DNSSEC

2/17/2012 Lunch and Learn

Topics

- DNSSEC Standard
- DNSSEC Products and Companies
- DNSSEC Initiatives
- Secure Naming Infrastructure Project (SNIP)

DNSSEC Standard

- A suite of protocols (RFCs 4033, 4034, 4035) extending current DNS specs.
  - Adds security services
    - Origin authentication and integrity assurance services for DNS data,
    - Including mechanisms for authenticated denial of existence of DNS data

Background: DNS Resource Records

- DNS Resource Records (RRs) contain network name and address information, and additional types of information to support the DNS process.

TYPE	RFC	Description
A	RFC 1035	Address record mapping hostname to IPv4 address
AAAA	RFC 3596	Address record mapping hostname to IPv6 address
CNAME	RFC 1035	Canonical name record, the alias of one name for another
MX	RFC 1035	Mail exchange, recording the message transfer agents for the domain
NS	RFC 1035	Name server record, delegates a DNS zone to an authoritative name server

New RR Types for DNSSEC

TYPE	RFC	Description
DNSKEY	RFC 4034	Public keys
NSEC	RFC 4034	Used to prove a name does not exist
RRSIG	RFC 4034	Signature over a set of RRs
DS	RFC 4034	Delegation signer, identifies the signing key of a delegated zone

RFC4033 Overview

- DNS Security Introduction and Requirements
- Defines concepts such as:

  Authentication Chain, Authentication Key, Authoritative RRset, Delegation Point, Island of Security, Key Signing Key (KSK), Non-Validating Security-Aware Stub Resolver, Non-Validating Stub Resolver, Security-Aware Name Server, Security-Aware Recursive Name Server, Security-Aware Resolver, Security-Aware Stub Resolver, Security-Oblivious <anything>, Signed Zone, Trust Anchor, Unsigned Zone, Validating Security-Aware Stub Resolver, Validating Stub Resolver, Zone Apex, Zone Signing Key (ZSK)

RFC4033 - DNSSEC Concepts

- Logical Objects
  - Keys
    - Authentication Key, Key Signing Key (KSK), Zone Signing Key (ZSK), Trust Anchor
  - Authentication Chain
  - Authoritative RRset
  - Island of Security
  - Zones (signed, unsigned, apex)
  - Delegation Point
- Physical Objects
  - Resolvers
    - Stub or non-stub
    - Validating or non-validating
    - Security-aware or security-oblivious
  - Name Servers
    - Security-Aware or security-oblivious
    - Recursive or non-recursive

RFC4033 – 3.1 Data Origin Authentication and Data Integrity

- DNSSEC provides authentication by associating cryptographically generated digital signatures with DNS RRsets. These digital signatures are stored in a new resource record, the RRSIG record. Typically, there will be a single private key that signs a zone's data, but multiple keys are possible. For example, there may be keys for each of several different digital signature algorithms.
- An important DNSSEC concept is that the key that signs a zone's data is associated with the zone itself and not with the zone's authoritative name servers.

RFC4033 - Security Aware Resolvers

- A security-aware resolver can learn a zone's public key either by having a trust anchor configured into the resolver or by normal DNS resolution. To allow the latter, public keys are stored in a new type of resource record, the DNSKEY RR. Note that the private keys used to sign zone data must be kept secure and should be stored offline when practical. To discover a public key reliably via DNS resolution, the target key itself has to be signed by either a configured authentication key or another key that has been

RFC4033 - What DNSSEC does not do

- DNS was originally designed with the assumptions that the DNS will return the same answer to any given query regardless of who may have issued the query, and that all data in the DNS is thus visible. Accordingly, DNSSEC is not designed to provide confidentiality, access control lists, or other means of differentiating between inquirers.

  DNSSEC provides no protection against denial of service attacks. Security-aware resolvers and security-aware name servers are vulnerable to an additional class of denial of service attacks based on cryptographic operations. Please see Section 12 for details.

RFC4033 - DNSSEC Data State

- Determined by a validating resolver
  - Secure: The validating resolver has a trust anchor, has a chain of trust, and is able to verify all the signatures in the response.
  - Insecure: The validating resolver has a trust anchor, a chain of trust, and, at some delegation point, signed proof of the non-existence of a DS record. This indicates that subsequent branches in the tree are provably insecure. A validating resolver may have a local policy to mark parts of the domain space as insecure.
  - Bogus: The validating resolver has a trust anchor and a secure delegation indicating that subsidiary data is signed, but the response fails to validate for some reason: missing signatures, expired signatures, signatures with unsupported algorithms, data missing that the relevant NSEC RR says should be present, and so forth.
  - Indeterminate: There is no trust anchor that would indicate that a specific portion of the tree is secure. This is the default operation mode.

RFC4033 - Resolver considerations

- A security-aware resolver has to be able to perform cryptographic functions necessary to verify digital signatures using at least the mandatory-to-implement algorithm(s). Security-aware resolvers must also be capable of forming an authentication chain from a newly learned zone back to an authentication key, as described above. This process might require additional queries to intermediate DNS zones to obtain necessary DNSKEY, DS, and RRSIG records. A security-aware resolver should be configured with at least one trust anchor as the starting point from which it will attempt to establish authentication chains.

RFC4033 - Stub Resolvers

- Stub resolvers are minimal DNS resolvers that use recursive query mode to offload most of the work of DNS resolution to a recursive name server.
- Even a security-oblivious stub resolver may benefit from DNSSEC if the recursive name servers it uses are security-aware, but for the stub resolver to place any real reliance on DNSSEC services, the stub resolver must trust both the recursive name servers in question and the communication channels between itself and those name servers.
- A security-aware stub resolver that does trust both its recursive name servers and its communication channel to them may choose to examine the setting of the Authenticated Data (AD) bit in the message header of the response messages it receives.

RFC 4033 - Zones

- There are several differences between signed and unsigned zones. A signed zone will contain additional security-related records (RRSIG, DNSKEY, DS, and NSEC records). RRSIG and NSEC records may be generated by a signing process prior to serving the zone. The RRSIG records that accompany zone data have defined inception and expiration times that establish a validity period for the signatures and the zone data the signatures cover.

RFC4033 - Zone Temporal Dependencies

- New Temporal Dependency Issues for Zones
  - Information in a signed zone has a temporal dependency that did not exist in the original DNS protocol. A signed zone requires regular maintenance to ensure that each RRset in the zone has a current valid RRSIG RR. The signature validity period of an RRSIG RR is an interval during which the signature for one particular signed RRset can be considered valid, and the signatures of different RRsets in a zone may expire at different times. Re-signing one or more RRsets in a zone will change one or more RRSIG RRs, which will in turn require incrementing the zone's SOA serial number to indicate that a zone change has occurred and re-signing the SOA RRset itself. Thus, re-signing any RRset in a zone may also trigger DNS NOTIFY messages and zone transfer operations.
- What does that mean? Ongoing work for somebody.

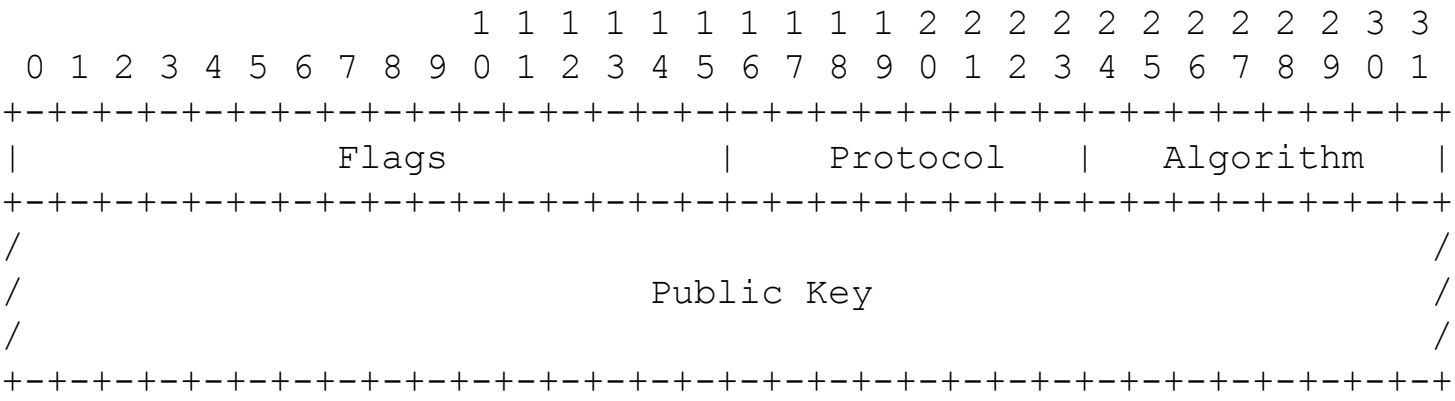
RFC4033 - Name Server Considerations

- If possible, the private half of each DNSSEC key pair should be kept offline, but this will not be possible for a zone for which DNS dynamic update has been enabled. In the dynamic update case, the primary master server for the zone will have to re-sign the zone when it is updated, so the private key corresponding to the zone signing key will have to be kept online. This is an example of a situation in which the ability to separate the zone's DNSKEY RRset into zone signing key(s) and key signing key(s) may be useful, as the key signing key(s) in such a case can still be kept offline and may have a longer useful lifetime than the zone signing key(s).
- By itself, DNSSEC is not enough to protect the integrity of an entire zone during zone transfer operations, as even a signed zone contains some unsigned, nonauthoritative data if the zone has any children. Therefore, zone maintenance operations will require some additional mechanisms (most likely some form of channel security, such as TSIG, SIG(0), or IPsec).

RFC4034

- Data formats for new DNS resource records
  - DNSKEY
  - RRSIG
  - NSEC
  - DS

RFC4034 - DNSKEY

- 

RFC4034 - DNSKEY Flags

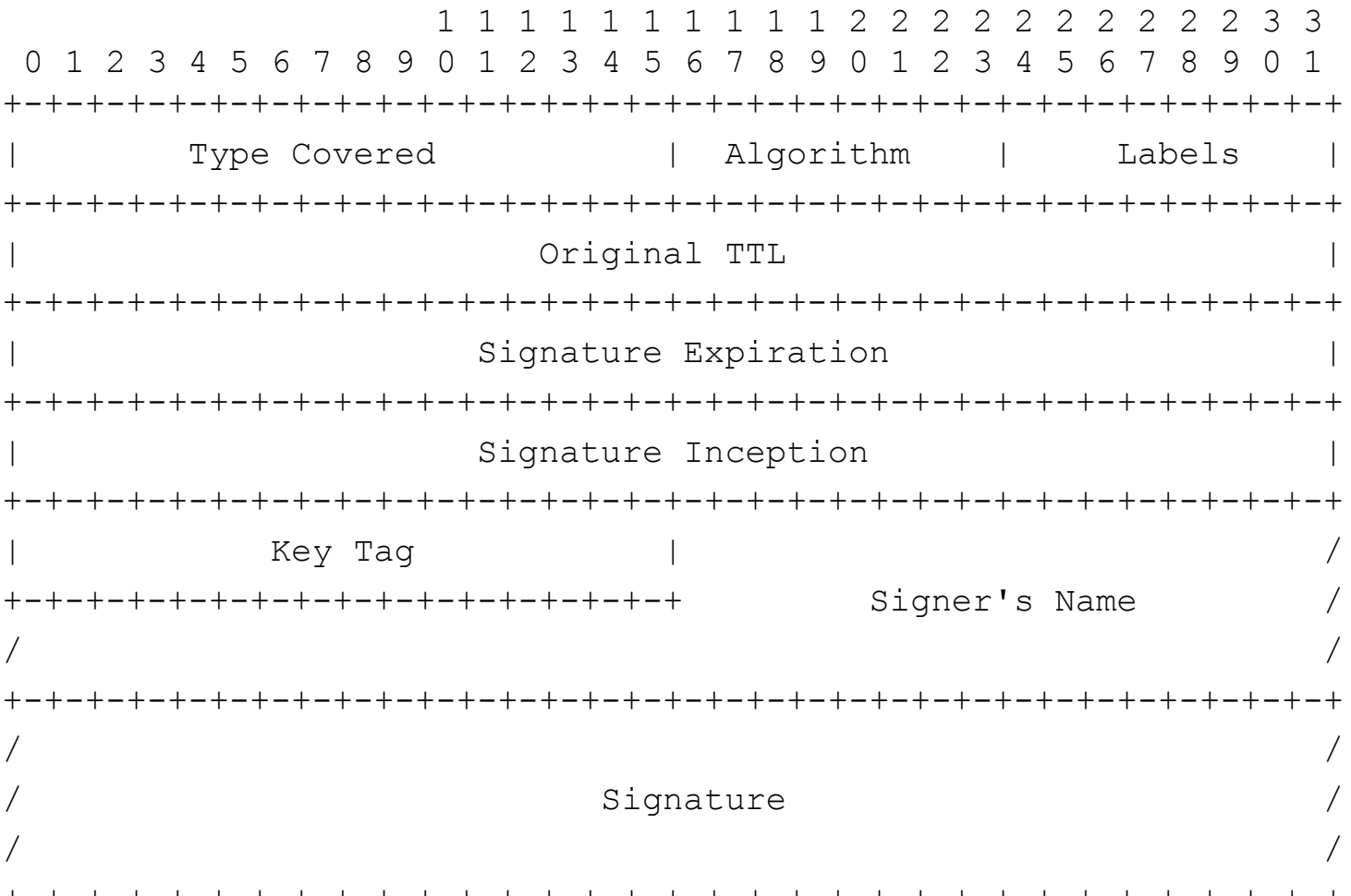
- Bit 7 of the Flags field is the Zone Key flag. If bit 7 has value 1, then the DNSKEY record holds a DNS zone key, and the DNSKEY RR's owner name MUST be the name of a zone. If bit 7 has value 0, then the DNSKEY record holds some other type of DNS public key and MUST NOT be used to verify RRSIGs that cover RRsets.

- Bit 15 of the Flags field is the Secure Entry Point flag, described in [RFC3757]. If bit 15 has value 1, then the DNSKEY record holds a key intended for use as a secure entry point. This flag is only intended to be a hint to zone signing or debugging software as to the intended use of this DNSKEY record; validators MUST NOT alter their behavior during the signature validation process in any way based on the setting of this bit. This also means that a DNSKEY RR with the SEP bit set would also need the Zone Key flag set in order to be able to generate signatures legally. A DNSKEY RR with the SEP set and the Zone Key flag not set MUST NOT be used to verify RRSIGs that cover RRsets.

RFC4034 - DNSKEY Fields

- Protocol: must be 3
- Algorithm: Appendix A.1, extended by additional RFCs
- Public Key: holds the public key in a algorithm specific format

RFC4034 - RRSIG



RFC4034 - RRSIG Fields

- The Signature Expiration and Inception fields specify a validity period for the signature. The RRSIG record MUST NOT be used for authentication prior to the inception date and MUST NOT be used for authentication after the expiration date.
- The Key Tag field contains the key tag value of the DNSKEY RR that validates this signature, in network byte order. Appendix B explains how to calculate Key Tag values.
- The Signature field contains the cryptographic signature that covers the RRSIG RDATA (excluding the Signature field) and the Rrset specified by the RRSIG owner name, RRSIG class, and RRSIG Type Covered field.

RFC4034 - RRSIG Example

```
host.example.com. 86400 IN RRSIG A 5 3 86400 20030322173103 (
                                20030220173103 2642 example.com.
                                oJB1W6WNGv+ldvQ3WDG0MQkg5IEhjRip8WTr
                                PYGv07h108dUKGMeDPKijVCHX3DDKdfb+v6o
                                B9wfuh3DTJXUAfI/M0zmO/zz8bW0Rznl8O3t
                                GNazPwQKkRN20XPXV6nwwfoXmJQbsLNrLfkG
                                J5D6fwFm8nN+6pBzeDQfsS3Ap3o= )
```

The first four fields specify the owner name, TTL, Class, and RR type (RRSIG). The "A" represents the Type Covered field. The value 5 identifies the algorithm used (RSA/SHA1) to create the signature. The value 3 is the number of Labels in the original owner name. The value 86400 in the RRSIG RDATA is the Original TTL for the covered A RRset. 20030322173103 and 20030220173103 are the expiration and inception dates, respectively. 2642 is the Key Tag, and example.com. is the Signer's Name. The remaining text is a Base64 encoding of the signature.

Note that combination of RRSIG RR owner name, class, and Type Covered indicates that this RRSIG covers the "host.example.com" A RRset. The Label value of 3 indicates that no wildcard expansion was used. The Algorithm, Signer's Name, and Key Tag indicate that this signature can be authenticated using an example.com zone DNSKEY RR whose algorithm is 5 and whose key tag is 2642.

RFC 3045 Overview

- Protocol Modifications for the DNS Security Extensions
  - Zone Signing, which consists of new DNS record types:
    - DNS Public Key
    - Resource Record Signature (RRSIG)
    - Next Secure (NSEC)
    - Delegation Signer (DS)

RFC 4035 – Signing A Zone

- To sign a zone, the zone's administrator generates one or more public/private key pairs and uses the private key(s) to sign authoritative RRsets in the zone. For each private key used to create RRSIG RRs in a zone, the zone SHOULD include a zone DNSKEY RR containing the corresponding public key.

DNSSEC Tools and Companies

DNSSEC Tools

- Zone Administrator Tools
  - Name Servers (BIND, NSD, UNBOUND, ANS, CNS)
  - Key Management (dnssec-keygen, dnssec-signzone, zonesigner, maintkeydb, …)
  - Hardware Support (Smartcard utility, pkcs11HSMtools)
- Monitoring/troubleshooting tools
- Appliances
- Secure Delegation Tools
- Validation Tools (trust anchor repositories, trust maintenance tools)
- DNSSEC capable applications (Firefox, Thunderbird, SSH, sendmail, postfix, …)

DNSSEC Companies

- Tool Developers
  - SPARTA, Verisign Labs, NIST, NLNet Labs, Nominum, …
- Applicance Vendors
  - Secure64, Xelerence, InfoWeapons, INS, Nixu, …

DNSSEC Initiatives

- DNSSEC Deployment Initiative (DHS)
- Secure Naming Infrastructure Pilot (NIST)

DNSSEC Deployment Initiative

- U.S. Department of Homeland Security Science and Technology (S&T) Directorate supports coordination of DNSSEC deployment within the government
- Providers resources and a discussion forum for vendors and implementers
- The DNSSEC Deployment Initiative will hold a workshop at the 2012 FOSE conference (April 3-5, 2012).

Secure Naming Infrastructure Project

- NIST operates SNIP, not sure of their role in the deployment initiative yet.
- They maintain interesting information such as the SNIP Integrity Status over the dnsops.gov and dnsops.biz domains.

SNIP Integrity Status as of 2/17/12

SNIP Zone Status

Zonename	Signed?	Status	Island or Chain?
dnsops.gov.	Signed	Valid	Chained
dnsops.biz.	Signed	Valid	Chained
404.dnsops.gov.	Unsigned	N/A	Chained
cbo.dnsops.gov.	Unsigned	N/A	Chained
defensesolutions.dnsops.gov.	Signed	Valid	Chained
denali.dnsops.gov.	Signed	Valid	Chained
dhs.dnsops.gov.	Signed	Valid	Chained
energy.dnsops.gov.	Unsigned	N/A	Error
epa.dnsops.gov.	Unsigned	N/A	Chained
fcc.dnsops.gov.	Unsigned	N/A	Chained
fda.dnsops.gov.	Unsigned	N/A	Chained
fdic.dnsops.gov.	Signed	Valid	Chained
federalreserve.dnsops.gov.	Unsigned	N/A	Chained
ferc.dnsops.gov.	Unsigned	N/A	N/A
ihs.dnsops.gov.	Unsigned	N/A	Chained
inl.dnsops.gov.	Signed	Valid	Chained
inel.dnsops.gov.	Signed	Valid	Chained
irs.dnsops.gov.	Signed	Valid	Chained
llnl.dnsops.gov.	Unsigned	N/A	Chained
mail.dnsops.gov.	Signed	Valid	Chained
mogov.dnsops.gov.	Signed	Valid	Chained
nalusda.dnsops.gov.	Signed	Valid	Chained
nga.dnsops.gov.	Signed	Error	Chained
nlrb.dnsops.gov.	Unsigned	N/A	Chained
ntis.dnsops.gov.	Unsigned	N/A	Chained
nws.dnsops.gov.	Unsigned	N/A	N/A
opm.dnsops.gov.	Signed	Error	Chained
ornl.dnsops.gov.	Unsigned	N/A	Chained
sandia.dnsops.gov.	Signed	Valid	Chained
sbatest.dnsops.gov.	Unsigned	N/A	Chained
secstate.dnsops.gov.	Unsigned	N/A	Chained
treas.dnsops.gov.	Unsigned	N/A	Chained
virginia.dnsops.gov.	Signed	Error	Chained
voa.dnsops.gov.	Signed	Valid	Chained
ymp.dnsops.gov.	Unsigned	N/A	Chained
akamai.dnsops.biz.	Signed	Valid	Chained
btdiamondip.dnsops.biz.	Unsigned	N/A	Chained
ctl.dnsops.biz.	Signed	Valid	Chained
f5.dnsops.biz.	Unsigned	N/A	Chained
infoblox.dnsops.biz.	Signed	Error	Chained
infoweapons.dnsops.biz.	Unsigned	N/A	Chained
nsd.dnsops.biz.	Unsigned	N/A	Chained
sgns.dnsops.biz.	Signed	Error	Chained
sparta.dnsops.biz.	Unsigned	N/A	Chained
usap.dnsops.biz.	Unsigned	N/A	Chained
xelerance.dnsops.biz.	Unsigned	N/A	Chained

Questions?