Global Information Assurance Certification Paper

DNSSec and BIND9 by Vivian Burns

When the Internet Software Consortium (ISC) released BIND9 in September 2000, at the top of the list of touted features was fully implemented DNSSec[1]. But what is DNSSec? What good is it? Do I need it? What do I need to know about it? This report intends to answer these questions by providing a description of DNSSec, its function, and some pertinent history, including the current state of development. This report is not intended to be an in-depth treatment of the subject; instead it is an overview of the most important ideas, events and people associated with DNSSec. This report assumes a basic understanding of DNS and encryption.

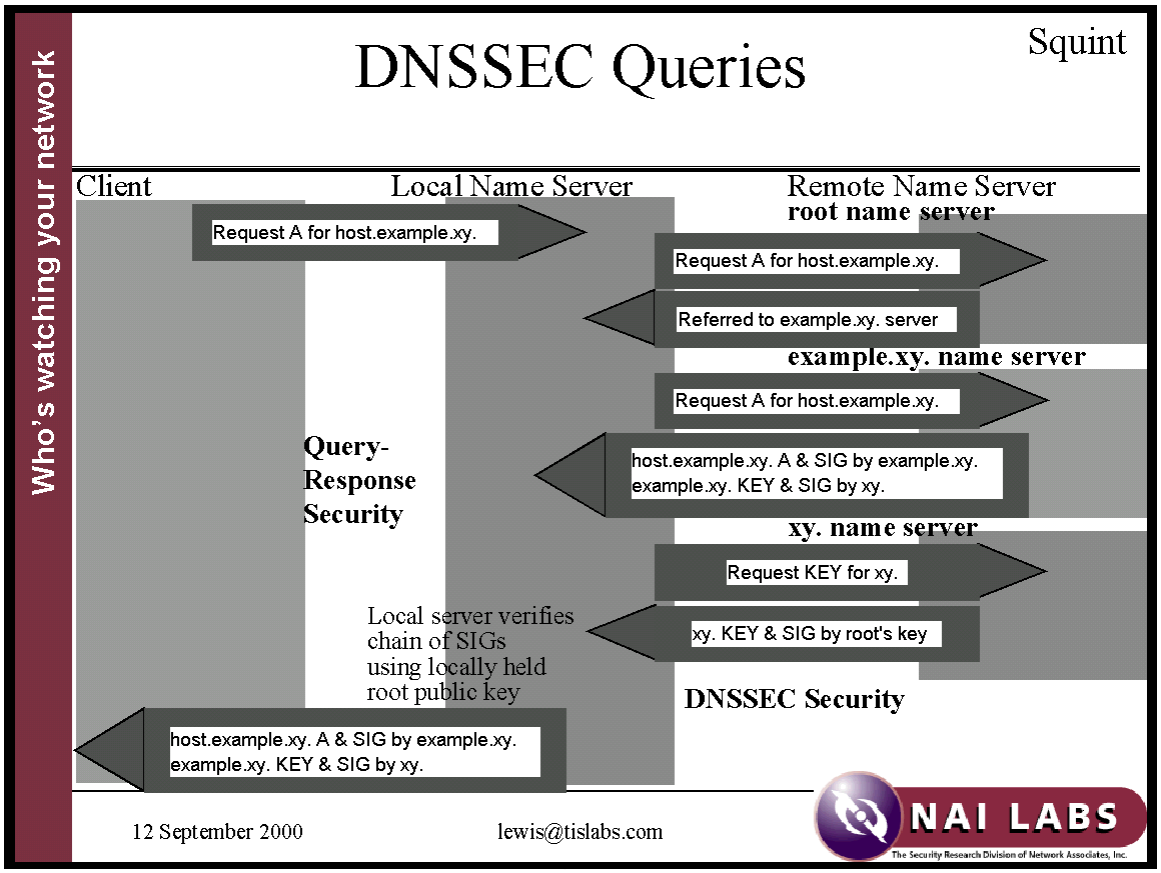
First of all, DNSSec is DNS Security Extensions. It's not a new protocol or application, but instead a set of extensions to the original DNS standard[2]. The DNS standard, which is described in RFC's 1034 and 1035, contained no provision for authenticating the source of a DNS response. Therefore, it allows attackers to redirect traffic to a hostile host by sending fake DNS responses. DNSSec remedies this security problem. It provides DNS data integrity and authentication through the use of cryptographic digital signatures. Once the DNS structure has been converted to this standard, DNS spoofing will be more difficult.

So what's behind these latest announcements? Let's take a brief look at the history of DNSSec. The standard was officially proposed to the Internet world with the arrival in January of 1997 of RFC 2065, "Domain Name System Security Extensions". RFC 2065 outlined three new resource records (RR's) for the DNS system: SIG for cryptographic signatures, KEY for zone public keys, and NXT, for the name of the next host.

DNSSec works like this. A secure DNS zone generates a signature for each set of resource records in its database. The signature is generated off-line so that the private key for the generation can stay secure. Then the signatures are added to the DNS database in the form of SIG records. Each time a secure DNS server sends a set of RR's, it sends the relevant signature with it.

The KEY RR contains a public key for decryption. The key is signed by a SIG RR from its parent zone. Of course the parent zone SIG must be validated using a public key, which has been signed by the parent's parent. And so on, until a zone is reached possessing a trusted key. The standard therefore requires the local host to be configured with a known trusted key that can be used to validate the rest of the chain.

The NXT RR permits authenticated denial of the existence of a name. It reinforces the integrity of this information by providing the name of the next host listed in the DNS database. This implies a standard ordering of DNS entries, which is also described in the RFC[3].



used by permission

Let's look at an example. When a client makes a request to the local name server, its first step is the same as usual. It makes a request to a server that it believes will know the answer, starting with root. Root refers our local name server to the name server authoritative for the domain requested. Then we make our request to the authoritative domain.

The next step is what's different. When the responding name server sends back the A record, it also sends a SIG record. The SIG record contains a previously generated cryptographic digital signature for the set of RR's. The responding server also sends a KEY record, accompanied by another SIG record. The KEY record contains the zone's public key so that the signature can be verified. The key has been signed by the parent -- in this case, "xy".

In order to verify the signature on the public key from the authoritative domain, the local name server requests the public key from the parent domain. The parent key is signed by the root. At that point, we make use of a trusted copy of the root key on the local server to complete the chain of authentication. The local machine must have a trusted key in the configuration for this reason[4].

Having reviewed the basics of RFC 2065, let's go back to DNSSec history. To become a draft standard, a proposed standard must have demonstrated proof that it works. With DNSSec, there have been difficulties. One of the difficulties was that the effort was taking place in the midst of other major standards changes for DNS as a whole. Dynamic DNS and IPv.6 were the most important of these[5]. At the same time, "The basic sleazeware produced in a drunken fury by a bunch of U C Berkeley grad students was still at the core of BIND," according to Paul Vixie, BIND9 architect. This rickety software structure was not judged an adequate basis for the complex changes needed by DDNS and DNSSec, so a decision was made to completely rewrite bind. "In 1998, Jerry Scharf, who was the Executive Director of ISC, convinced the remaining UNIX vendors and a few government agencies that the only way to support all of the new DNS protocol enhancements was to totally rewrite BIND."[6] As a result, in August of 1998 DARPA awarded a contract to TIS (NAI labs) to write the software in collaboration with ISC. [7]

In March of 1999, ISC released BIND 8.2, which contained a partial implementation of DNSSec[8]. That May, a NIC-SE workshop convened "to set up DNSSec with use of BIND 8.2 and see how it works. During the workshop the contributors [tried] to implement DNSSec and simulate signing, key exchange and key verification, in order to identify what weaknesses can be addressed during the contacts between the different parts involved in the process."[9] They did find a number of weaknesses in this implementation, and raised a large number of questions about operation. More on that in a moment.

In the meantime, work on the standard itself forged ahead, resulting in RFC 2535, which obsoleted the original proposed standard. As of this writing, RFC 2535 and its updates are still the proposed DNSSec standard[10]. The DNSSec working group also produced standards-track specifications for the encryption algorithms used (RFC 2536, 2537, 2539) and for a new CERT RR (RFC 2538), which would enable DNSSec to be used for certificate storage. Then DNS security tasks and issues were merged into the DNSEXT (DNS Extensions) working group, which has a broader charter than the original DNSSec working group did, including all types of DNS extensions[11].

Some of the significant updates to the specification were: DSA became a mandatory algorithm; RSA/MD5 became optional; ECC and Diffie-Hellman were added; the specification for ordering of records was fleshed out; and operational considerations were moved into a separate, informational RFC (2541)[12].

In September of 1999, the Collaborative Advanced Internet Research Network (CAIRN), got involved. CAIRN is an internetwork testbed funded by DARPA.[13] They organized a workshop attended by all the main players in DNSSec. During the workshop, CAIRN set up a DNSSec testbed, announcing that they would "provide top level key signing services for any secure subdomain whose natural parent was not doing so," " to allow organizations to immediately begin using DNSSEC."[14] Any interested organization had only to set up a secure domain, generate their keys and provide them to CAIRN. As of this writing, participants include UCLA, UCB, UCSC, SRI, 3Com and others[15].

Coming into the year 2000, the following had not been adequately addressed by the DNSSec standard, according to the participants at the CAIRN workshop[16]:

--Compatibility with older issues of BIND, which do not handle the new resource records.

--The necessity for a standard, secure key distribution mechanism and for parent-child key signing exchanges. Work is still in progress on this issue[17].

--A less computationally expensive method than public key cryptography was needed for the "last leg" between the client and the local name server, and for zone transfers. The proposed TSIG standard, therefore, provides transaction level authentication. The RFC, 2845, came out in May 2000. TSIG is an additional RR type which must not be cached. The standard specifies the use of shared secrets and one way hashing to accomplish authentication. It provides no distribution mechanism for the shared secrets, but suggests "some out of band mechanism such as sneaker-net."[18] To remedy this problem, a TKEY RR was proposed in RFC 2930, which came out in September 2000.The TKEY standard provides a means for the resolver and server to agree on secret material for use with TSIG without their communication being secret. RFC 2931, an update to 2535, also addressed a piece of this issue by specifying under what circumstances the public key method (SIG(0)) should be used; for example to authenticate TKEY[19].

--An adequate mechanism for secure zone transfer. The advent of DDNS considerably complicates matters. The original DNSSec specification supposed that private keys would be kept off-line for security's sake, but this would prevent a dynamic server from signing new records automatically. RFC 2137 addresses this issue, but work is in progress on a replacement for RFC 2137[20].

--NXT RR's have turned out to be unpopular. Their use is not as well understood as the other RR's, partly because of unclear issues on how to handle delegations. Concerns also exist about the ability to "step through" all a zone's records using NXT. An IETF draft exists addressing this issue by the use of an alternative RR type.

--Until DNSSec is widespread, there will be gaps in the key-signing chain. This is a little bit of a chicken-and-egg problem, since widespread use is unlikely to occur until DNSSec has been well demonstrated to be effective. As stated above, CAIRN's project is intended to address this problem by enabling organizations to adopt DNSSec without waiting for the official root servers to be converted.

So where does all this leave us with BIND9? Most importantly for DNSSec, it is the first complete implementation of the standard. Therefore BIND9 provides the first opportunity to demonstrate fully that the standard works. Here are some facts to consider:

--The experts are encouraging its adoption. In June of 2000, RFC 2870 was accepted by

the IETF as "Best Current Practice" for root name server operations. The RFC states that "The root zone MUST be signed by the Internet Assigned Numbers Authority (IANA) in accordance with DNSSec.... It is understood that DNSSec is not yet deployable on some common platforms, but will be deployed when supported." Also, Network Fusion reported that the military intends to implement DNSSec in the .mil domain next year.[21]

--Sun, HP, and Red Hat are planning to include BIND9 with their products, according to Network Fusion. This will ease the job of implementation a little bit[22].

--Third party vendors are already beginning to create products based on DNSSec. An example is Ladon, "A Distributed Authentication System for SSH using DNSSec."[23]

--According to Network Fusion, Nominum and UltraDNS are offering outsourcing services for secure DNS. This means that if your organization doesn't have the technical expertise or the time to implement BIND9, you can have others do it for you. Nominum developers were involved in the development of BIND9[24].

--The drawbacks are: the need to learn the software -- it really was built from the ground up; greater configuration complexity; more frequent need to "touch" DNS, and increased computational resources on the server that runs DNS.

It's clear that better security for DNS is needed. DNSSec is the best thing we have so far, and it's problems are rapidly being solved. Here's what Paul Vixie has to say about BIND9: "The major feature ... is robustness. BIND9 was written by a large team of professional software developers who had enough time and enough money to 'get it right.'"[25]

Note: All RFCs referenced in this report can be found at http://www.ietf.org.

Notes:
[1] Internet Software Consortium , "ISC Bind 9", http://www.isc.org/products/BIND/bind9.html as of 11/15/00.
[2] Eastlake, Donald, "Domain Name System Security Extensions", March 1999, http://www.ietf.org/rfc/rfc2535.txt as of 11/15/00.
[3] All information in preceding paragraphs can be found in the RFC.
[4] Lewis, Edward, "DNS Security Extensions" PowerPoint presentation, Sep 12, 2000, can be downloaded from http://www.pgp.com/research/nailabs/network-security/domain-name.asp as of 11/15/00.
[5] See RFC's 1886, 2136 and 2874.
[6] Both quotations from Wreski, Dave, "Paul Vixie and David Conrad on BINDv9 and Internet Security", 10/3/2000, http://www.LinuxSecurity.com/feature_stories/conrad_vixie-1.html as of 11/12/00
[7] Network Associates, "Network Associates Selected to Develop New Internet Security Standard", August 25, 1998,

http://www.nai.com/naicommon/aboutnai/press/pr_template.asp?PR=/PressMedia/082598a.asp&Sel=304, as of 11/11/00.
[8] See note 4.
[9] Liman, Lars-Johan, et.al, "Report from the Workshop on DNSSEC ", May 18-19, 1999, http://www.isoc-se.a.se/dns-ws.html as of 11/15/00.
[10] For current status, see http://www.ietf.org/iesg/1rfc_index.txt as of 11/15/00.
[11] The DNSEXT charter at http://www.ietf.org/html.charters/dnsext-charter.html explains that the DNSEXT WG assumed the issues of the DNSSEC working group. It is not stated exactly when this happened, but the DNSSEC WG was clearly still active in early 1999.
[12] See RFC 2535.
[13] Author unstated, "Collaborative Advanced Internet Research Network (CAIRN) ", http://www.isi.edu/CAIRN/ as of 11/11/00.
[14] Author unstated, "Using DNSSec in the Internet Today," 10/14/99, http://www.cairn.net/DNSSEC/ as of 11/15/00.
[15] See the clickable map of the testbed topology at http://latte.east.isi.edu/CAIRNMON/WEBDATA/cairnimage.html as of 11/15/00.
[16] See note 14. Most of these problems were cited by CAIRN.
[17] The work in progress is an Internet draft.
[18] All of this is in the RFC cited.
[19] See the RFC's cited.
[20] The work in progress is an Internet draft.
[21] Marsan, Carolyn Duffy, "DNS security upgrade promises a safer 'Net", 10/16/00, http://www.nwfusion.com/news/2000/1016dnsec.html as of 11/11/00
[22] See note 21.
[23] John Hopkins University, "LADON A Distributed Authentication System for SSH using DNSSEC", http://www.cs.jhu.edu/~smang/sshproject.html as of 11/15/00.
[24] See note 21.
[25] Wreski, Dave, "Paul Vixie and David Conrad on BINDv9 and Internet Security", 10/3/2000, http://www.LinuxSecurity.com/feature_stories/conrad_vixie-1.html as of 11/12/00

References

RFC:
1034, "Domain Names - Concepts And Facilities", P. Mockapetris, November 1987.
1035, "Domain Names - Implementation And Specification", P. Mockapetris, November 1987.
2065, "Domain Name System Security Extensions", D. Eastlake, 3rd and C. Kaufman, January 1997.

2136, "Dynamic Updates in the Domain Name System", P. Vixie and others, April 1997.
2137, "Secure Domain Name System Dynamic Update", D. Eastlake 3rd, April 1997.
2535, "Domain Name System Security Extensions", D. Eastlake, March 1999.
2536, "DSA KEYs and SIGs in the Domain Name System", D. EastLake, March 1999.

2537, "RSA/MD5 KEYs and SIGs in the Domain Name System ", D. EastLake, March 1999.
2538, "Storing Certificates in the Domain Name System", D. EastLake, March 1999.
2539, "Storage of Diffie-Hellman Keys in the Domain Name System", D. EastLake, March 1999.
2541, "DNS Security Operational Considerations", D. EastLake, March 1999.
2845, "Secret Key Transaction Authentication for DNS", P. Vixie and others, May 2000.
2870, "Root Name Server Operational Requirements", R. Bush and others, June 2000.
2930, "Secret Key Establishment for DNS", D. Eastlake, 3rd, September 2000.
2931, "DNS Request and Transaction Signatures," D. Eastlake, 3rd, September 2000.

Web references, viewed 11/15/00:

BIND9:

Internet Software Consortium, "ISC BIND 9",
http://www.isc.org/products/BIND/bind9.html

Resource lists:

NLNetLabs, "DNSSEC resources", http://www.nlnetlabs.nl/dnssec/, reasonably complete listing of DNS Security resources.
András Salamon, "DNS Resources Directory", http://www.dns.net./dnsrd/ Listing of DNS (not only DNS security) resources.

***Explanations, how-to for DNSSec**:*

NAI Labs, "Domain Name System (DNS) Security",
http://www.pgp.com/research/nailabs/network-security/domain-name.asp, contains links to three powerpoint presentations by Edward Lewis, including **BIND9 how-to**.

Arends, Roy, http://open.nlnetlabs.nl/dnssec/dnssec-how-to.html for how-to sign a zone.
NIC-SE, http://www.nic-se.se./dnssec/, "NIC-SE reports on DNS Security", May 1999, information describing the workshop mentioned in this report; includes three powerpoint presentations by Edward Lewis.
*Davidowicz, Diane, "*Domain Name System (DNS) Security", 1999,
http://www.geocities.com/compsec101/papers/dnssec/dnssec.html
Davidowicz, Diane and Vixie, Paul, "Securing the Domain Name System", 1/1/00,
http://www.networkmagazine.com/article/NMG20000509S0039
Liu, Cricket , http://education.hp.dk/dns/ for explanation of basic cryptography, DNSSec and how to sign a zone using BIND 8.2 - pdf. The page is Dutch, but the pdfs are English.
Wellington, Brian, "Domain Name System (DNS) Security", January 22, 1999,
http://www.pgp.com/research/nailabs/network-security/an-introduction.asp.

Discussion:

Durham, *Mark,* "Vixie Wraps BIND", November 1999,
http://www.sendmail.net/?CssUID=&CssServer=&SessionName=&feed=interview000lisa01, A summary of talk by Paul Vixie concerning his involvement with BIND. He says,

"It's a thing of beauty. I have not got a single line of code in BIND 9 - and I hope that's not the reason that it's a thing of beauty."
Wreski, Dave, "Paul Vixie and David Conrad on BINDv9 and Internet Security", 10/3/2000, http://www.LinuxSecurity.com/feature_stories/conrad_vixie-1.html

LADON:
John Hopkins University, "LADON A Distributed Authentication System for SSH using DNSSEC", http://www.cs.jhu.edu/~smang/sshproject.html.

Last Updated: October 19th, 2017

Upcoming Training

SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201710,	Oct 23, 2017 - Nov 29, 2017	vLive
SANS Seattle 2017	Seattle, WA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS San Diego 2017	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	Live Event
San Diego Fall 2017 - SEC401: Security Essentials Bootcamp Style	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	vLive
SANS Gulf Region 2017	Dubai, United Arab Emirates	Nov 04, 2017 - Nov 16, 2017	Live Event
Community SANS Vancouver SEC401^	Vancouver, BC	Nov 06, 2017 - Nov 11, 2017	Community SANS
Community SANS Colorado Springs SEC401~	Colorado Springs, CO	Nov 06, 2017 - Nov 11, 2017	Community SANS
SANS Miami 2017	Miami, FL	Nov 06, 2017 - Nov 11, 2017	Live Event
SANS Paris November 2017	Paris, France	Nov 13, 2017 - Nov 18, 2017	Live Event
SANS Sydney 2017	Sydney, Australia	Nov 13, 2017 - Nov 25, 2017	Live Event
SANS San Francisco Winter 2017	San Francisco, CA	Nov 27, 2017 - Dec 02, 2017	Live Event
Community SANS St. Louis SEC401	St Louis, MO	Nov 27, 2017 - Dec 02, 2017	Community SANS
SANS London November 2017	London, United Kingdom	Nov 27, 2017 - Dec 02, 2017	Live Event
Community SANS Portland SEC401	Portland, OR	Nov 27, 2017 - Dec 02, 2017	Community SANS
SANS Khobar 2017	Khobar, Saudi Arabia	Dec 02, 2017 - Dec 07, 2017	Live Event
SANS Austin Winter 2017	Austin, TX	Dec 04, 2017 - Dec 09, 2017	Live Event
SANS Munich December 2017	Munich, Germany	Dec 04, 2017 - Dec 09, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Dec 04, 2017 - Dec 09, 2017	Community SANS
SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201712,	Dec 11, 2017 - Jan 24, 2018	vLive
SANS Bangalore 2017	Bangalore, India	Dec 11, 2017 - Dec 16, 2017	Live Event
SANS Cyber Defense Initiative 2017	Washington, DC	Dec 12, 2017 - Dec 19, 2017	Live Event
SANS Cyber Defense Initiative 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Dec 14, 2017 - Dec 19, 2017	vLive
SANS Security East 2018	New Orleans, LA	Jan 08, 2018 - Jan 13, 2018	Live Event
Community SANS Nashville SEC401^	Nashville, TN	Jan 08, 2018 - Jan 13, 2018	Community SANS
Community SANS Hawaii SEC401	Honolulu, HI	Jan 08, 2018 - Jan 13, 2018	Community SANS
Mentor Session - SEC401	Memphis, TN	Jan 09, 2018 - Mar 13, 2018	Mentor
SANS Amsterdam January 2018	Amsterdam, Netherlands	Jan 15, 2018 - Jan 20, 2018	Live Event
Northern VA Winter - Reston 2018	Reston, VA	Jan 15, 2018 - Jan 20, 2018	Live Event
Mentor Session - SEC401	Minneapolis, MN	Jan 16, 2018 - Feb 27, 2018	Mentor
SANS Las Vegas 2018	Las Vegas, NV	Jan 28, 2018 - Feb 02, 2018	Live Event
Las Vegas 2018 - SEC401: Security Essentials Bootcamp Style	Las Vegas, NV	Jan 28, 2018 - Feb 02, 2018	vLive