DNS Secure Update

Donald E. Eastlake 3rd
CyberCash, Inc.
2100 Reston Parkway, Suite 430
Reston, VA 22091 USA
<mailto:dee@cybercash.com>

DNS Secure Update

- DNS Security and Beta Code Availability
- KEY Format and Structure
- SIG Format and Use in Update
- The in-key.int. Domain

<ftp://ftp.isi.edu/draft-ietf-dnssec-update-00.txt>

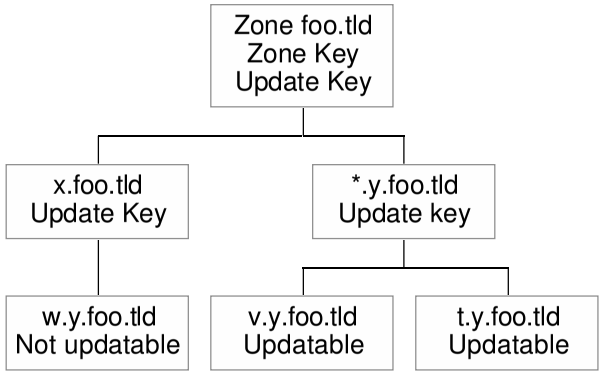
DNS Security

- Authenticates DNS data with digital signatures
- Provides for general public key storage
- See draft-ietf-dnssec-secext-09.txt in the IETF shadow directories.
- In IETF Last Call now.

Beta DNSSEC Code Available

- TIS/DNSSEC based on bind-4.9.3-REL
  - <ftp://ftp.tis.com/pub/DNSSEC/README>
  - <mailto:tisdnssec-support@tis.com>
- uses RSAREF
- comes with a security enabled DIG
  - <ftp://ftp.tis.com/pub/DNSSEC/sdig.sunos4.gz>
- first secure zone: sd-bogus.tis.com

Key Hierarchy in a Zone



DNS KEY Format

```
OWNER NAME, Type: KEY, Class (IN), TTL, RDSIZE,
                     1 1 1 1 1 1 1 1 1 1 2 2 2 2 2 2 2 2 2 2 3 3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|            flags              |    protocol   |   algorithm   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               /
/                          public key                           /
/                                                               /
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-|

For RSA Algorithm, public key=
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| pub exp length|        public key exponent                    /
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               /
+-                          modulus                            /
|                                                               /
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-/
```


DNS KEY Flags

0	Don't use for authentication
1	Don't use for confidentiality
2	Experimental
3-4	(reserved)
5	User
6	Host/End-Entity
7	Zone
8	Reserved for IPSEC
9	Reserved for email
10-11	(reserved)
12-15	Signatory Field

DNS KEY Signatory Flags

```
UPDATE KEY RR SIGNATORY FIELD BITS
       12          13          14          15
   +-----------+-----------+-----------+-----------+
   |   zone    |  strong   |  unique   |  general  |
   +-----------+-----------+-----------+-----------+

ZONE KEY RR SIGNATORY FIELD BITS
       12          13          14          15
   +-----------+-----------+-----------+-----------+
   |   mode    |  strong   |  unique   |  general  |
   +-----------+-----------+-----------+-----------+

   mode=0 -> mode A,  mode=1 -> mode B
```

DNS Signature Format

```
OWNER NAME, Type: SIG, Class (IN), TTL, RDSIZE,
                     1 1 1 1 1 1 1 1 1 1 2 2 2 2 2 2 2 2 2 2 3 3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|        type covered           |  algorithm    |     labels    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                         original TTL                          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                      signature expiration                     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                         time signed                           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|         key footprint         |                              /
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+         signer's name        /
/                                                             /
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                             /
+-                          signature                         /
/                                                             /
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```


Signed Updates

```
MODE A

Header, op code = update
Pre-requisites
Signed Data
Request Signatures


MODE B

Header, op code = update
Pre-requisites
Unsigned Data
Request Signatures
```


Dynamic Secure Zone Modes

SUMMARY OF DYNAMIC SECURE ZONE MODES

CRITERIA:	MODE A	MODE B
Zone Key	Off line	On line
Server Workload	Low	High
Static Data Security	Very High	Medium-High
Dynamic Data Security	Medium	Medium-High
Dynamic Key Rollover	No	Yes
Key Restrictions	Fine grain	Coarse grain

The in-key.int. Domain

```
<key-hash>.<key-footprint>.algorithm.in-key.int.

$ORIGIN xxxx.xxxx.xxxx.xxxx.xxxx.xxxx.xx
                  xx.xxxx.xxxx.xxxx.xxxx.1.in-key.int.
   IN KEY <flags> 0 1 (45IkskceFGgiWCn/GxHhai6VAuHAoNUz4YoUMxF
   cby9k/yvedMfQgKzhH5er0Mu/vILz80jEeC8aTrO+KKmCaY1tVfSCqQYn6/
    /11U6Nld=    ;key )
   IN SIG KEY 1 3 ( ;type-cov=PTR, alg=1, labels=3
                    19991202030405 ;signature expiration
                    19951211100908 ;time signed
                    2143658709     ;key footprint
                    example.tld.       ;signer
   MxFcby9k/yvedMfQgKzhH5er0Mu/vILz45IkskceFGgiWCn/GxHhai6VAuH
   AoNUz4YoU1tVfSCSqQYn6//11U6Nld80jEeC8aTrO+KKmCaY=
                    ;signature
                    )
```