Network Working Group
Request for Comments: 3655
Updates: 2535
Category: Standards Track

B. Wellington
O. Gudmundsson

November 2003

Redefinition of DNS Authenticated Data (AD) bit

Status of this Memo

Copyright Notice

Abstract

This document alters the specification defined in RFC 2535. Based on implementation experience, the Authenticated Data (AD) bit in the DNS header is not useful. This document redefines the AD bit such that it is only set if all answers or records proving that no answers exist in the response has been cryptographically verified or otherwise meets the server's local security policy.

1. Introduction

Familiarity with the DNS system [RFC1035] and DNS security extensions [RFC2535] is helpful but not necessary.

As specified in RFC 2535 (section 6.1), the AD (Authenticated Data) bit indicates in a response that all data included in the answer and authority sections of the response have been authenticated by the server according to the policies of that server. This is not especially useful in practice, since a conformant server SHOULD never reply with data that failed its security policy.

This document redefines the AD bit such that it is only set if all data in the response has been cryptographically verified or otherwise meets the server's local security policy. Thus, neither a response containing properly delegated insecure data, nor a server configured without DNSSEC keys, will have the AD set. As before, data that failed to verify will not be returned. An application running on a host that has a trust relationship with the server performing the

recursive query can now use the value of the AD bit to determine whether the data is secure.

1.1. Motivation

A full DNSSEC capable resolver called directly from an application can return to the application the security status of the RRsets in the answer. However, most applications use a limited stub resolver that relies on an external recursive name server which incorporates a full resolver. The recursive nameserver can use the AD bit in a response to indicate the security status of the data in the answer, and the local resolver can pass this information to the application. The application in this context can be either a human using a DNS tool or a software application.

The AD bit SHOULD be used by the local resolver if and only if it has been explicitly configured to trust the remote resolver. The AD bit SHOULD be ignored when the recursive name server is not trusted.

An alternate solution would be to embed a full DNSSEC resolver into every application, but this has several disadvantages.

- DNSSEC validation is both CPU and network intensive, and caching SHOULD be used whenever possible.

- DNSSEC requires non-trivial configuration - the root key must be configured, as well as keys for any "islands of security" that will exist until DNSSEC is fully deployed. The number of configuration points should be minimized.

1.2. Requirements

The key words "MAY", "MAY NOT" "MUST", "MUST NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", in this document are to be interpreted as described in BCP 14, RFC 2119 [RFC2119].

1.3. Updated documents and sections

The definition of the AD bit in RFC 2535, Section 6.1, is changed.

2. Setting of AD bit

The presence of the CD (Checking Disabled) bit in a query does not affect the setting of the AD bit in the response. If the CD bit is set, the server will not perform checking, but SHOULD still set the AD bit if the data has already been cryptographically verified or

complies with local policy. The AD bit MUST only be set if DNSSEC records have been requested via the DO bit [RFC3225] and relevant SIG records are returned.

2.1. Setting of AD bit by recursive servers

Section 6.1 of RFC 2535 says:

"The AD bit MUST NOT be set on a response unless all of the RRs in the answer and authority sections of the response are either Authenticated or Insecure."

The replacement text reads:

"The AD bit MUST NOT be set on a response unless all of the RRsets in the answer and authority sections of the response are Authenticated."

"The AD bit SHOULD be set if and only if all RRs in the answer section and any relevant negative response RRs in the authority section are Authenticated."

A recursive DNS server following this modified specification will only set the AD bit when it has cryptographically verified the data in the answer.

2.2. Setting of AD bit by authoritative servers

A primary server for a secure zone MAY have the policy of treating authoritative secure zones as Authenticated. Secondary servers MAY have the same policy, but SHOULD NOT consider zone data Authenticated unless the zone was transferred securely and/or the data was verified. An authoritative server MUST only set the AD bit for authoritative answers from a secure zone if it has been explicitly configured to do so. The default for this behavior SHOULD be off.

Note that having the AD bit clear on an authoritative answer is normal and expected behavior.

2.2.1. Justification for setting AD bit w/o verifying data

The setting of the AD bit by authoritative servers affects only the small set of resolvers that are configured to directly query and trust authoritative servers. This only affects servers that function as both recursive and authoritative. Iterative resolvers SHOULD ignore the AD bit.

The cost of verifying all signatures on load by an authoritative server can be high and increases the delay before it can begin

answering queries. Verifying signatures at query time is also expensive and could lead to resolvers timing out on many queries after the server reloads zones.

Organizations requiring that all DNS responses contain cryptographically verified data will need to separate the authoritative name server and signature verification functions, since name servers are not required to validate signatures of data for which they are authoritative.

3. Interpretation of the AD bit

A response containing data marked Insecure in the answer or authority section MUST never have the AD bit set. In this case, the resolver SHOULD treat the data as Insecure whether or not SIG records are present.

A resolver MUST NOT blindly trust the AD bit unless it communicates with a recursive nameserver over a secure transport mechanism or using a message authentication such as TSIG [RFC2845] or SIG(0) [RFC2931] and is explicitly configured to trust this recursive name server.

4. Applicability statement

The AD bit is intended to allow the transmission of the indication that a resolver has verified the DNSSEC signatures accompanying the records in the Answer and Authority section. The AD bit MUST only be trusted when the end consumer of the DNS data has confidence that the intermediary resolver setting the AD bit is trustworthy. This can only be accomplished via an out of band mechanism such as:

- Fiat: An organization that can dictate whether it is OK to trust certain DNS servers.

- Personal: Because of a personal relationship or the reputation of a recursive nameserver operator, a DNS consumer can decide to trust that recursive nameserver.

- Knowledge: If a recursive nameserver operator posts the configured policy of a recursive nameserver, a consumer can decide that recursive nameserver is trustworthy.

In the absence of one or more of these factors AD bit from a recursive name server SHOULD NOT be trusted. For example, home users frequently depend on their ISP to provide recursive DNS service; it

is not advisable to trust these recursive nameservers. A roaming/traveling host SHOULD not use recursive DNS servers offered by DHCP when looking up information where security status matters.

In the latter two cases, the end consumer must also completely trust the path to the trusted recursive name servers, or a secure transport must be employed to protect the traffic.

When faced with a situation where there are no satisfactory recursive nameservers available, running one locally is RECOMMENDED. This has the advantage that it can be trusted, and the AD bit can still be used to allow applications to use stub resolvers.

5. Security Considerations

This document redefines a bit in the DNS header. If a resolver trusts the value of the AD bit, it must be sure that the responder is using the updated definition, which is any DNS server/resolver supporting the DO bit [RFC3225].

Authoritative servers can be explicitly configured to set the AD bit on answers without doing cryptographic checks. This behavior MUST be off by default. The only affected resolvers are those that directly query and trust the authoritative server, and this functionality SHOULD only be used on servers that act both as authoritative and recursive name servers.

Resolvers (full or stub) that blindly trust the AD bit without knowing the security policy of the server generating the answer can not be considered security aware.

A resolver MUST NOT blindly trust the AD bit unless it communicates such as IPsec, or using message authentication such as TSIG [RFC2845] or SIG(0) [RFC2931]. In addition, the resolver must have been explicitly configured to trust this recursive name server.

6. IANA Considerations

None.

7. Internationalization Considerations

None. This document does not change any textual data in any protocol.

8. Intellectual Property Rights Notice

9. Acknowledgments

The following people have provided input on this document: Robert Elz, Andreas Gustafsson, Bob Halley, Steven Jacob, Erik Nordmark, Edward Lewis, Jakob Schlyter, Roy Arends, Ted Lindgreen.

10. Normative References

[RFC1035] Mockapetris, P., "Domain Names - Implementation and Specification", STD 13, RFC 1035, November 1987.

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

[RFC2535] Eastlake, D., "Domain Name System Security Extensions", RFC 2535, March 1999.

[RFC2845] Vixie, P., Gudmundsson, O., Eastlake 3rd, D. and B. Wellington, "Secret Key Transaction Authentication for DNS (TSIG)", RFC 2845, May 2000.

[RFC2931] Eastlake, D., "DNS Request and Transaction Signatures (SIG(0))", RFC 2931, September 2000.

[RFC3225] Conrad, D., "Indicating Resolver Support of DNSSEC", RFC 3225, December 2001.

11. Authors' Addresses

Brian Wellington
Nominum Inc.
2385 Bay Road
Redwood City, CA, 94063
USA

EMail: Brian.Wellington@nominum.com

Olafur Gudmundsson
3821 Village Park Drive
Chevy Chase, MD, 20815
USA

EMail: ogud@ogud.com

12. Full Copyright Statement

Acknowledgement

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