Digital Object Identifier: 10.1007/978-3-642-36516-4_13

URL: http://link.springer.com/chapter/10.1007%2F978-3-642-36516-4_13

Measuring Occurrence of DNSSEC Validation

Matthäus Wander and Torben Weis

University of Duisburg-Essen, Duisburg, Germany
Email: dnssec@vs.uni-due.de,
Web: http://dnssec.vs.uni-due.de

Abstract. DNSSEC is a security extension that adds public-key signatures to the Domain Name System for the purpose of data authenticity and integrity. While DNSSEC signatures are being deployed on an increasing number of name servers, little is known about the deployment advancements of client-side DNSSEC validation. In this paper we present a methodology to determine whether a client is protected by DNSSEC validation. We applied our methodology over a period of 7 months collecting results from different data sources. After data cleaning, we gathered 131,320 results from 98,179 distinct IP addresses, out of which 4.8% had validation enabled. The ratio varies significantly per country, with Sweden, the Czech Republic and the United States having the largest ratios of validating clients in the field.

1 Introduction

The original Domain Name System (DNS) specification did not provide any security measures to protect from forged domain names. As DNS heavily relies on UDP messages, an attacker can send spoofed DNS responses, as e.g. demonstrated by Kaminsky in 2008 [1]. In order to mitigate DNS spoofing, senders currently encode random entropy into DNS messages without breaking the message format, e.g. random transaction ID and source port. This lowers the attackers' spoofing success rate, but still attacks remain feasible for insistent remote attackers and trivial for local attackers, e.g. when eavesdropping on a public Wi-Fi hotspot. Cryptographic DNS protocol extensions have been proposed to make DNS spoofing infeasible, most notably DNSSEC [2] which is being deployed right now. DNSSEC utilizes public-key cryptography to sign and verify public DNS data. For verification, the public key of the root zone must be known beforehand to the resolver (DNS client). A delegation signer (DS) record indicates whether a child zone is signed and contains the fingerprint (hash value) of the child zone's public key. The resolver can thus securely retrieve the public key of the child zone when needed.

Apart from establishing secure name resolution, DNSSEC deployment implies some side effects. The cryptographic enhancement increases CPU and network load on name servers and validating resolvers. Distributed denial of service attacks which abuse the public DNS infrastructure for traffic amplification become more effective with large DNSSEC responses. Rogue DNS redirects become impossible for malicious attackers but also for governments and ISPs which

may act legitimated by national law or company policy. This includes redirects to governmental censorship or legal notices, DNS injection [3] and redirects to advertisement web pages [4]. Unlike e.g. SSL/TLS certificate failures, there is currently no application-level handling of DNSSEC validation failures [5]. When validation fails on a DNSSEC-enabled resolver, it passes a general name resolution error back to the application (e.g. web browser) which is indistinguishable from a network error.

Our contribution in this paper is a methodology to measure the occurrence of client-side DNSSEC validation and an analysis of such a measurement in practice. Different validation measures are possible, e.g. the number of clients protected by validation, the number of resolvers performing validation or the number of responses received by validating resolvers. We chose to count the number of clients because from this measure one can deduce the amount of users protected by DNSSEC.

2 Methodology

We set up a DNS zone VERTEILTESYSTEME.NET, signed it and added a DS record to the .NET zone. Two domain names in our zone return an A record, SIGOK with a valid signature and SIGFAIL with a placeholder signature, which is syntactically correct but fails to validate. We are using two test types: a scripted test that provides user feedback [6] and a hidden test that can be embedded into other web pages.

2.1 Scripted Test

The web-based scripted test uses client-side JavaScript to load an image from the SIGFAIL domain name. When loading the image succeeds, the resolver does not validate DNSSEC signatures as it failed to recognize the invalid signature. When loading fails, the script attempts to load an image from the SIGOK domain name. This happens to rule out other error sources, e.g. a stalled network connection or an unrelated DNS resolution fault. If the second image has been loaded, the resolver correctly validates DNSSEC signatures. Should the second image fail to load as well, then the test was inconclusive. The result is displayed to the user and posted to our web server in background.

2.2 Hidden Test

The web-based hidden test uses two `<img>` tags which can be embedded into existing web pages (Fig. 1). The two image URLs redirect the client browser to a transparent 1×1 pixel image at *ID*.SIGOK and *ID*.SIGFAIL. *ID* is a hexadecimal number 0000 to FFFF used to identify the client. As most clients do not resolve domain names by themselves, the client IP address seen by our web server usually differs from the resolver IP address seen by our name server. The ID number relates browser queries to resolver queries and enables us to analyze

```
<img src="http://dnssec.vs.uni-due.de/r/a" alt="" height="1" width="1">
<img src="http://dnssec.vs.uni-due.de/r/b" alt="" height="1" width="1">
```

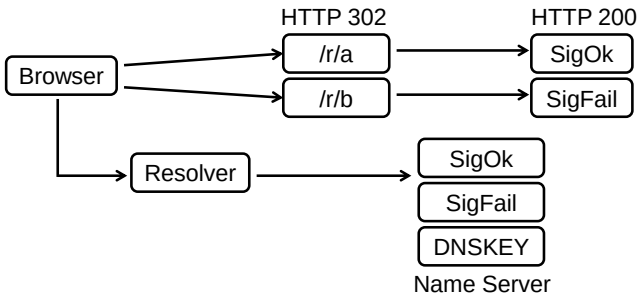

Fig. 1. Static HTML code block and queries of hidden test

their coherent behavior. This method is similar to the one used by Mao et al. in 2002 [7] but instead of embedding the IP address a 16 bit hash value is derived from the IP address. The rationale behind this method is as follows:

1. By using an HTTP redirect we can embed a static HTML code snippet into existing web pages and track the queries by client ID. When including the ID directly into the image URLs this would require to dynamically generate the HTML code.
2. The DNS zone is moderately sized when using 16 bit for the ID. As we need to deliver valid and invalid signatures, we pre-generate the DNS zone, sign it and then replace the SIGFAIL signatures with broken placeholders. This results in an 88 MB zone file with 2^{19} resource records (A and RRSIG, NSEC and RRSIG, for both SIGOK and SIGFAIL). If we dynamically created and signed the resource records as needed, this would require either a customized name server or an unusual zone layout which might pose a pitfall for some resolvers.
3. By deriving the ID number from the client IP address we get a simple stateless mapping which does not change while the same client is visiting multiple web pages and is unlikely to collide with another client at the same time.

DNSSEC validation is enabled if there were HTTP GET requests for the two redirect URLs and the SIGOK image but none for the SIGFAIL image. It is disabled if there were HTTP GET requests for the redirect URLs and both images.

2.3 Accuracy

For a positive test result we require the client to load an image from the signed SIGOK domain name. This is meant to catch faults that could spoil the result, e.g. blocking our signed domain name, not automatically loading images, not following cross-domain HTTP redirects or failing to receive EDNS0 messages

> 512 bytes. The responses for SIGOK and SIGFAIL are nearly the same size with a packet size of < 1000 bytes. Nevertheless, one of the images could fail to load for an unrelated reason, e.g. temporary network fault or user closes web page before it has been loaded completely. Should this happen, then the following faults are possible:

1. None of the images are loaded: does not affect our results.
2. SIGFAIL loads and SIGOK does not load: does not affect our results.
3. SIGOK loads and SIGFAIL does not load: causes a false positive in our results.

To estimate the ratio of false positives caused by case 3, we calculate the number of occurrence of case 2. Both cases can only occur with non-validating resolvers and correspond to the same fault pattern. Note that this type of fault can not cause false negatives.

Another possible fault source is caching. All tests mentioned above use a time to live (TTL) value of 60 seconds for the SIGOK and SIGFAIL resource records. To minimize the impact of browser caching, we return *no-cache* headers in image responses. Caching can spoil the result if the validation configuration has changed, i.e. when the resolvers have been reconfigured or when a client has moved to another network.

3 Analysis

We logged 3,387,622 DNS and HTTP requests over a period of 7 months starting in May 2012. This comprises three data sources: 1) participants of our scripted test 2) visits from *autosurf* websites which generate page views[1] in exchange for community credits 3) visits from websites which kindly included our hidden test. The results were evaluated offline by parsing the web server and name server logfiles. We grouped the requests together by ID into Bernoulli trials when the time delta between two requests was < 30s. Larger time deltas were grouped into different trials which resulted in 419,747 trials.

3.1 Data Cleaning

We removed 146,786 invalid trials which were lacking the minimum required set of requests. A valid trial requires at least both HTTP redirects to SIGOK and SIGFAIL, both DNS queries and an HTTP query to the SIGOK image. Fig. 2 shows the occurrence of invalid trials. Most are caused by a client browsing a website over a couple of minutes, loading the hidden test URLs with each page view. While the HTTP redirects are intended to be cached, web browsers also excessively cache DNS responses in disregard of their low TTL values. Another cause for invalid trials are web crawlers or similar noise. As explained in Section 2.3, incorrectly missing SIGFAIL image queries are causing false positives in our measurement. The equivalent fault pattern of a missing SIGOK image query

Missing query	Both	SIGOK	SIGFAIL
HTTP redirect	55,052	4,431	5,010
DNS query	74,560	3,673	2,050
HTTP image	1,634	376	-

Fig. 2. Invalid trials

Filter condition	Count
12h duplicates	141,433
ID hash collision	11
DNSKEY missing	425

Fig. 3. Filtered trials (overlapping)

occurred in 376 trials, which makes an estimate of 0.14% false positives of all valid trials.

We then applied different filters to the remaining trials to remove duplicate or dubious results. In total one or more filter conditions applied to 141,641 trials (Fig. 3). Most trials are filtered by ignoring duplicate results: we consider each client IP address only once every 12h. When users browse a participating website for a couple of minutes, they leave several trials, one for each page view. The deduplication period should be long enough to cover the whole browsing session of the user but not longer than the assignment of a dynamic IP address. Dynamic IP addresses cause two problems in combination with deduplication: 1. the same client may be counted twice with different IP addresses (unlike clients with static IP addresses) 2. another client may be filtered when assigned the same IP address. Xie et al. estimated the time interval between two different users on the same dynamic IP address to be >12h in 80% of all cases [8]. With a period of 12h we expect to filter duplicates without adding significant bias due to differences between dynamic and static clients. Experiments with different deduplication periods from 2h to 7d show a minor influence on the overall validation ratio (±0.3% points).

A negligible amount of trials (<0.01%) became useless because a hash collision occurred in our IP address to ID mapping. 425 trials (0.16%) were filtered because they were classified as positive but lacked a DNSKEY query. This indicates a false positive and is comparable to the estimate above. We do not count these as negative results because there is a possible scenario in which we might mistakenly include an actually true positive. When a validating resolver uses two or more non-validating forwarders[2], we may receive queries for SIGOK and SIGFAIL from one IP address and a query for DNSKEY from another IP address. The DNSKEY query would be missing in this trial because we correlate DNSKEY queries by IP address and not by ID. This limitation could be improved in future by including the ID into DNSKEY records.

We did not attempt to identify single users behind the same public NAT IP address because clients within a local network typically share the same DNS configuration. In some cases we observed inconsistent client IP addresses. The HTTP redirects need to be queried from the same client IP address, otherwise this would result in two different IDs and thus invalid trials. The HTTP images may be queried from a different IP address as they are correlated by ID. This

[1] visits are mostly unattended but in end user environment and thus serve our purpose
[2] such setup is debatable as it limits the ability to scatter retries when validation fails

happened in 1.4% of all valid trials, often clearly by the same user with multiple client IP addresses due to enterprise NAT. We also identified a German regional ISP which operates carrier-grade NAT for broadband customers. As we did not find any unwanted effect on our results, we kept trials with inconsistent client IP addresses in our result set.

3.2 Results

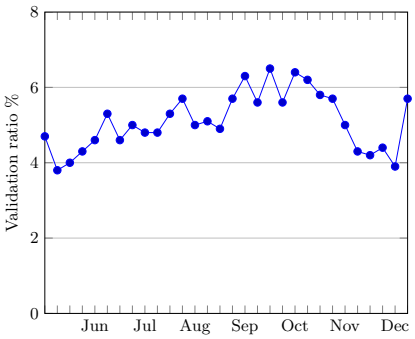

Fig. 4. Overall validation

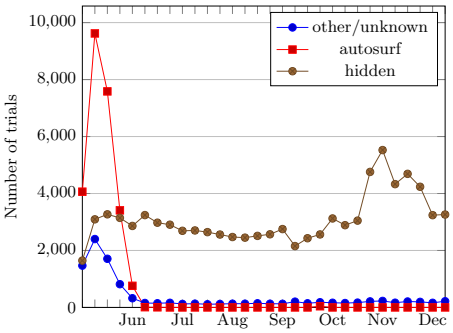

Fig. 5. Data sources

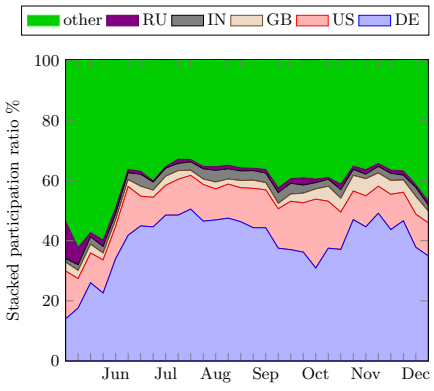

Fig. 6. Top 5 participating countries

AS	$\frac{V}{V_{total}}$	$\frac{V}{V+N}$	cli=dns
Comcast 7922	29.1%	69.0%	0.5%
KabelBW 29562	14.3%	86.4%	0.3%
M-Net 8767	6.1%	46.6%	3.9%
Telia SE 3301	3.3%	73.8%	1.5%
O2 CZ 5610	3.0%	69.2%	0.5%
Telenor 2119	2.2%	54.1%	0.7%
pt.lu 6661	1.7%	83.5%	0.0%
rub.de 29484	1.6%	34.1%	0.0%
TELE2 1257	1.5%	52.4%	0.0%
DFN 680	1.5%	3.3%	4.3%
other	35.9%	1.9%	17.8%

Fig. 7. Top 10 validating ASes

After data cleaning there are 131,320 remaining trials from 98,179 distinct client IP addresses. According to HTTP referers, most clients originate from the website CrypTool.org (67%) and from the autosurf communities TrafficSpammer (10%) and eBesucher (9%). We consider a trial as negative if

it contains an HTTP query to SIGFAIL or if all DNS queries are sent without DNSSEC OK flag. In contrast, a positive result does not contain any SIGFAIL HTTP query and at least one DNS query was sent with EDNS0 and DNSSEC OK flag. Overall 6,323 trials were positive (4.8%) and Fig. 4 shows the results per week. The dips in May and November correlate with the distribution of data sources (see Fig. 5) and can be explained by differences per country. The autosurf communities have a broad user base from various countries while the hidden website test was accessed mainly from Germany (43% of all "hidden" accesses) and the United States (12%). Changes in the country participation ratio (Fig. 6), e.g. fewer accesses from the U.S. in November, influence the overall validation ratio. The results per country are hence more meaningful than the overall ratio which is inclined towards the DE and US numbers.

#	Country	Trials	Validation ratio	#	Country	Trials	Validation ratio
1.	SE	1099	$56.3\% \pm 1.5$	11.	GR	1939	$3.7\% \pm 0.4$
2.	CZ	957	$31.1\% \pm 1.5$	12.	IT	1537	$3.5\% \pm 0.5$
3.	US	15368	$13.1\% \pm 0.3$	13.	ID	1332	$2.6\% \pm 0.4$
4.	HU	526	$9.9\% \pm 1.3$	14.	PT	602	$2.5\% \pm 0.6$
5.	CH	2975	$5.6\% \pm 0.4$	15.	UA	1922	$1.9\% \pm 0.3$
6.	FR	3043	$4.8\% \pm 0.4$	16.	AU	1053	$1.5\% \pm 0.4$
7.	BR	1319	$4.5\% \pm 0.6$	17.	CA	1562	$1.4\% \pm 0.3$
8.	NL	2076	$4.1\% \pm 0.4$	18.	GB	4312	$1.3\% \pm 0.2$
9.	PL	2107	$3.9\% \pm 0.4$	19.	AR	577	$1.2\% \pm 0.5$
10.	DE	46624	$3.8\% \pm 0.1$	20.	RS	983	$1.1\% \pm 0.3$

Fig. 8. Validation ratio per country ($\pm$ standard deviation in binomial distribution)

There are 79 countries in the data set with >100 trials and 40 countries with >500 trials. Fig. 8 shows the top validating countries out of the >500 trials subset, sorted by validation ratio. Half of the countries in the >500 trials subset have a validation ratio of $\leq$1%.

Fig. 7 shows the top validating autonomous systems (AS) by absolute number of trials. $\frac{V}{V_{total}}$ is the fraction of the positive results of one AS to all ASes. $\frac{V}{V+N}$ is the fraction of positive to all results within one AS. While some are fairly high, no AS is fully protected by DNSSEC. The last column cli=dns is the fraction of trials in which the client IP address equals at least one DNS resolver being used. The low number indicates that most validating clients use the DNS infrastructure of the AS operator as forwarder.

2,150 trials are negative results despite containing a DNSKEY query, suggesting that a single DNSKEY query is an unsuitable validation indicator. This comprises trials with one and with multiple resolver IP addresses. Using multiple resolvers (or forwarders) is quite common, though mostly within the same AS. In 4,991 trials DNS resolvers appeared from different ASes. Most commonly seen AS numbers for resolvers outside of the client AS were AS15169 (Google),

AS36692 (OpenDNS) and AS3356 (Level 3). The complete anonymized data set grouped into trials is available for public download [6].

4 Related Work

There exists thorough work on measuring and analyzing the server-side DNSSEC deployment advances [9] [10], i.e. the number and status of signed zones. Our scope in this paper is the client-side DNSSEC deployment, i.e. the number of clients protected by validators.

4.1 Passive Measurements

Public statistics from RIPE NCC [11] indicate that about 70% of all queries at the K-root name server are coming from resolvers that are capable of parsing DNSSEC answers. However, one can not deduce from this indicator whether validation is actually enabled. Another number measured at K-root are the queries for DNSKEY resource records which was about 2 queries/s in August 2012. Validating resolvers are expected to refresh the root DNSKEY within specified intervals [12] but the total number of resolvers querying K-root is unknown and so is the amount of extra DNSKEY queries due to pollution [13]. Hence, this measurement allows for observing the validation tendency but not the actual validation ratio.

Gudmundsson and Crocker [14] measured the validation ratio in 2010/11 by analyzing network traces from authoritative name servers for .ORG. Capturing and processing network traces is resource-intensive, therefore they were limited to 50 min traces from a subset of name servers. As resolvers do not distribute evenly across redundant name servers but instead prefer low latency, this subset might pose an incomplete view. They applied different criteria and found out that looking for DS queries is more effective in their scenario than looking for DNSKEY queries. The ratio of validating resolvers was 0.8% (mistakenly stated as 1.2%) which accounted for 8–10% observed queries to .ORG, though part of the queries may have been pollution due to dropped EDNS0 packets or amplification attacks. The geographical distribution and the number of clients served by these resolvers is unknown.

Fujiwara performed a similar measurement for .JP over a period of one year [15] [16]. He acquired 2 day network traces from all authoritative name servers for .JP on selected dates and interpolated interjacent numbers by analyzing partial log files. The number of resolvers querying for DNSKEY rose from 3,000 (0.2%) in March 2011 to 10,000 in February 2012.

4.2 Web-based Tests

VeriSign runs a web-based project to quantify validating resolvers [17]. It uses the link prefetching feature of web browsers but does not require any HTTP requests. The target domain name resolves to an unsigned record, though there is

a DS record indicating that it ought to be signed. A non-validating resolver will accept this response while a validating one will retry several times. The query pattern observed is used to fingerprint the resolver implementation. Despite using a different measure—counting resolvers not clients—the overall validation ratio is comparable to our results. The geographic distribution confirms our top two results for Sweden and the Czech Republic. The U.S. result is much lower, presumably because the large user base of AS7922 (Comcast) is served by few resolvers. VeriSign also provides a web page TEST.DNSSEC-OR-NOT.NET for users to check their validation status.

Another web-based DNSSEC test is provided by SIDN [18]. The client loads a web page DNSSECTEST.SIDN.NL which embeds an `<img>` tag pointing to a 1×1 pixel image. The domain name of the image URL contains a random ID and is signed with a valid chain of trust. Validating and non-validating resolvers both resolve the domain name, but only the validating resolver is expected to retrieve the DNSKEY record. When the image has been loaded, the JavaScript code queries the SIDN database whether the DNSKEY was retrieved and displays the result to the user. SIDN does not provide public statistics.

Test	JavaScript	Images	Criteria
dnssec.vs.uni-due.de	yes	yes	image loads
dnssec.vs.uni-due.de (hidden)	no	yes	image loads
test.dnssec-or-not.net	no	no	3× query retry
dnssectest.sidn.nl	yes	yes	DNSKEY

Fig. 9. Comparison of web-based test methods

Fig. 9 shows an overview of all tests described above. As the tests use different mechanics, they may return different results under certain conditions. We confirmed this for mixed validation when a client uses validating and non-validating resolvers. The VeriSign and SIDN tests are positive if the pattern of one validating resolver is found, even if the client falls back to a non-validating secondary resolver and actually resolves the domain name without validation. Our tests are positive, if all resolvers queried by the client reject the incorrectly signed domain name.

5 Conclusions

We presented a web-based methodology to determine whether a client uses DNSSEC validation. After applying this methodology in a practical measurement, we identified and eliminated various effects that could distort the results. DNSSEC validation does occur in practice but there are major differences in the adoption between countries. Most countries covered in our measurement have a validation ratio of less than 5%. A remaining issue is the investigation of using

mixed validating and non-validating resolvers. We expect our test to yield a negative result in case of mixed validation but the effect on the client application is not well understood yet.

References

1. Kaminsky, D.: Black ops 2008: It's the end of the cache as we know it. Black Hat USA (August 2008)
2. Arends, R., Austein, R., Larson, M., Massey, D., Rose, S.: DNS Security Introduction and Requirements. RFC 4033 (March 2005)
3. Anonymous: The collateral damage of internet censorship by dns injection. SIGCOMM Comput. Commun. Rev. **42**(3) (2012) 21–27
4. Weaver, N., Kreibich, C., Paxson, V.: Redirecting DNS for Ads and Profit. In: USENIX Workshop on Free and Open Communications on the Internet (FOCI), San Francisco, CA, USA (August 2011)
5. Hirsch, T., Iacono, L.L., Wechsung, I.: How much network security must be visible in web browsers? In: Proceedings of 9th International Conference on Trust, Privacy & Security in Digital Business (TrustBus). (2012)
6. Wander, M., Weis, T.: Dnssec resolver test. http://dnssec.vs.uni-due.de
7. Mao, Z.M., Cranor, C.D., Bouglis, F., Rabinovich, M., Spatscheck, O., Wang, J.: A precise and efficient evaluation of the proximity between web clients and their local dns servers. In: In Proceedings of USENIX Annual Technical Conference, USENIX Association (2002) 229–242
8. Xie, Y., Yu, F., Achan, K., Gillum, E., Goldszmidt, M., Wobber, T.: How dynamic are ip addresses? In: Proceedings of the 2007 conference on Applications, technologies, architectures, and protocols for computer communications. SIGCOMM '07, New York, NY, USA, ACM (2007) 301–312
9. Osterweil, E., Massey, D., Zhang, L.: Deploying and monitoring dns security (dnssec). In: Proceedings of the 2009 Annual Computer Security Applications Conference. ACSAC '09, Washington, DC, USA, IEEE Computer Society (2009) 429–438
10. Deccio, C., Sedayao, J., Kant, K., Mohapatra, P.: Quantifying and improving dnssec availability. In: Computer Communications and Networks (ICCCN), 2011 Proceedings of 20th International Conference on. (31 2011-aug. 4 2011) 1 –7
11. RIPE NCC: Status for k.root-servers.net. http://k.root-servers.org/statistics/ROOT/daily/ (accessed September 2012).
12. St.Johns, M.: Automated Updates of DNS Security (DNSSEC) Trust Anchors. RFC 5011 (September 2007)
13. Castro, S., Wessels, D., Fomenkov, M., Claffy, K.: A day at the root of the internet. SIGCOMM Comput. Commun. Rev. **38**(5) (September 2008) 41–46
14. Ólafur Gudmundsson, Crocker, S.D.: Observing dnssec validation in the wild. In: Securing and Trusting Internet Names (SATIN). (2011)
15. Fujiwara, K.: Dnssec validation measurement. DNS-OARC Workshop, San Francisco, CA, USA (March 2011)
16. Fujiwara, K.: Number of possible dnssec validators seen at jp. IEPG Meeting @ IETF 83, Paris, France (March 2012)
17. Yu, Y., Wessels, D.: Quantifying dnssec validators. DNS-OARC Workshop, Toronto, Canada (October 2012)
18. SIDN: Dnssec test. http://dnssectest.sidn.nl (accessed August 2012).