. Such a utility does not reduce the benefits of other security protections. For example, the object-level security assurances that are offered by DNSSEC are cooperative with the

session-level security of IPsec. Additional discussions are available in [IPSEC_APPEAL]. Moreover, the protections described herein also offer cooperative benefits with higher layer protocol protections, like TLS [RFC5246]. Any combination of these types of protections offer both defense-in-depth (securing transactions at multiple levels) and offer security practitioners a larger mosaic of security tools from which to construct and maintain their security postures.

5.1. Interactions

This document requires that all fully qualified domain names [RFC1035] must be secured by DNSSEC. This includes domains in the reverse tree of DNS (which represent IP addresses). An important question in this context is whether an unvalidated IPSECA record would be better than nothing. In other words, would it be better to tolerate failed validation or even unsigned (non-DNSSEC) IPSECA records than to refuse to allow a connection? Permitting the use of unsigned records introduces a vector for downgrade attacks.

The use of IPSECA resource records does not constitute a source of information leakage. Rather, it provides a mechanism to help bolster confidentiality, by obfuscating DNS transactions.

Expressing tunnel endpoints through DNS may allow adversaries a vehicle to learn where OE is being offered by name servers. However, OE tunnels to these name servers will only be attempted if querying resolvers are configured to attempt IPsec. As a result, adversaries may be able to learn of potential tunnel endpoints, but if they aim to disrupt active IPsec traffic, they must still observe which

resolvers are trying to initiate IPsec communications. Therefore, adversaries would have no greater opportunity to disrupt IPsec traffic than they already do. They would still begin by (for example) observing VPN tunnel setup on wireless LANs (such as at public WiFi hot-spots).

5.2. Last Mile Security Analysis

For the last mile, we define one type of attack as the case where an adversary intercepts messages that can be undetectably spoofed. For example, if a zone (like example.com) has deployed DNSSEC, then if an

adversary responds to a DNS query for www.exmaple.com, a validating DNS resolver should be able to detect the forgery. However, if an adversary responds to a query that is sent for a non-DNSSEC zone, a resolver cannot distinguish the spoofed response from an authentic response. In addition to this, many bootstrapping protocols (such as DHCP [RFC2131]) represent the first opportunity for an adversary to disrupt DNS transactions (by subverting the bootstrapping of the resolver itself on stub-resolvers). Under this model, a DNS stub-resolver's security posture is enhanced by keeping an adversary's attack window to the smallest value possible.

Therefore, the attack window offered by DNS clients in a given time span T is comprised of the set of transactions that bootstrap configurations W_cfg(T), plus any DNS transactions that are not verifiable. Of note, however, is that the DNSSEC transactions between stub-resolvers and recursive resolvers are not protected by DNSSEC's cryptography. The only indication of protections is a header bit (the AD bit), which is spoofable. As a result, the attack window includes all DNS transactions W_rDNS(T).

From this, the attack window can be expressible as:

W(T) = W_cfg(T) + W_rDNS(T)

Of note is that under most circumstances, resolvers issue many more queries than configuration requests. So,

W_cfg(T) = 1, and W_rDNS(T) >> W_cfg(T).

However, consider the attack window when using OE: {W(T)}. If the initial configuration includes a DNSKEY trust anchor that can be used to verify DNSSEC data that corresponds to a resolver's corresponding reverse zone (i.e., the IPSECA RR under in-addr.arpa or ip6.arpa), then {W_cfg(T)} = 1 and {W_rDNS(T)} = 0. Therefore, since W_rDNS(T) >> W_cfg(T) and {W_rDNS(T)} = 0, then by the transitive property,

W(T) >> {W(T)}.

While this protocol is designed to enable best effort encryption for IPsec without any prearrangement between entities, this mechanism

does not attempt to provide authentication. Entities that are security conscious may choose to undergo an authentication and verification process at a certification authority to obtain a certificate that attests to the organization's identity. Entities that are concerned about the IP resource ownership or route origin may consider adopting an additional mechanism that is designed for that purpose.

6. Acknowledgements

The editors would like to express their thanks for the early support and insights given by Danny McPherson.

7. References

7.1. Normative References

[RFC1035] Mockapetris, P., "Domain names - implementation and specification", STD 13, RFC 1035, November 1987.

[RFC1918] Rekhter, Y., Moskowitz, R., Karrenberg, D., Groot, G., and E. Lear, "Address Allocation for Private Internets", BCP 5, RFC 1918, February 1996.

[RFC4033] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "DNS Security Introduction and Requirements", RFC 4033, March 2005.

[RFC4034] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Resource Records for the DNS Security Extensions", RFC 4034, March 2005.

[RFC4035] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Protocol Modifications for the DNS Security Extensions", RFC 4035, March 2005.

[RFC4301] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, December 2005.

[RFC5248] Hansen, T. and J. Klensin, "A Registry for SMTP Enhanced Mail System Status Codes", BCP 138, RFC 5248, June 2008.

[RFC6698] Hoffman, P. and J. Schlyter, "The DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS) Protocol: TLSA", RFC 6698, August 2012.

[RFC6810] Bush, R. and R. Austein, "The Resource Public Key Infrastructure (RPKI) to Router Protocol", RFC 6810, January 2013.

[RFC7218] Gudmundsson, O., "Adding Acronyms to Simplify Conversations about DNS-Based Authentication of Named Entities (DANE)", RFC 7218, April 2014.

7.2. Informative References

[DANE_SATIN12]
Osterweil, E., Kaliski, B., Larson, M., and D. McPherson, "Reducing the X.509 Attack Surface with DNSSEC's DANE", Proceedings of Securing and Trusting Internet Names, SATIN '12, March 2012.

[I-D.draft-ogud-dane-vocabulary]
Gudmundsson, O., "Harmonizing how applications specify DANE-like usage", October 2013.

[IPSEC_APPEAL]
Osterweil, E. and D. McPherson, "IPsec's Appeal: Protecting DNS Under the Covers", Verisign Labs Technical Report #1130006 Revision 1, January 2013.

[RFC2131] Droms, R., "Dynamic Host Configuration Protocol", RFC 2131, March 1997.

[RFC2409] Harkins, D. and D. Carrel, "The Internet Key Exchange (IKE)", RFC 2409, November 1998.

[RFC3596] Thomson, S., Huitema, C., Ksinant, V., and M. Souissi, "DNS Extensions to Support IP Version 6", RFC 3596, October 2003.

[RFC4025] Richardson, M., "A Method for Storing IPsec Keying Material in DNS", RFC 4025, March 2005.

[RFC4322] Richardson, M. and D. Redelmeier, "Opportunistic Encryption using the Internet Key Exchange (IKE)", RFC 4322, December 2005.

[RFC5246] Dierks, T. and E. Rescorla, "The Transport Layer Security

[RFC5280] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, May 2008.

[RFC5996] Kaufman, C., Hoffman, P., Nir, Y., and P. Eronen, "Internet Key Exchange Protocol Version 2 (IKEv2)", RFC 5996, September 2010.

[RFC6071] Frankel, S. and S. Krishnan, "IP Security (IPsec) and Internet Key Exchange (IKE) Document Roadmap", RFC 6071, February 2011.

[RFC6960] Santesson, S., Myers, M., Ankney, R., Malpani, A., Galperin, S., and C. Adams, "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP", RFC 6960, June 2013.

[TASRS] Osterweil, E. and D. McPherson, "TASRS: Towards a Secure Routing System Through Internet Number Resource Certification", Verisign Labs Technical Report #1130009 Revision 1, February 2013.

Appendix A. Name Server OE Configuration Example

<STUBBED OUT SECTION>

NAME SERVER SIDE

- Config SPD to accept connections from any on port 53 only
- Zones add IPSECA RRs for each NS domain name and configure DNSSEC: <examples>

RESOLVER SIDE

- resolver processing logic to intercept referrals and look for IPSECA RR(s).

- When an IPSECA RR is found, create SPD for that IP and port 53.

</STUBBED OUT SECTION>

Appendix B. Recursive Resolver OE Configuration Example

<STUBBED OUT SECTION>

RESOLVER SIDE

- If public resolver, create SPD entry that only allows IPsec from port 53. If internal resolver, limit to addresses serviced.

REVERSE DNS ZONE

- Add IPSECA RR(s) and configure DNSSEC

STUB SIDE

- Configure reverse zone DNSKEY (if 1918) as a local TA (such as over DHCP). Then do onetime DNSSEC validation for fetching IPSECA RR.

- Tools include dnskey-grab and/or NLnet Labs' xxxxx.

</STUBBED OUT SECTION>

Authors' Addresses

Eric Osterweil
VeriSign, Inc.
Reston, VA
USA

Email: eosterweil@verisign.com

Glen Wiley
VeriSign, Inc.
Reston, VA

USA

Email: gwiley@verisign.com

Tomofumi Okubo
VeriSign, Inc.
Reston, VA
USA

Email: tomokubo@Verisign.com

Ramana Lavu
VeriSign, Inc.
Reston, VA
USA

Email: RLavu@verisign.com

Aziz Mohaisen
VeriSign, Inc.
Reston, VA
USA

Email: amohaisen@verisign.com