Network Working Group
Internet-Draft
Intended status: Informational
Expires: December 1, 2014

Xiaodong. Lee, Ed.
Haikuo. Zhang, Ed.
Nan. Wang, Ed.
Peng. Zuo, Ed.
Xiali. Yan, Ed.
Ce. Luo, Ed.
Hongtao. Li, Ed.
cnnic

May 30, 2014

Weak Trust Anchor Introduction
draft-zhang-dnsop-weak-trust-anchor-00

Abstract

DNS Security Extensions (DNSSEC) is an effective method to provide security protection for resolvers and end users in the DNS protocols. But the DNSSEC is too aggressive for the DNS service in the poor network infrastructure, because the domain name will be invisible when large DNSSEC messages were dropped by some other network equipments, like the routers which have MTU problem or the old firewalls which do not support ENDS0. This document defines a new concept weak trust anchor which can be used on a security-aware resolver to get rid of the above problem.

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 December 1, 2014.

Table of Contents

1. Introduction

DNSSEC is described in a set of RFC documents, they are [RFC4033][RFC4034] [RFC4035] [RFC4641] [RFC5011] [RFC5155] and so on. DNSKEY has been introduced into signed zone file to help resolvers build a chain of trust. The chain of trust is comprised of some Delegation of Signing (DS) RRs, Key signing Key (KSK) RRs, Zone signing key (ZSK) RRs, traditional RRs(like AAAA RRs), related resource record signatures (RRsig),and so on [RFC4641].NSEC and NSEC3 RR can be used to prove non-existence of domain names in the zone [RFC5155].

The security-aware resolver will verify DNS packets in the recursive query process. If DNS packets are tampered by the man-in-the-middle attack, the resolver will return Servfail to end users. Trust anchor is used as starting point in the chain of trust at the security-aware resolver side.

The size of a DNSSEC packet may be larger than 1500 bytes, and EDNS0 protocol has extended the size limitation of the regular DNS packet. But this kind of DNSSEC packets could be lost or dropped in the global network environment, because some routers in the transmission may have MTU problem or some old firewalls could not support ENDS0. Then some domains could be invisible for the end users who are using this security-aware resolver, and this case is out of control for

ISPs, so this situation may block the DNSSEC deployment at resolver side.

Weak trust anchor is introduced to handle this problem.

2. Terms

MTU: Maximum Transmission Unit. It is the size of the largest data unit that the layer can pass onwards.

Trust Anchor: DNSKEY RR or DS RR hash of a DNSKEY RR, and it is the starting point of the authentication chain in the DNSSEC verification. Described in [RFC4034].

Weak Trust Anchor: Almost same as Trust Anchor, except that Weak Trust Anchor is relatively moderate. The resolver which was configured with Trust Anchor should send DNSSEC queries to Authoritative name servers. It is possible that the DNSSEC message from authoritative name servers was blocked or dropped because of some old network apparatuses which are mentioned above. In this case, recursive name servers would return ServFail responses to stub resolvers due to verification failure. However, the security-aware resolver which is configured with Weak Trust Anchor should send non-DNSSEC queries again to Authoritative name servers to get non-DNSSEC responses when the DNSSEC packets were lost or dropped. If the security-aware resolver gets non-DNSSEC responses, the resolver will send the result to the end user as insecure DNS data.

3. Authoritative Name server Considerations

Weak trust anchor is only configured at the resolver side, so it is useless to Authoritative name servers.

4. Resolver Considerations

Typically, a security-aware resolver will do the DNSSEC validation in the process of a DNS query. This validation would fail if any DNS message was faked or the DNS packet was dropped in the transmission. With the implementation of DNSSEC, the DNS packet is growing larger and its size would probably exceed 1500 bytes. Although both security-aware resolvers and Authoritative name servers should support EDNS0 to receive and send large packets, the problem still exists because the packet loss possibly happens in some special area in the Internet. In this case, the DNSSEC validation will be failed because of the internet devices, and then the related domain names will be invisible for some end users because the DNSSEC validation failed.

This document tries to solve this problem with weak trust anchor. If the security-aware resolver was configured with the weak trust anchor, it would do the DNSSEC verification as usual. It takes the responsibilities of recursive requests and the DNSSEC validation.

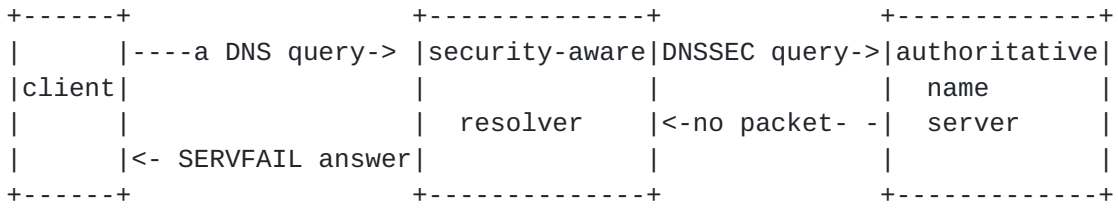
After sending a request with DO bit set, there are three possibilities at the security-aware resolver side:

- Receives a DNS packet with DNSSEC information
- Receives a DNS packet without DNSSEC information
- Receives nothing

If the security-aware resolver was configured with weak trust anchor, the DNSSEC verification process is no different from the one with a normal trust anchor in the first two cases. The resolver will use this anchor to do the DNSSEC validation as the rule of [RFC4033][RFC4034] [RFC4035].

Things are different in the third case. If the resolver was configured with a weak trust anchor and got nothing after sending a request with DO bit set, then it should clear DO bit in the EDNS0 in the query message and query again to the authoritative name server. So it could receive a normal DNS message (with no DNSSEC information, if the previous packet loss was caused by large size) and continue its DNS query process, then return the result as an insecure message.

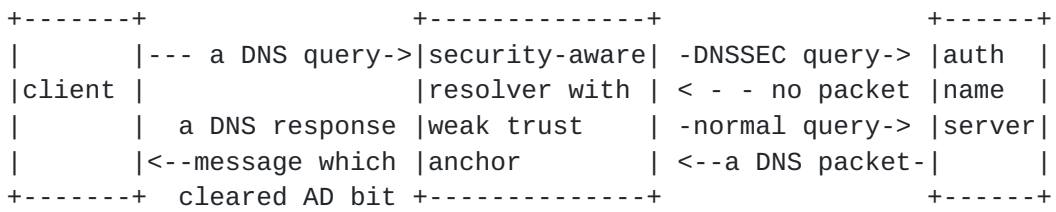
The normal process is followed:



normal process of dnssec query

Figure 1

The process of a security- aware resolver with weak trust anchor is shown as below:



weak trust anchor process of dnssec query

Figure 2

5. Security Considerations

This document tries to solve the problem that DNSSEC validation may fail in some certain networks because of the packet loss. ISPs could use this protocol to transfer the DNS service to DNSSEC-enabled DNS service when they do not know the complicated network environment.

If the DNS packet was tampered in the man-in-the-middle attack, the security-aware resolver will return servfail because of the DNSSEC verification failure in the weak trust anchor protocol. If DNSSEC packets are lost in the flight, the security-aware resolver can use non-DNSSEC process to query the authoritative name server again when it is configured with weak trust anchor, this technique can reduce the loss for the ISPs and end users.

6. Acknowledgments

Thanks to jianjun and others who reviewed this draft and give some valuable feedback.

7. References

7.1. Normative References

[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.

[RFC5011] StJohns, M., "Automated Updates of DNS Security (DNSSEC) Trust Anchors", RFC 5011, September 2007.

[RFC5155] Laurie, B., Sisson, G., Arends, R., and D. Blacka, "DNS Security (DNSSEC) Hashed Authenticated Denial of Existence", RFC 5155, March 2008.

7.2. Informative References

[RFC4641] Kolkman, O. and R. Gieben, "DNSSEC Operational Practices", RFC 4641, September 2006.

Authors' Addresses

Xiaodong Lee (editor)
cnnic

EMail: xl@cnnic.cn

Haikuo Zhang (editor)
cnnic

EMail: zhanghaikuo@cnnic.cn

Nan Wang (editor)
cnnic

EMail: wangnan@cnnic.cn

Peng Zuo (editor)
cnnic

EMail: zuopeng@cnnic.cn

Xiali Yan (editor)
cnnic

EMail: yanxiali@cnnic.cn

Ce Luo (editor)
cnnic

EMail: luoce@cnnic.cn

Hongtao Li (editor)
cnnic

EMail: lihongtao@cnnic.cn