Available online at www.sciencedirect.com

SciVerse ScienceDirect

journal homepage: www.elsevier.com/locate/ijcip

Maintenance, mishaps and mending in deployments of the domain name system security extensions (DNSSEC)

Casey Deccio

Informatics and Systems Assessments Department, Sandia National Laboratories, P.O. Box 969, Livermore, California 94551, USA

ARTICLE INFO

Article history:
Received 18 February 2012
Accepted 16 May 2012
Published online 2 June 2012

Keywords:
Domain name system (DNS)
Domain name system security extensions (DNSSEC)
Misconfiguration

ABSTRACT

The Domain Name System Security Extensions (DNSSEC) add an element of authentication to the DNS, which is a foundational component of the Internet. However, the maintenance of a DNSSEC deployment is more complex than that of its insecure counterpart. This paper discusses some specific misconfigurations that impact DNSSEC deployments, analyzes their prevalence via an extended survey of production DNS zones implementing DNSSEC, and assesses the maintenance and corrective actions. Our survey indicated that more than one-half of the zones analyzed were affected by misconfigurations. Also, the survey revealed a significant number of repeat occurrences and average correction times of up to two weeks. This paper summarizes the survey findings and suggests approaches for improving the quality of DNSSEC deployments.

1. Introduction

The Domain Name System (DNS) [1,2] is a distributed database for looking up data based on domain name and query type and, as such, is one of the foundational components of the Internet. The most common use of DNS is mapping domain names to Internet addresses.

The Domain Name System Security Extensions (DNSSEC) [3–5] were introduced to protect the integrity of DNS responses. DNSSEC allows DNS administrators to cryptographically sign and validate DNS data. The number of DNSSEC-signed zones has increased significantly in the last year and these include the DNS root zone and a large number of top-level domains (TLDs) [6–8]. However, in order to achieve its security benefits, DNSSEC adds complexity to the DNS. This increases the chances of a DNS outage if DNSSEC is not properly deployed or maintained. The effects of misconfigurations have been felt at various levels in the DNS hierarchy, including TLDs. An understanding of DNSSEC components, their relationships and the protocol itself are essential for proper deployment.

This paper reviews the results of analyzing a portion of the DNSSEC deployment over approximately one year (June 2010–July 2011) in an attempt to answer three questions: (i) What DNSSEC maintenance practices are being employed? (ii) What is the prevalence of misconfiguration among DNSSEC deployments? (iii) How are operators addressing broken DNSSEC deployments?

The analysis is based on a survey of a sample of DNSSEC-signed zones polled over an extended period of time. The results of the analysis are used to suggest tools whose functionality could improve the quality of DNSSEC deployments.

2. DNS background

In the DNS [1,2], a "resolver" queries "authoritative servers" to receive answers. The resolver learns authoritative servers for a "DNS zone" by starting at the "root zone" and following referrals downward in delegated DNS namespace until it receives an authoritative response. The queries include a

E-mail address: ctdecci@sandia.gov.

1874-5482/$ - see front matter
doi:10.1016/j.ijcip.2012.05.002

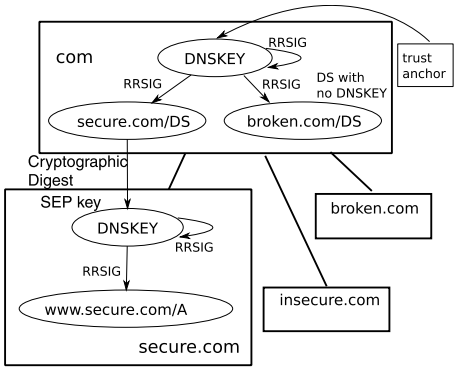

Fig. 1 – Chain of trust for several zones under the *com* zone.

name and type, and the answers are comprised of "resource records" (RRs), which have a name, type and record data. Resource records are grouped by name and type into "resource record sets" (RRsets).

DNSSEC [3–5] adds authentication to the DNS. RRsets are signed on a per-zone basis and each signature is contained in an RRSIG RR. Authoritative servers return RRSIGs with any RRsets they cover. The public keys of a zone are published in the DNSKEY RRset of the zone. Using an RRSIG and the corresponding DNSKEY, a validating resolver can verify the integrity of the RRset it covers.

DNSSEC scales by establishing a "chain of trust" upwards through the namespace hierarchy, and anchoring it with the DNSKEY of a common ancestor zone, typically the root. The link between zones is accomplished by the introduction of "delegation signer" (DS) RRs in the parent zone. A DS includes the cryptographic digest of a DNSKEY in the child zone of the same name. When the DNSKEY corresponding to an authenticated DS or trust anchor is used to the sign the DNSKEY RRset of a zone, it becomes a "secure entry point" (SEP) and all DNSKEYs in the RRset are authenticated. A common practice is for a zone to sign only its DNSKEY RRset with the SEP key (a "key signing key" (KSK)) and sign other zone data with a second key (a "zone signing key" (ZSK)). Fig. 1 illustrates the DNSSEC chain of trust.

DNSSEC also provides "authenticated denial of existence"–an assurance that an RRset with queried name and type does not exist. This is accomplished using "next-secure" (NSEC) RRs, which are provided in a response to show a validator where the non-existent RRset would appear (i.e., in a canonical ordering of the names in the zone) if it did exist. "Hashed authenticated denial of existence" using NSEC3 RRs is a newer protocol that address the challenges inherent in the use of NSEC [9].

3. DNSSEC challenges

DNSSEC carries additional maintenance considerations, and negligence or misconfigurations can result in validation failures. This section discusses DNSSEC maintenance and misconfigurations.

Since RRSIGs have a limited lifetime, the RRsets they cover must be periodically re-signed to replace RRSIGs that would otherwise go stale. While DNSKEYs technically do not expire, it is recommended that they be replaced periodically using a process called "key rollover" [10]. Non-SEP DNSKEYs can be rolled over without involving third-parties and are, thus, self-contained. However, when a SEP DNSKEY is rolled over, the parent zone must be involved to handle the change in DS RRs. Likewise, a validator must be engaged when a configured trust anchor is rolled over [11].

A misconfiguration of a DNSSEC deployment can result in a broken chain of trust and failed validation for the RRsets involved. We enumerate six specific misconfigurations that are considered in this paper:

- DS Mismatch: If DS RRs are present in a parent zone, but none of them correspond to any self-signing DNSKEYs in the child zone, then the chain of trust is broken and RRsets in the child zone and below are deemed bogus. This is the case with *broken.com* in Fig. 1.
- DNSKEY Missing: If a DNSKEY referenced in an RRSIG or DS is necessary to complete a chain of trust, but is not included in the DNSKEY RRset, then the chain is broken.
- NSEC Missing: The lack of NSEC RRs in a negative response (e.g., non-existent domain name) results in failed validation of the response. Validated negative responses are particularly critical to insecure delegations for proving that no DS RRs exist for a child zone and, thus, that there is no secure link from parent to child zone. This is the case with *insecure.com* in Fig. 1.
- RRSIG Missing: If an authoritative server does not provide the RRSIGs necessary to complete a chain of trust for a given RRset, then the chain is broken.
- RRSIG Bogus: The signature in the record data of an RRSIG must validate against the RRset it covers, or it is invalid.
- RRSIG Dates: If an RRSIG is allowed to expire or is published before its inception date, then it fails to validate.

4. DNSSEC deployment survey and analysis

Our survey of DNSSEC deployments involved the periodic polling of production DNS zones signed with DNSSEC. The polling was performed over a period of just over one year—June 2010–July 2011. Each signed zone was analyzed several times per day by querying each of its authoritative servers to elicit various DNSSEC-related responses. The zones came from three sources: hostnames extracted from URLs indexed by the Open Directory Project (ODP) [12]; names queried to recursive resolvers at the Supercomputing 2008 Conference; and names submitted by third parties to the web-based DNSViz analysis tool [13].

We identified production signed zones in the data set by considering only those zones that signaled their intent to be validated by resolvers—those with an authentication chain to the root zone trust anchor (after the July 2010 signing of the root [7]) or to the trust anchor at ISC's DNSSEC Lookaside Validation (DLV) service [14]. DLV [15] was introduced to allow an arbitrary zone to be securely linked to a zone other than its hierarchical parent for trust anchor scalability prior to root signing. We also excluded zones that were apparently not set up for production DNSSEC—those containing the names