DNS Protocol Security Extensions

Overview and Selected Details

Donald E. Eastlake 3rd

Charles W. Kaufman

Digital Equipment Corporation

March 28, 1994

Goals:

- Authenticate the information returned by DNS.
- Provide a means for storing the RSA public keys of DNS-named entities.

Non-Goals:

- Provide access controls on information in DNS (all information is assumed public).
- Provide privacy for interactions with DNS servers.

Approach:

- Define RSA keys for DNS zones
- Sign all the data in DNS with RSA signatures
- Optionally return the signatures with the data
- Have security aware resolvers verify the signatures before believing the data

[Note: for reasonable security, resolvers must be configured with the public key of at least one zone; it can then securely learn the public keys of other zones via signed "glue" records. Greater security is obtained by configuring resolvers with the keys of all critical zones].

Alternate Approach:

(also specified)

- Assign RSA keys to DNS servers.
- Have DNS servers sign responses to queries.
- Have resolvers verify those signatures.

Advantages:

- Non-existence of data can be signed.
- Revocation is secure and immediate.

Disadvantages:

- DNS servers are less trustworthy than off line Zone CAs.
- Performance of on-line RSA signatures is not likely to be wonderful.

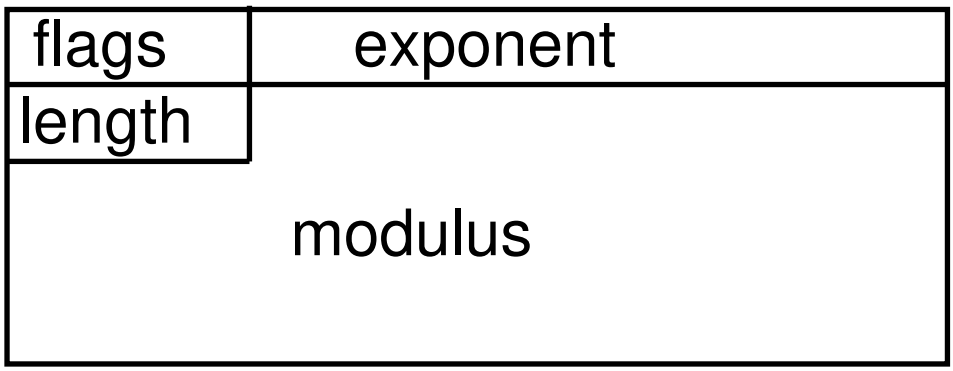
Design Overview:

- Two new resource record types:
  - SIG: RSA signature
  - RSA: RSA public key
- Optional protocol modifications for better performance
  - Client can request that corresponding signatures come back with data
  - Protocol changes are not required even for secure operation
  - Protocol modifications minimize number of interactions between client and server when both data and signatures are needed
- Substantial "hacks" to make security possible without a substantial performance penalty

Optimizations:

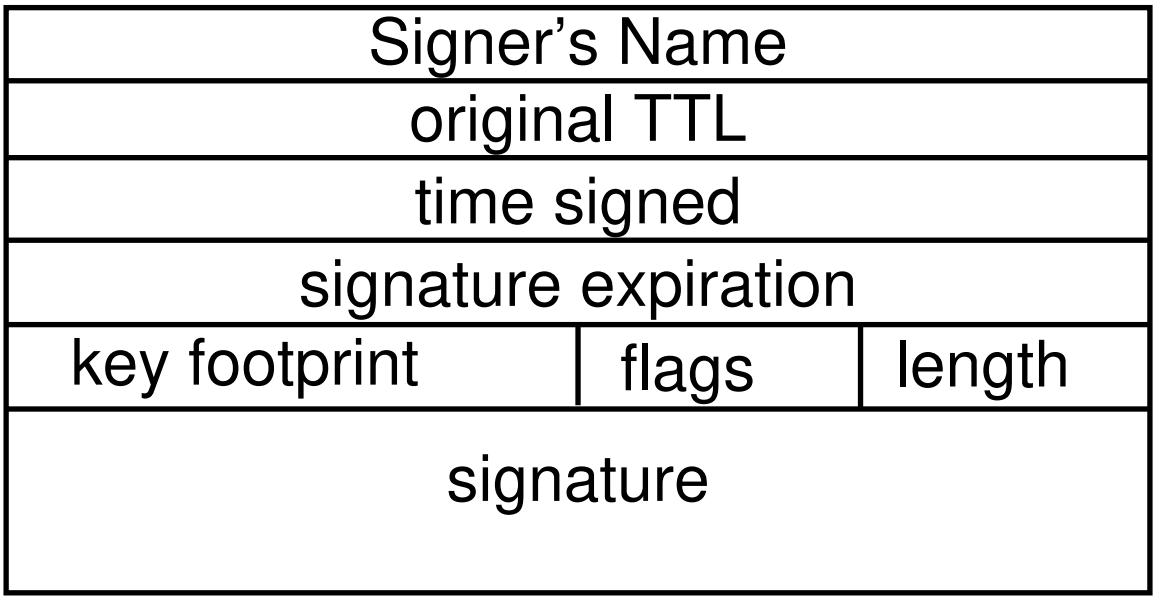
- RSA signatures are big (64-256 bytes) and are expensive to verify
  - — Sign multiple RRs for a single name with one signature
  - — When signing small RRs, include the signed value in the signature and don't return the RRs except implicitly in the signature
- Server interactions are expensive
  - — Return signatures corresponding to the data requested without being asked

RSA RR:



- flags: specifies the range of authority of this public key
- exponent: public exponent (<2^24)
- length: 640 - 2048 bits
- modulus: public modulus

SIG RR



Signature

(after decryption)

Types of Signets:

- Direct Resource Record
- Hashed Resource Record
- Flags:
  - — Partial SIG
  - — Partial RR Set
- Hashed query
- Hashed response
- Direct Glue Record
- Hashed Glue Record