DNS SECURITY TROUBLESHOOTING GUIDE

INTERNET DEPLOYMENT OF DNS SECURITY

27 November 2006

Table of Contents

1. Introduction

When the Domain Name System (DNS) is working properly, everything on the Internet simply works. Names are resolved, web sites are viewed, and email flows. When the DNS breaks, almost everything on the Internet grinds to a halt. In general, the DNS is largely a robust, resilient, and invisible service to users; however, to the operators that run the network this critical infrastructure service can be viewed as either a service enabler or a major problem depending on the operating status of DNS.

Like most infrastructure services security was not initially built into the service, rather it was added on. Furthermore, when DNS security breaches occur the damaged parties may not even know that they have been compromised until after the fact. Therefore, securing DNS requires preventive measures such as those found in the DNS Security Extensions (DNSSEC).

DNSSEC adds some “moving pieces” to the DNS that can break. This guide aims to explain the various ways that DNS Security can break and how to determine what has broken when a signed zone is not working properly.

It is expected that the reader already possesses working knowledge of DNS and can capably troubleshoot a broken DNS system at some level. References are listed at the end for more basic troubleshooting of the DNS without DNSSEC. This guide also assumes that the reader is familiar with DNS Security and how to deploy it.

2. DNS Security Specific Failure Modes

There are a number of DNS Security (DNSSEC) specific ways that the DNS can break. This section lists some of the most common problems.

2.1 Signatures

DNSSEC adds public key signatures to the DNS. These signatures have a lifetime value and will expire after a certain amount of time. Unlike in plain DNS where data can potentially live forever, in secured DNS these signatures will expire.

2.1.1 Signature Expiration

When a DNS zone is signed, the zone administrator specifies a time in the future that the generated signatures will expire; this is known as the signature expiration time. If the zone administrator does not resign the zone, which refreshes the signatures, before the signature expiration time, the signatures are considered invalid and resolvers will not use them to validate the zone data.

2.2 Trust Anchors

On the resolving-side of DNS, DNSSEC adds the notion of trust anchors. Trust anchors are the public keys that are configured into DNS resolvers to validate the signatures of received DNS zone data. Zones may potentially have multiple keys published as part of the zone data. The zone administrator will designate specific keys that resolver administrators should configure as trust anchors. These public keys are called the Secure Entry Point (SEP) Keys. These trust anchors can be changed in a number of ways in the zone that they represent.

2.2.1 Secure Entry Point Key Rollover

During the normal course of operating a signed zone, a zone administrator will perform key rollovers on the keys within the zone. For the SEP keys that are configured as trust anchors, these rollovers will necessitate a corresponding action at each of the resolvers that have configured the trust anchors. If the resolvers are not updated, the old trust anchors will no longer be capable of validating the signatures generated by the new SEP keys.

2.2.2 Secure Entry Point Deletion

If a zone administrator deletes the SEP keys that are configured as trust anchors in resolvers, then a similar situation as the rollover situation will occur. Only instead of the resolvers being unable to validate the signatures, there will be no signatures to validate and so the resolver will consider the zone as invalid.

2.2.3 Resolver Misconfiguration

On the resolving side of DNS, the resolver itself can be misconfigured by the resolver administrator. If the administrator makes a typographical error while entering the trust anchor, or does not fully enable DNSSEC support in the resolver, then the resolver will not work properly. In the first case, the zone will be considered invalid, in the second case the zone will simply appear to be unsigned.

2.3 Malicious Modification

A third possible way for DNSSEC to malfunction is in the face of malicious attack. An attacker can modify DNS responses while in transit on the network and if the attacker does not possess the private key that created the signatures on the response data, the signatures will be invalid due to the data modification. If the attacker does possess the private key, then there are bigger security issues with the zone than can be solved with troubleshooting.

3. Troubleshooting Tools

3.1 BIND Server Logs [URL_BIND]

Probably the most obvious “tool” to use is BIND itself and the logs that it generates when performing DNS operations. For DNSSEC, the relevant portions of a logging configuration are:

```
channel dnssec {
  file "/var/log/dnssec" versions 10 size 300k;
  print-time yes;
  print-category no;
  print-severity yes;
  severity debug 3;
  //severity info;
};
category dnssec { dnssec; };
```

For the most verbose logging, `severity level debug 3` is recommended. For production servers level 3 information is too voluminous; therefore, `severity level info` is recommended. Examples of each type of level will be provided.

3.2 dig – DNS Lookup Utility [URL_BIND]

The BIND dig utility is a command-line program that sends DNS query requests to servers. The dig command is DNSSEC aware and can be used to query both authoritative and recursive servers. A typical dig command for DNSSEC troubleshooting looks like:

```
% dig badsign-A.test.dnssec-tools.org +dnssec
```

This command sends a query to the first server listed in the `/etc/resolv.conf` file. If dig does not get an answer from that server, it will query the other servers listed. The query sent will indicate support for DNSSEC, so the reply given should provide any DNSSEC-relevant information. The `+dnssec` flag can not be specified, in which case the query will not indicate DNSSEC support.. What is important to remember, however, is that even if the `+dnssec` flag is not specified, the server will attempt to perform validation if it can.

One configuration option that is especially useful for dig is the `+multiline` option. This option formats the output to be more readable and less compact. It can be added to a

`.digrc` file in the administrator's home directory so that it will always be applied. All dig output examples in this document will be shown in the `+multiline` format.

3.3 donuts – DNS Lint Application [URL_DNST]

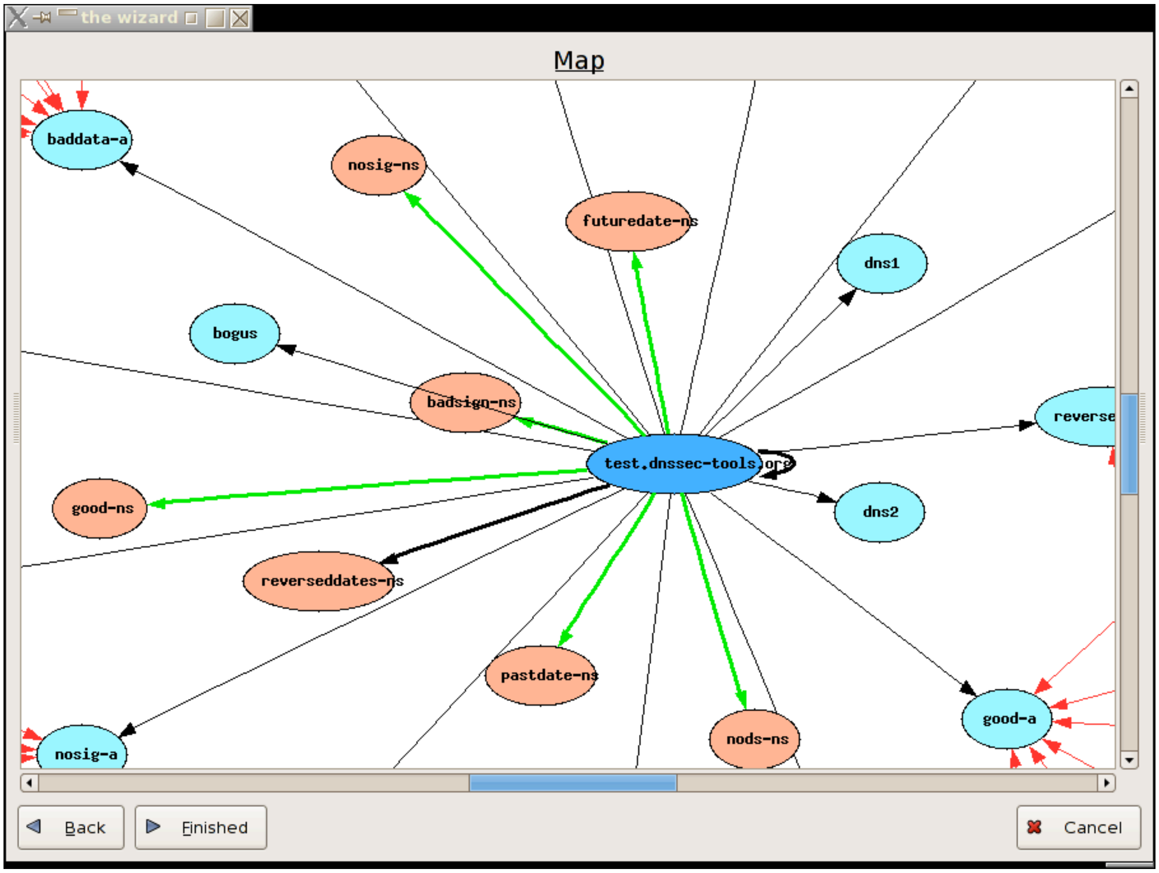
DoNutS is a DNS Lint application that examines DNS zone files looking for particular problems. It is specifically designed for DNSSEC and most of the checks are related to DNSSEC problems. It is run by the zone administrator on a local zone file. DoNutS produces output like the following:

```
# donuts --level 8 -v example.com.signed example.com

--- loading rule file /usr/share/donuts/rules/dnssec.rules.txt
    rules: DNSSEC_RRSIG_TTL_MATCH_ORGTTL DNSSEC_MEMORIZE_NS_RECORDS
DNSSEC_MISSING_NSEC_RECORD DNSSEC_MISSING_RRSIG_RECORD
DNSSEC_RRSIG_NOT_SIGNING_RRSIG DNSSEC_RRSIG_FOR_NS_GLUE_RECORD
DNSSEC_NSEC_FOR_NS_GLUE_RECORD DNSSEC_RRSIG_SIGEXP DNSSEC_NSEC_TTL
DNSSEC_DNSKEY_MUST_HAVE_SAME_NAME DNSSEC_DNSKEY_PROTOCOL_MUST_BE_3
DNSSEC_BOGUS_NS_MEMORIZE DNSSEC_MISSING_RRSIG_RECORD
DNSSEC_RRSIG_TTL_MUST_MATCH_RECORD DNSSEC_MISSING_NSEC_RECORD
DNSSEC_RRSIG_SIGNER_NAME_MATCHES DNSSEC_NSEC_RRSEC_MUST_NOT_BE_ALONE
DNSSEC_RRSIGS_MUST_NOT_BE_SIGNED DNSSEC_MEMORIZE_KEYS DNSSEC_RRSIGS_VERIFY
--- loading rule file /usr/share/donuts/rules/parent_child.rules.txt
    rules: DNS_MULTIPLE_NS DNSSEC_SUB_NOT_SECURE
DNSSEC_DNSKEY_PARENT_HAS_VALID_DS DNSSEC_DS_CHILD_HAS_MATCHING_DNSKEY
--- loading rule file /usr/share/donuts/rules/parent_child_temp.txt
    rules: DNSSEC_SUB_NS_MISMATCH
--- loading rule file /usr/share/donuts/rules/recommendations.rules.txt
    rules: DNS_REASONABLE_TTLS DNS_SOA_REQUIRED DNS_NO_DOMAIN_MX_RECORDS
--- Analyzing individual records in example.com.signed
--- Analyzing records for each name in example.com.signed
example.com:
  Rule Name:   DNS_NO_DOMAIN_MX_RECORDS
  Level:       8
  Warning:     At least one MX record for example.com is suggested

sub2.example.com:
  Rule Name:   DNSSEC_SUB_NOT_SECURE
  Level:       3
  Error:       sub-domain sub2.example.com is not securely delegated.  It is
missing a DS record.

results on testing example.com.signed:
  rules considered: 28
  rules tested:           25
  records analyzed: 52
  names analyzed:   8
  errors found:           2
```

From this output, the most interesting error is that the zone checked has a delegation that is not secured.

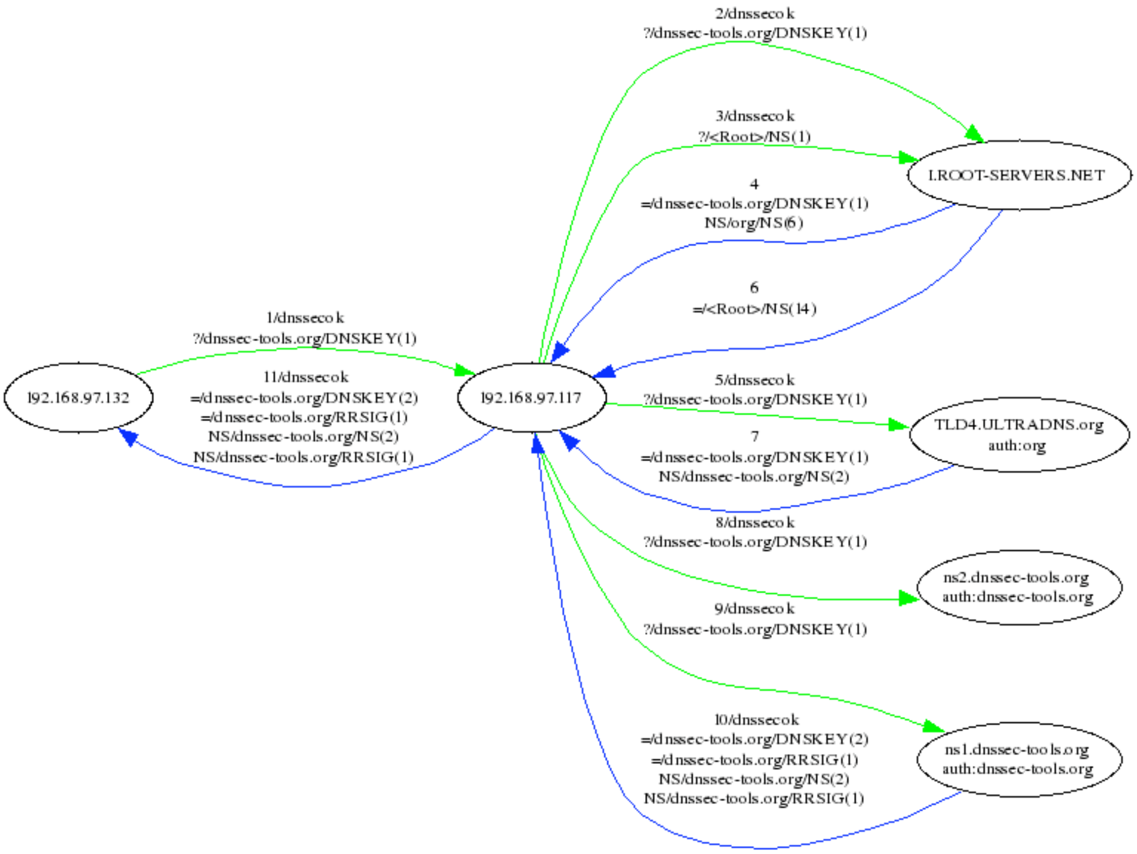
3.4 mapper – DNS Graphical Mapper [URL_DNST]

The mapper application creates a graphical map of one or more zone files. The output gives a graphical representation of a DNS zone or zones. The result can be useful for getting a more intuitive view of a zone or set of zones. It is extremely useful for visualizing DNSSEC deployment within a given zone as well as to help discover problem spots. Large organizations might also find mapper useful in visualizing a DNS deployment. A small portion of the map for the zone test.dnssec-tools.org is depicted below:



3.5 dnspktflow – Analyze DNS Flows [URL_DNST]

The dnspktflow application analyzes and draws DNS flow diagrams from packet capture files made with tcpdump, or any other libpcap-generating program. This tool is very useful for debugging dns queries being issued to and by resolvers. An example flow is:


2/dnssecok
?/dnssec-tools.org/DNSKEY(1)
3/dnssecok
?/<Root>/NS(1)
I.ROOT-SERVERS.NET
4
=/dnssec-tools.org/DNSKEY(1)
NS/org/NS(6)
6
=/<Root>/NS(14)
1/dnssecok
?/dnssec-tools.org/DNSKEY(1)
192.168.97.132
11/dnssecok
=/dnssec-tools.org/DNSKEY(2)
=/dnssec-tools.org/RRSIG(1)
NS/dnssec-tools.org/NS(2)
NS/dnssec-tools.org/RRSIG(1)
192.168.97.117
5/dnssecok
?/dnssec-tools.org/DNSKEY(1)
TLD4.ULTRADNS.org
auth:org
7
=/dnssec-tools.org/DNSKEY(1)
NS/dnssec-tools.org/NS(2)
8/dnssecok
?/dnssec-tools.org/DNSKEY(1)
ns2.dnssec-tools.org
auth:dnssec-tools.org
9/dnssecok
?/dnssec-tools.org/DNSKEY(1)
10/dnssecok
=/dnssec-tools.org/DNSKEY(2)
=/dnssec-tools.org/RRSIG(1)
NS/dnssec-tools.org/NS(2)
NS/dnssec-tools.org/RRSIG(1)
ns1.dnssec-tools.org
auth:dnssec-tools.org

3.6 validate – DNS Validation [URL_DNST]

The validate application is a command-line standalone DNS validation utility along the lines of dig. Some example output is given below.

```
% ./validate -o 6:stdout -p badsign-A.test.dnssec-tools.org
Result: ****START****
Result:         FAILED: Some results were not validated successfully
Original query: name=badsign-A.test.dnssec-tools.org class=IN type=A from-
server=157.185.80.32, Query-status=Q_ANSWERED:4
  Result: VAL_BOGUS:130
    name=badsign-A.test.dnssec-tools.org class=IN type=A from-
server=157.185.80.32 status=VAL_AC_NOT_VERIFIED:51
    name=test.dnssec-tools.org class=IN type=DNSKEY[tag=28827] from-
server=157.185.80.32 status=VAL_AC_TRUST_KEY:88
Result: ****END****

DNSSEC status: VAL_BOGUS [130]
Non-validated response:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 0
;; flags:; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0
;;      badsign-A.test.dnssec-tools.org, type = A, class = IN
badsign-A.test.dnssec-tools.org.  1D IN A  168.150.236.43
```

4. Troubleshooting DNS Security

To effectively troubleshoot DNSSEC, an administrator will need to make use of a combination of the tools mentioned above. What follows is an example session to introduce some of the tools and how a typical troubleshooting session might go.

4.1 Example Session

It should be noted that this example session was run on Friday, November 10, 2006. As such, the example output will show valid signature expiration times for that date. The example names were chosen, however, such that if the session was recreated at a later date, the valid names would still be valid and the invalid names would still be invalid.

When DNSSEC breaks, the application will indicate that the name being requested could not be found. A resolver administrator using dig to query the recursive server would see output like the following:

```
% dig badsign-A.test.dnssec-tools.org

; <<>> DiG 9.3.2 <<>> badsign-A.test.dnssec-tools.org
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 46037
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;badsign-A.test.dnssec-tools.org. IN A

;; Query time: 712 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Fri Nov 10 10:45:13 2006
;; MSG SIZE  rcvd: 49
```

The important piece of information in the output is the `status` code, which in this example is `SERVFAIL`. When DNSSEC problems are encountered, the status code will always be `SERVFAIL`. This makes troubleshooting somewhat difficult, as it is not clear why the server failed to get an answer.

The relevant log entries in the dnssec log for this query are shown below. The things to notice about these log entries are that all of them are at `level debug 3` except for two, both of which state ‘no valid signature found’ for the name under validation.

```
10-Nov-2006 10:45:12.979 debug 3: validating @0x8249000: badsign-A.test.dnssec-
tools.org A: starting

10-Nov-2006 10:45:12.979 debug 3: validating @0x8249000: badsign-A.test.dnssec-
tools.org A: attempting positive response validation

10-Nov-2006 10:45:12.980 debug 3: validating @0x8249000: badsign-A.test.dnssec-
tools.org A: keyset with trust 7
```

```
10-Nov-2006 10:45:12.986 debug 3: validating @0x8249000: badsign-A.test.dnssec-
tools.org A: verify rdataset: RRSIG failed to verify

10-Nov-2006 10:45:12.987 debug 3: validating @0x8249000: badsign-A.test.dnssec-
tools.org A: failed to verify rdataset

10-Nov-2006 10:45:12.987 debug 3: validating @0x8249000: badsign-A.test.dnssec-
tools.org A: verify failure: RRSIG failed to verify

10-Nov-2006 10:45:12.988 info: validating @0x8249000: badsign-A.test.dnssec-
tools.org A: no valid signature found

10-Nov-2006 10:45:12.988 debug 3: validator @0x8249000: dns_validator_destroy

10-Nov-2006 10:45:13.178 debug 3: validating @0x827d800: badsign-A.test.dnssec-
tools.org A: starting

10-Nov-2006 10:45:13.179 debug 3: validating @0x827d800: badsign-A.test.dnssec-
tools.org A: attempting positive response validation

10-Nov-2006 10:45:13.179 debug 3: validating @0x827d800: badsign-A.test.dnssec-
tools.org A: keyset with trust 7

10-Nov-2006 10:45:13.185 debug 3: validating @0x827d800: badsign-A.test.dnssec-
tools.org A: verify rdataset: RRSIG failed to verify

10-Nov-2006 10:45:13.186 debug 3: validating @0x827d800: badsign-A.test.dnssec-
tools.org A: failed to verify rdataset

10-Nov-2006 10:45:13.186 debug 3: validating @0x827d800: badsign-A.test.dnssec-
tools.org A: verify failure: RRSIG failed to verify

10-Nov-2006 10:45:13.187 info: validating @0x827d800: badsign-A.test.dnssec-
tools.org A: no valid signature found

10-Nov-2006 10:45:13.187 debug 3: validator @0x827d800: dns_validator_destroy
```

At this point the administrator knows that the recursive server cannot validate the name being asked for because it cannot find a valid signature. It would be useful to know what the authoritative server for test.dnssec-tools.org is serving. To start, the administrator will find the name servers for the zone:

```
% dig test.dnssec-tools.org ns

; <<>> DiG 9.3.2 <<>> test.dnssec-tools.org ns
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 54654
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;test.dnssec-tools.org. IN NS

;; ANSWER SECTION:
test.dnssec-tools.org.  84486 IN NS dns2.test.dnssec-tools.org.
test.dnssec-tools.org.  84486 IN NS dns1.test.dnssec-tools.org.

;; Query time: 10 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Fri Nov 10 11:16:37 2006
;; MSG SIZE  rcvd: 77
```

Once an authoritative name server is found, it will be queried directly for the data:

```
% dig @dns2.test.dnssec-tools.org badsign-A.test.dnssec-tools.org

; <<>> DiG 9.3.2 <<>> @dns2.test.dnssec-tools.org badsign-A.test.dnssec-
tools.org
; (1 server found)
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 22606
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 2

;; QUESTION SECTION:
;badsign-A.test.dnssec-tools.org. IN A

;; ANSWER SECTION:
badsign-A.test.dnssec-tools.org. 86400 IN A 168.150.236.43

;; AUTHORITY SECTION:
test.dnssec-tools.org.  86400 IN NS dns1.test.dnssec-tools.org.
test.dnssec-tools.org.  86400 IN NS dns2.test.dnssec-tools.org.

;; ADDITIONAL SECTION:
dns1.test.dnssec-tools.org. 86400 IN A 168.150.236.43
dns2.test.dnssec-tools.org. 86400 IN A 63.195.146.66

;; Query time: 92 msec
;; SERVER: 63.195.146.66#53(63.195.146.66)
;; WHEN: Fri Nov 10 11:17:34 2006
;; MSG SIZE  rcvd: 135
```

The previous command was used to illustrate how the `+dnssec` flag affects queries and responses. The administrator here is looking for DNSSEC-relevant data, but because it wasn’t explicitly asked for in the previous query the server did not return it. So the administrator resends the query with the `+dnssec` flag set:

```
% dig @dns2.test.dnssec-tools.org badsign-A.test.dnssec-tools.org +dnssec

; <<>> DiG 9.3.2 <<>> @dns2.test.dnssec-tools.org badsign-A.test.dnssec-
tools.org +dnssec
; (1 server found)
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 53334
;; flags: qr aa rd; QUERY: 1, ANSWER: 2, AUTHORITY: 3, ADDITIONAL: 5

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;badsign-A.test.dnssec-tools.org. IN A

;; ANSWER SECTION:
badsign-A.test.dnssec-tools.org. 86400 IN A 168.150.236.43
badsign-A.test.dnssec-tools.org. 86400 IN RRSIG A 5 4 86400 20061126155159
(20061027155159 51767 test.dnssec-tools.org.
cZndYlk2EdIhFfOhTCLkcaCMVlcEicX0wuDfnlnv7GBNO58JHQ3KgqaFwBHOI9JVBFUBKL6bqVJf0GC
8wyctP8MyqUe/czOaxbQvs98yy1jgIVDELG95KcNa9QG9H0TK4kJViU9br9XXJdRUlz+oTRDToaZ3M/
WtVX5IEIlaquyfpW/oDouDKfBQzcFf7GYDmP8eSrthe6ia3drOsU6Hav6Neu7GumYfMlP8cdI5r7lcs
vJHLiugUnyEza8nquEYh0xNmxWGzcAYPWY4HuR3HSP3rNwLph0KNy/Yh9C4sp/4/YIMYmtc7mjyzVHR
oEBzsbwoxQ68096oFKKQunRqvQ== )

;; AUTHORITY SECTION:
test.dnssec-tools.org.  86400 IN NS dns2.test.dnssec-tools.org.
test.dnssec-tools.org.  86400 IN NS dns1.test.dnssec-tools.org.
test.dnssec-tools.org.  86400 IN RRSIG NS 5 3 86400 20061126155159
(20061027155159 51767 test.dnssec-tools.org.
g3KDL9VUyQmdaSlpX/SX4Co8jkQ3sKt3SNvsIxJQzCmfPi10V3L+4RzH2xl8hFzn1yRQtO7ZIY311TB
8X0h+E1+VUpL7VCbY32rbQWt5gDh5UG1GzqOh0rMkqjuDykomolPqjjheoEsSa8B/QIZCSpEeKJgZXb
LkbdBQWmPp8mXjAU5HDSmFDW/Z1bLBUvRdueeNtXXmMJrH/+rYb0le3LxdXJxaByquf02jZBu3a3DEm
xErkOdk7jC8dZk2F00+E5XYVwkBxJyZqYui18SITztuNPYzvMYG968Zj4viFSEJk6fvkT3eCbtGcrmy
ISWSmE2WUBiljxODt3nRCKJQ3A== )

;; ADDITIONAL SECTION:
dns1.test.dnssec-tools.org. 86400 IN A 168.150.236.43
dns2.test.dnssec-tools.org. 86400 IN A 63.195.146.66
dns1.test.dnssec-tools.org. 86400 IN RRSIG A 5 4 86400 20061126155159
(20061027155159 51767 test.dnssec-tools.org.
GWZm9GJ0XCsBoIVvnrbhcXxi573RkWCKlN+1xIsuDHMlK1F+Dbsfe2jlnqXEEBgFijFydCSx/BztzaO
jfBHV3HcTl6A3D+wNAnZkeCRExD2hZA19PmSgIVF6Lq8O2scV5ZRHr31oVUgEvPHBfNWgmioc8fQiYE
gkOxl/Gck2sPKz+F2ZmZaQaIh0/qbYaUL/Q3VN+HnKgdP4KCU4S4/cIo/Y2D5tRHen+RcUe6AKZ/bjw
xfu8tIVHU71eGvNXO79FjBCSgRDmGVWMTgRookoIap5sxG+150dP5+036bd0G/mUdb96QHbJS3htr8T
1ZoFhlDE1LWCiGMAUnoNCZXMlw== )
dns2.test.dnssec-tools.org. 86400 IN RRSIG A 5 4 86400 20061126155159
(20061027155159 51767 test.dnssec-tools.org.
gRtAJpqdDMiq6JzSaBAOgXy3eI4P9NCqfF9liK86gtSgyW6ydvxx+W1FAN92G+weWEj3pp1u+6sWxLO
xy36opIE9J0Rbrs69STEKgLDbpun7UG7+HcdQcY85IbIiBummCU/j+D4gApxIi+m7GLaVhteGEACmr5
1Z5Sxg9DSz77LxfVnTHKqpNYOxZBn9wMJyTrC1H4A0wQe+osjoJdOaN3BllDmTuKuak1VZmkbZw8LEh
pEE6RUvSll4GJqzoH2OaTXd0Oka963oDA3wEXXV7j8dKIcnbP1qaIUGLkBnIOEkYVyGkiN1I12ZhbE6
VG5GrPHX12RkbXS7FBflxFf2hQ== )

;; Query time: 142 msec
;; SERVER: 63.195.146.66#53(63.195.146.66)
;; WHEN: Fri Nov 10 11:19:32 2006
;; MSG SIZE  rcvd: 1382
```

There are a number of things to check in this output:

1. Is there a signature for the name?
2. Has the signature expired?
3. Is the signature from a key that is published in the zone?

Using the previous output, a zone administrator would provide the following answers to the questions:

1. Yes. The first `RRSIG` in the output covers an `A` record at `badsign-A.test.dnssec-tools.org.`
2. No. The signature expiration date is the first date listed in the `RRSIG` record. In this case it is `20061126155159` which is 26 Nov 2006 15:51:59.
3. To determine this, the key id field in the `RRSIG` record, which is the first field after the 2 date fields, is checked. The key id is a unique identifier for the keys published by the zone. In this case it is `51767`. To check this value, another query must be performed for the DNSKEYs published in the zone:

```
; <<>> DiG 9.3.2 <<>> @dns2.test.dnssec-tools.org test.dnssec-tools.org DNSKEY
; (1 server found)
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 1137
;; flags: qr aa rd; QUERY: 1, ANSWER: 3, AUTHORITY: 2, ADDITIONAL: 2

;; QUESTION SECTION:
;test.dnssec-tools.org. IN DNSKEY

;; ANSWER SECTION:
test.dnssec-tools.org.  86400 IN DNSKEY 256 3 5
(AQOxosf/UIhWBFufgkBYL4bx5d897k8wgMQvXNmkOU+L4uu1CB3wgHePnKCJscdDm9UXJyT0Z5Pdlq
rr+05SO614HWKXij5niHWMhBbZJaZSWAFBb1N8aMTtf+SZ6niocoajBcqU0UTMtAgxsdh3siaAPiLam
RFc4c/EuI3f8Z0iR0td54KPt+8u8hUkWoLRTbOOCXtSzCl+ZsUws5HyhyHjI16sodP5xtDqxzC0Xn+G
xWZWxUX/10kwb4Nu/jCHjRKDAh0UZ/aFskdUouVPRCoIlTD0QIDScPgtp3hFBimChAJbraHdBI58J/g
RWEVIDS5wP3ictR9n6xhLLmEUElwb) ; key id = 51767
test.dnssec-tools.org.  86400 IN DNSKEY 256 3 5
(AQPjJwI0ETCO7504DFIytx019KSZLlsXO2XeBloKihyMRz5WQjJKki7iYcYxKVrPZsdIljw+0HB+63
uuyJr1JlcJ7fwPbTXFoxpVaw22wyA6KEHitcywiuL1YU9JbTBE4iThk6dRRDm3idhIZBf7SkNbbpWbN
f0GtEtL+u15fHW/YHVYXdSkEnTAwkpnhu/VSeDITbCjXhzLSylUhpbZVcS7pGlG0Mhagu2jbFW9R1Cn
7NZ155cqNGXkvHQxeQDhUpy5DNf9HTH/6hFzjMXFey5A1x5A9otCy3RduR2poX+8CQ9m3Q0MxxqbWRu
EozR1eYRVS/ZHHOpdqJ8mZcT9zQiT) ; key id = 16442
test.dnssec-tools.org.  86400 IN DNSKEY 257 3 5
(AQPUlH65Otuo6toxYX2zHCwdojmAKFa9gobYWrNEojKQAWJuvGMd4okTnlOJTL0hBWKC4Uhf40ePpD
R8QJayeI/eZg29UZLMBleZ96a0mSo/JU4Sq3G06X9d5Z01EVCvTkJUHHEvvmzZhBsO+43NcWYrSUoXX
1JbXs9QKuO1BLPHuS5G/UfEsyVonfl39dGrEput1gDWxIvov2UENM2eX0LE5ZIyGiX2uDdN4SVIa0Rd
+F2pSCiddE1bYxIi2IlW6bpeim+mdC1BDJkEB70+ekeBR3as5D339z+9KeMyZgPs82SAQswbGdZvkWL
8mgSdbf6DiuTkkNIUzbS/6fxlQO/GOdq0NlTr28sW4Byj9gkpb2Clbqog72yJJ3s5CV4LGZ1jtpnoFc
sKwMlLnOj0X+L2iY7Spe5M9D59Jqxl9cAWjATsSXG5TvCUNBT2Eh6Jw7OimThJe4pUmFxGqhplPqs2d
lnDgfcuVNf9lwa36Re7pUt+FlT0A9FIWk4utfUgZO3eWnKrw1Fw8QF9wKm252iscULNzKwYvfK8NGSB
OfyYRvAw7ZnAoxMKFIOLq3W8IsFjti5dLhLYWpFEGZOT+eDc/lPhyaEsmsjHQnEEyj4TmomV8n91s3H
8IbrKu0cdIH1/k5iu+sLi9EIAprOnxrxO+tHDiEZUoimBRFtETCcmsQ==) ; key id = 28827

;; AUTHORITY SECTION:
test.dnssec-tools.org.  86400 IN NS dns2.test.dnssec-tools.org.
test.dnssec-tools.org.  86400 IN NS dns1.test.dnssec-tools.org.

;; ADDITIONAL SECTION:
dns1.test.dnssec-tools.org. 86400 IN A 168.150.236.43
dns2.test.dnssec-tools.org. 86400 IN A 63.195.146.66

;; Query time: 131 msec
;; SERVER: 63.195.146.66#53(63.195.146.66)
;; WHEN: Fri Nov 10 11:34:22 2006
;; MSG SIZE  rcvd: 1187
```

Looking at this output, the first `DNSKEY` record listed has a key id of `51767` which matches the key id in the `RRSIG` record. So the answer to the final question is yes, the signature is from a key that is published in the zone.

At this point the administrator now knows that that the authoritative server is serving what appears to be good and valid data but the recursive server is unable to validate that data. The server should be able to validate the data but it can’t. This could indicate that an attacker is targeting either the zone being queried and modifying answers from that zone, or the site where the recursive server is located and modifying all answers being returned to that site.

This entire example was chosen to illustrate a couple of things. First, even when everything looks like it should work, sometimes it won't. Second, there is likely no way to really know if what appears to be broken is due to a malicious attack or some other error.

In this case, it should be obvious that there is not attack actually occurring. Instead, the name being queried has a deliberately bad signature associated with it (`badsign-A.test.netsec.tislabs.com`).

4.2 Additional Examples

It is instructive to look at some additional examples briefly to see the output associated with various scenarios.

4.2.3 Expired Signature

Following is the response from the authoritative server for the name `pastdate-A.test.dnssec-tools.org`. The dig output shows a signature expiration time (highlighted) that is in the past. The ADDITIONAL section has been deleted here for brevity. When querying the recursive server, the response will still have a `status` code of `SERVFAIL`.

```
; <<>> DiG 9.3.2 <<>> @dns1.test.dnssec-tools.org pastdate-A.test.dnssec-
tools.org +dnssec
; (1 server found)
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 12871
;; flags: qr aa rd; QUERY: 1, ANSWER: 2, AUTHORITY: 3, ADDITIONAL: 5

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;pastdate-A.test.dnssec-tools.org. IN A

;; ANSWER SECTION:
pastdate-A.test.dnssec-tools.org. 86400 IN A 168.150.236.43
pastdate-A.test.dnssec-tools.org. 86400 IN RRSIG A 5 4 86400 20061027094727
(20060927095227 51767 test.dnssec-tools.org.
c7R6gkZNaSh05n1d5juelxMux5kGzOZyV6nmtO7mnYxG2O/SmDycq5SBKfp0L00PX3QWwHo3yTI9jE2
cLpnkRGNjhQLKzm/+uHEoMI95EuiU/unNduMdXbREj7XKi/khFqN4IGR8csjtWhHcf8jpY84n3MKLEE
4Q8LJX8qM/cvidFOpYA82tpWUg2yTVUtpyyOYtwwhjO7v+XXBw/U+zrL1MwNc651zCVI4zm+JFrgGyK
8xRoorAqRU+7eutmzp0+5MKIxtav3UBk5feGws3pMk7EPiuxH3c0bLs/rftWexYK2eXuT88/Ru2wXOP
w2/IIr/X4rCV3r7mPWqz+RM9mg== )

;; AUTHORITY SECTION:
test.dnssec-tools.org.  86400 IN NS dns1.test.dnssec-tools.org.
test.dnssec-tools.org.  86400 IN NS dns2.test.dnssec-tools.org.
test.dnssec-tools.org.  86400 IN RRSIG NS 5 3 86400 20061126155159
(20061027155159 51767 test.dnssec-tools.org.
g3KDL9VUyQmdaSlpX/SX4Co8jkQ3sKt3SNvsIxJQzCmfPi10V3L+4RzH2xl8hFzn1yRQtO7ZIY311TB
8X0h+E1+VUpL7VCbY32rbQWt5gDh5UG1GzqOh0rMkqjuDykomolPqjjheoEsSa8B/QIZCSpEeKJgZXb
LkbdBQWmPp8mXjAU5HDSmFDW/Z1bLBUvRdueeNtXXmMJrH/+rYb0le3LxdXJxaByquf02jZBu3a3DEm
xErkOdk7jC8dZk2F00+E5XYVwkBxJyZqYui18SITztuNPYzvMYG968Zj4viFSEJk6fvkT3eCbtGcrmy
ISWSmE2WUBiljxODt3nRCKJQ3A== )

;; Query time: 265 msec
;; SERVER: 168.150.236.43#53(168.150.236.43)
;; WHEN: Fri Nov 10 13:13:51 2006
;; MSG SIZE  rcvd: 1383
```

4.2.4 No Signature

The following is the response from the authoritative server for the name `nosig-A.test.dnssec-tools.org`. The dig output shows an answer containing no associated signature. The ADDITIONAL section has been deleted here for brevity. When querying the recursive server, the response will still have a `status` code of `SERVFAIL`.

```
% dig @dns1.test.dnssec-tools.org nosig-A.test.dnssec-tools.org +dnssec

; <<>> DiG 9.3.2 <<>> @dns1.test.dnssec-tools.org nosig-A.test.dnssec-tools.org
+dnssec
; (1 server found)
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 38768
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 3, ADDITIONAL: 5

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;nosig-A.test.dnssec-tools.org. IN A

;; ANSWER SECTION:
nosig-A.test.dnssec-tools.org. 86400 IN A 168.150.236.43

;; AUTHORITY SECTION:
test.dnssec-tools.org.  86400 IN NS dns2.test.dnssec-tools.org.
test.dnssec-tools.org.  86400 IN NS dns1.test.dnssec-tools.org.
test.dnssec-tools.org.  86400 IN RRSIG NS 5 3 86400 20061126155159
(20061027155159 51767 test.dnssec-tools.org.
g3KDL9VUyQmdaSlpX/SX4Co8jkQ3sKt3SNvsIxJQzCmfPi10V3L+4RzH2xl8hFzn1yRQtO7ZIY311TB
8X0h+E1+VUpL7VCbY32rbQWt5gDh5UG1GzqOh0rMkqjuDykomolPqjjheoEsSa8B/QIZCSpEeKJgZXb
LkbdBQWmPp8mXjAU5HDSmFDW/Z1bLBUvRdueeNtXXmMJrH/+rYb0le3LxdXJxaByquf02jZBu3a3DEm
xErkOdk7jC8dZk2F00+E5XYVwkBxJyZqYui18SITztuNPYzvMYG968Zj4viFSEJk6fvkT3eCbtGcrmy
ISWSmE2WUBiljxODt3nRCKJQ3A== )

;; Query time: 185 msec
;; SERVER: 168.150.236.43#53(168.150.236.43)
;; WHEN: Fri Nov 10 13:21:28 2006
;; MSG SIZE  rcvd: 1071
```

4.3 Server Misconfiguration

Incorrect server configuration includes a number of possibilities ranging from having the authoritative server load the wrong zone data to mistyping the trust anchor data in the recursive server. In most of these cases, the server will refuse to load in some manner. In these situations consulting the error output from the server will reveal what needs to be fixed. The donuts utility can also perform a number of checks on a zone and flag any possible inconsistencies that might be considered okay by the server. If the authoritative server is configured to load the unsigned zone instead of the signed zone then the server will load the data without error. Using the dig and donuts utilities should quickly reveal that the zone data being served is not signed.

References

Books

[BK_ALBI] Albitz, Paul and Liu, Cricket, “DNS and BIND, Fourth Edition”, O’Reilly, April 2001.

[BK_LIU] Liu, Cricket, “DNS and BIND Cookbook”, O’Rielly, October 2002.

Contract Reports

[CDRL_A004] “DNS Security Deployment Plan: Domain Name System Security Roadmap, Software Pieces”, Technical Information Report, Contract FA8750-04-C-0229, Internet Deployment of DNS Security, March 2005.

[CDRL_A005] “DNS Security System Specification”, Technical Information Report, Contract FA8750-04-C-0229, Internet Deployment of DNS Security, August 2005.

[CDRL_A006] “Step-by-step DNS Security Operator Guidance Document”, Software User Manual (SUM): Training, Procedural, and Development Documentation, Contract FA8750-04-C-0229, Internet Deployment of DNS Security, August 2005.

[CDRL_A009] “Extended DISA/USMC DNSSEC Experiment Report”, Technical Report, Contract FA8750-04-C-0229, Internet Deployment of DNS Security, August 2005.

Internet Drafts

[ID_KRISH] Krishnaswamy, S., “Split-View DNSSEC Operational Practices”, draft-krishnaswamy-dnsop-dnssec-split-view-00 (work in progress), February 2005.

[ID_KOLK] Kolkman, O., Geiben, R., “DNSSEC Operational Practices”, draft-ietf-dnsop-dnssec-operational-practices-04 (work in progress), March 2005.

[ID_WEIL1] Weiler, S., “Clarifications and Implementation Notes for DNSSECbis”, draft-ietf-dnsext-dnssec-bis-updates-01 (work in progress), May 2005.

[ID_WEIL2] Weiler, S., Ihren, J., “Minimally Covering NSEC Records and

DNSSEC On-Line Signing", draft-ietf-dnsext-dnssec-online-signing-00 (work in progress), May 2005.

[ID_WONG] Wong, M., Schlitt, W., "Sender Policy Framework (SPF) for Authorizing Use of Domains in E-MAIL, version 1", draft-schlitt-spf-classic-02 (work in progress), June 2005.

RFCs

[RFC_2536] Eastlake, D., "DSA KEYs and SIGs in the Domain Name System (DNS)", RFC 2536, March 1999.

[RFC_2537] Eastlake, D., "RSA/MD5 KEYs and SIGs in the Domain Name System (DNS)", RFC 2537, March 1999.

[RFC_2821] Klensin, J., Editor, "Simple Mail Transfer Protocol", RFC 2821, April 2001.

[RFC_3110] Eastlake, D, "RSA/SHA-1 SIGs and RSA KEYs in the Domain Name System (DNS)", May 2001.

[RFC_3493] Gilligan, R., Thomson, S., Bound, J., McCann, J., Stevens, W., "Basic Socket Interface Extensions for IPv6", RFC 3493, February 2003.

[RFC_3833] Atkins, D., Austein, R., "Threat Analysis of the Domain Name System", RFC 3833, March 2005.

[RFC_4033] Arends, R., Austein, R., Larson, M., Massey, D., and Rose, S., "DNS Security Introduction and Requirements", RFC 4033, March 2005.

[RFC_4034] Arends, R., Austein, R., Larson, M., Massey, D., and Rose, S., "Resource Records for the DNS Security Extensions", RFC 4034, March 2005.

[RFC_4035] Arends, R., Austein, R., Larson, M., Massey, D., and Rose, S.,, "Protocol Modifications for the DNS Security Extensions", RFC 4035, March 2005.

URLs

[URL_BIND] http://www.isc.org/

[URL_DNSS] http://www.dnssec.net

[URL_DNST] http://www.dnssec-tools.org

[URL_GVIZ] http://www.graphviz.org/

[URL_LOGW] http://www2.logwatch.org:81/

[URL_LSPF2] http://www.libspf2.org

[URL_MILT] http://www.milter.org/milter_api/

[URL_MOZL] http://www.mozilla.org/products/mozilla1.x

[URL_OSSL] http://www.openssl.org

[URL_PFIX] http://www.postfix.org

[URL_PSPF] http://www.ipnet6.org/postfix/spf

[URL_SEND] http://www.sendmail.org

[URL_SPF] http://spf.pobox.com

[URL_SPFM] http://www.acme.com/software/spfmilter/

[URL_SRFG] http://sourceforge.net/projects/dnssec-tools

[URL_SRVY] http://www.tty1.net/smtp-survey/index_en.html

[URL_TBRD] http://www.mozilla.org/products/thunderbird