Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: October 12, 2014

P. Wouters
Red Hat

April 10, 2014

Best Common Practise for using OPENPGPKEY records
draft-ietf-dane-openpgpkey-usage-00

Abstract

The OPENPGPKEY DNS Resource Record can be used to match an email address to an OpenPGP key. This document specifies a Best Common Practise ("BCP") for email clients, MUA's and MTA's for using the OPENPGPKEY DNS Resource Record.

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 October 12, 2014.

Copyright Notice

Table of Contents

1. Introduction

This document describes a Best Current Practise ("BCP") for using OPENPGPKEY DNS Resource Records xref target="OPENPGPKEY"/ in email clients, MUA’s and MTA.

1.1. Terminology

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 RFC 2119 [RFC2119].

This document also makes use of standard DNSSEC and DANE terminology. See DNSSEC [RFC4033], [RFC4034], [RFC4035], and DANE [RFC6698] for these terms.

2. The OPENPGPKEY record presence

A user who publishes an OPENPGPKEY record in DNS explicitly prefers receiving encrypted email over receiving unencrypted email.

A user who publishes an OPENPGPKEY record in DNS still expects senders to perform their due diligence by additional verification of their public key via other out-of-band methods before sending any confidential or sensitive information

In other words, the OPENPGPKEY record in DNS, without any additional verification, should be used only as an alternative to sending plaintext email. It SHOULD NOT be used to change one's opinion on whether it is safe or appropriate to sent the content via email in the first place.

3. OpenPGP public key considerations

Once an OPENPGPKEY resource record has been found and the OpenPGP public keyring has been decoded, the right public key must be located inside the keyring. For a public key in the keyring to be usable, the public key has to have a key uid as specified in [RFC4648] that matches the email address for which the OPENPGPKEY RR lookup was performed.

3.1. Public Key UIDs and email addresses

An OpenPGP public key can be associated with multiple email addresses by specifying multiple key uids. The OpenPGP public key obtained from a OPENPGPKEY RR can be used as long as the target recipient's email address appears as one of the OpenPGP public key uids. The name part (left of the @) should appear in the native format, not its SHA2-224 hash that was used to lookup the OPENPGPKEY RR.

3.2. Public Key UIDs and IDNA

Internationalized domains that use non-ascii characters (U-label) are encoded in DNS using IDNA [RFC5891] - also referred to as punycode or A-label. When matching OpenPGP public key uids, both the email address specified using U-label and A-label should be considered as valid public key uids.

3.3. Public Key UIDs and synthesized DNS records

CNAME's (see [RFC2181]) and DNAME's (see [RFC6672]) can be followed to obtain an OPENPGPKEY RR, as long as the original recipient's email address appears as one of the OpenPGP public key uids. For example, if the OPENPGPKEY RR query for hugh@example.com (8d57[...]b7._openpgpkey.example.com) yields a CNAME to 8d57[...]b7._openpgpkey.example.net, and an OPENPGPKEY RR for 8d57[...]b7._openpgpkey.example.net exists, then this OpenPGP public key can be used, provided one of the key uids contains "hugh@example.com". This public key cannot be used if it would only contain the key uid "hugh@example.net".

If one of the OpenPGP key uids contains only a single wildcard as the LHS of the email address, such as "*@example.com", the OpenPGP public key may be used for any email address within that domain. Wildcards

at other locations (eg hugh@*.com) or regular expressions in key uids are not allowed, and any OPENPGPKEY RR containing these should be ignored.

3.4. OpenPGP Key size and DNS

Although the reliability of the transport of large DNS Resoruce Records has improved in the last years, it is still recommended to keep the DNS records as small as possible without sacrificing the security properties of the public key. The algorithm type and key size of OpenPGP keys should not be modified to accomodate this section.

OpenPGP supports various attributes that do not contribute to the security of a key, such as an embedded image file. It is recommended that these properties are not exported to OpenPGP public keyrings that are used to create OPENPGPKEY Resource Records. Some OpenPGP software, for example GnuPG, have support for a "minimal key export" that is well suited to use as OPENPGPKEY RDATA.

4. Security Considerations

The main goal of the OPENPGPKEY resource record is to stop passive attacks against plaintext emails. While it can also twart some active attacks (such as people uploading rogue keys to keyservers in the hopes that others will encrypt to these rogue keys), this resource record is not a replacement for verifying OpenPGP public keys via the web of trust signatures, or manually via a fingerprint verification.

Various components could be responsible for encrypting an email message to a target recipient. It could be done by the sender’s email client or software plugin, the sender’s Mail User Agent (MUA) or the sender’s Mail Transfer Agent (MTA). Each of these have their own characteristics. An email client can direct the human to make a decision before continuing. The MUA can either accept or refuse a message. The MTA must deliver the message as-is, or encrypt the message before delivering. Each of these programs should ensure that the security of an email message is never downgraded, and that an unencrypted received message will be encrypted whenever possible.

Organisations that require to be able to read everyone’s encrypted email should publish the escrow key as the OPENPGPKEY record. Upon receipt, such mail servers can optionally re-encrypt the message to the individual’s OpenPGP key.

4.1. Email address information leak

DNS zones that are signed with DNSSEC using NSEC for denial of existence are susceptible to zone-walking, a mechanism that allow someone to enumerate all the names in the zone. Someone who wanted to collect email addresses from a zone that uses OPENPGPKEY might use such a mechanism. DNSSEC-signed zones using NSEC3 for denial of existence are significantly less susceptible to zone-walking. Someone could still attempt a dictionary attack on the zone to find OPENPGPKEY records, just as they can use dictionary attacks on an SMTP server or grab the entire contents of existing PGP key servers to see which addresses are valid.

4.2. OpenPGP security and DNSSEC

DNSSEC key sizes are chosen based on the fact that these keys can be rolled with next to no requirement for security in the future. If one doubts the strength or security of the DNSSEC key for whatever reason, one simply rolls to a new DNSSEC key with a stronger algorithm or larger key size.

This effectively means that anyone who can obtain a DNSSEC private key of a domain name via coercion, theft or brute force calculations, can replace any OPENPGPKEY record in that zone and all of the delegated child zones, irrespective of the key length strength of the OpenPGP keypair.

Therefor, DNSSEC is not an alternative for the "web of trust" or for manual fingerprint verification by humans. It is a solution aimed to ease obtaining someone’s public key, and without manual verification should be treated as "better then plaintext" only. While this twarts all passive attacks that simply capture and log all plaintext email content, it is not a security measure against active attacks.

4.3. MTA behaviour

An MTA could be operating in a stand-alone mode, without access to the sender’s OpenPGP public keyring, or in a way where it can access the user’s OpenPGP public keyring. Regardless, the MTA MUST NOT modify the user’s OpenPGP keyring.

An MTA sending an email MUST NOT add the public key obtained from an OPENPGPKEY resource record to a permanent public keyring for future use beyond the TTL.

If the obtained public key is revoked, the MTA MUST NOT use the key for encryption, even if that would result in sending the message in plaintext.

If a message is already encrypted, the MTA SHOULD NOT re-encrypt the message, even if different encryption schemes or different encryption keys were used.

If an OPENPGPKEY resource record is received without DNSSEC protection, it MAY still be used for encryption.

If the DNS request for an OPENPGPKEY record returned an "indeterminate" or "bogus" answer, the MTA MUST NOT sent the message and queue the plaintext message for delivery at a later time. If the problem persists, the email should be returned via the regular bounce methods.

If multiple non-revoked OPENPGPKEY resource records are found, the MTA SHOULD pick the most secure RR based on its local policy. [or should it encrypt to both?]

4.4. MUA behaviour

If the public key for a recipient obtained from the locally stored sender’s public keyring differs from the recipient’s OPENPGPKEY RR, the MUA MUST NOT accept the message for delivery.

If the public key for a recipient obtained from the locally stored sender’s public keyring contains contradicting properties for the same key obtained from an OPENPGPKEY RR, the MUA SHOULD NOT accept the message for delivery.

If multiple non-revoked OPENPGPKEY resource records are found, the MUA SHOULD pick the most secure OpenPGP public key based on its local policy.

4.5. Email client behaviour

Email clients should adhere to the above listed MUA behaviour. Additionally, an email client MAY interact with the user to resolve any conflicts between locally stored keyrings and OPENPGPKEY RRdata.

An email client that is encrypting a message SHOULD clearly indicate to the user the difference between encrypting to a locally stored and humanly verified public key and encrypting to an unverified (by the human sender) public key obtained via an OPENPGPKEY resource record.

5. References

5.1. Normative References

[OPENPGPKEY] Wouters, P., "DANE for OpenPGP public keys", draft-ietf-wouters-dane-openpgp (work in progress), April 2014.

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

[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.

[RFC4648] Josefsson, S., "The Base16, Base32, and Base64 Data Encodings", RFC 4648, October 2006.

[RFC4880] Callas, J., Donnerhacke, L., Finney, H., Shaw, D., and R. Thayer, "OpenPGP Message Format", RFC 4880, November 2007.

[RFC5891] Klensin, J., "Internationalized Domain Names in Applications (IDNA): Protocol", RFC 5891, August 2010.

5.2. Informative References

[RFC2181] Elz, R. and R. Bush, "Clarifications to the DNS Specification", RFC 2181, July 1997.

[RFC2822] Resnick, P., "Internet Message Format", RFC 2822, April 2001.

[RFC4255] Schlyter, J. and W. Griffin, "Using DNS to Securely Publish Secure Shell (SSH) Key Fingerprints", RFC 4255, January 2006.

[RFC6530] Klensin, J. and Y. Ko, "Overview and Framework for Internationalized Email", RFC 6530, February 2012.

[RFC6672] Rose, S. and W. Wijngaards, "DNAME Redirection in the DNS", RFC 6672, June 2012.

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

Author's Address

Paul Wouters
Red Hat

Email: pwouters@redhat.com