DNS Security Working Group   Donald E. Eastlake 3rd
INTERNET-DRAFT   CyberCash
Expires: September 1998   March 1998

DNS Operational Security Considerations
--- ----------- -------- --------------

Status of This Document

This draft, file name draft-ietf-dnssec-secops-01.txt, is intended to be become an Informational RFC. Some of this material was included in [RFC 2065] but that RFC is obsoleted by [draft-ietf-dnssec-secext2-*.txt] which does not include this material. Distribution of this document is unlimited. Comments should be sent to the DNS Security Working Group mailing list <dns-security@tis.com> or to the authors.

Abstract

Secure DNS is based on cryptographic techniques. A necessary part of the strength of these techniques is careful attention to the operational aspects of key and signature generation, lifetime, size, and storage. In addition, special attention must be paid to the security of the high level zones, particularly the root zone. This document discusses these operational aspects for keys and signatures used in connection with the KEY and SIG DNS resource records.

Acknowledgments

The contributions and suggestions of the following persons (in alphabetic order) are gratefully acknowledged:

John Gilmore
Olafur Gudmundsson
Charlie Kaufman

Table of Contents

1. Introduction

This document describes operational considerations for the generation, lifetime, size, and storage of DNS cryptographic keys and signatures for use in the KEY and SIG resource records [draft-ietf-dnssec-secext2-*.txt]. Particular attention is paid to high level zones and the root zone.

2. Public/Private Key Generation

Careful generation of all keys is a sometimes overlooked but absolutely essential element in any cryptographically secure system. The strongest algorithms used with the longest keys are still of no use if an adversary can guess enough to lower the size of the likely key space so that it can be exhaustively searched. Technical suggestions for the generation of random keys will be found in [RFC 1750].

Long term keys are particularly sensitive as they will represent a more valuable target and be subject to attack for a longer timer than short period keys. It is strongly recommended that long term key generation occur off-line in a manner isolated from the network via an air gap or, at a minimum, high level secure hardware.

3. Public/Private Key Lifetimes

No key should be used forever. The longer a key is in use, the greater the probability that it will have been compromised through carelessness, accident, espionage, or cryptanalysis. Furthermore, if key rollover is a rare event, there is an increased risk that, when the time does come to change the key, no one at the site will remember how to do it or operational problems will have developed in the key rollover procedures.

While public key lifetime is a matter of local policy, these considerations suggest that no long term key should have a lifetime significantly over four years. In fact, a reasonable guideline for long term keys that are kept off-line and carefully guarded is a 13 month lifetime with the intent that they be replaced every year. A reasonable maximum lifetime for keys that are used for transaction security or the like and are kept on line is 36 days with the intent that they be replaced monthly or more often. In many cases, a key lifetime of somewhat over a day may be reasonable.

4. Public/Private Key Size Considerations

There are a number of factors that effect public key size choice for use in the DNS security extension. Unfortunately, these factors usually do not all point in the same direction. Choice of zone key size should generally be made by the zone administrator depending on their local conditions.

For most schemes, larger keys are more secure but slower. In addition, larger keys increase the size of the KEY and SIG RRs. This increases the chance of DNS UDP packet overflow and the possible necessity for using higher overhead TCP in responses.

4.1 RSA Key Sizes

Given a small public exponent, verification (the most common operation) for the MD5/RSA algorithm will vary roughly with the square of the modulus length, signing will vary with the cube of the modulus length, and key generation (the least common operation) will vary with the fourth power of the modulus length. The current best algorithms for factoring a modulus and breaking RSA security vary roughly with the 1.6 power of the modulus itself. Thus going from a 640 bit modulus to a 1280 bit modulus only increases the verification time by a factor of 4 but may increase the work factor of breaking the key by over 2^900.

The recommended minimum RSA algorithm modulus size, 640 bits, is believed by the author to be secure at this time but high level zones in the DNS tree may wish to set a higher minimum, perhaps 1000 bits, for security reasons. (Since the United States National Security Agency generally permits export of encryption systems using an RSA modulus of up to 512 bits, use of that small a modulus, i.e. n, must be considered weak.)

For an RSA key used only to secure data and not to secure other keys, 640 bits should be adequate at this time.

4.2 DSS Key Sizes

DSS keys are probably roughly as strong as an RSA key of the same length but DSS signatures are significantly smaller.

5. Private Key Storage

It is recommended that, where possible, zone private keys and the zone file master copy be kept and used in off-line non-network connected physically secure machines only. Periodically an application can be run to add authentication to a zone by adding SIG and NXT RRs and adding no-key type KEY RRs for subzones/algorithms where a real KEY RR for the subzone with that algorithm is not provided. Then the augmented file can be transferred, perhaps by sneaker-net, to the networked zone primary server machine.

The idea is to have a one way information flow to the network to avoid the possibility of tampering from the network. Keeping the zone master file on-line on the network and simply cycling it through an off-line signer does not do this. The on-line version could still be tampered with if the host it resides on is compromised. For maximum security, the master copy of the zone file should be off net and should not be updated based on an unsecured network mediated communication.

This is not possible if the zone is to be dynamically updated securely [RFC 2137]. At least a private key capable of updating the SOA and NXT chain must be one line in that case.

Secure resolvers must be configured with some trusted on-line public key information (or a secure path to such a resolver) or they will be unable to authenticate. Although on line, this public key information must be protected or it could be altered so that spoofed DNS data would appear authentic.

Non-zone private keys, such as host or user keys, generally have to be kept on line to be used for real-time purposes such as DNS transaction security.

6. High Level Zones, The Root Zone, and The Meta-Root Key

Higher level zones are generally more sensitive than lower level zones. Anyone controlling or breaking the security of a zone thereby obtains authority over all of its subdomains (except in the case of resolvers that have locally configured the public key of a subdomain). Therefore, extra care should be taken with high level zones and strong keys used.

The root zone is the most critical of all zones. Someone controlling or compromising the security of the root zone would control the entire DNS name space of all resolvers using that root zone (except in the case of resolvers that have locally configured the public key of a subdomain). Therefore, the utmost care must be taken in the securing of the root zone. The strongest and most carefully handled keys should be used. The root zone private key should always be kept off line.

Many resolvers will start at a root server for their access to and authentication of DNS data. Securely updating an enormous population of resolvers around the world will be extremely difficult. Yet the guidelines in section 3 above would imply that the root zone private key be changed annually or more often and if it were staticly configured at all these resolvers, it would have to be updaed when changed.

To permit relatively frequent change to the root zone key yet minimize exposure of the ultimate key of the DNS tree, there will be a "meta-root" key used very rarely and then only to sign a sequence of regular root key RRsets with overlapping time validity periods that are to be rolled out. The root zone contains the meta-root and current regular root KEY RR(s) signed by SIG RRs under both the meta-root and other root private key(s) themselves.

For example, assume that the regular root zone key is to be changed once a month. If the meta-root key were to be exposed only once a year, then for each exposure you might use the meta-key to sign twenty four key RRsets as follows:

     one with a date signed of the middle of January and expiring the middle of February with the January and Jan/Feb root keys,

     one with a date signed of the beginning of February and expiring the end of February with the Jan/Feb and February root keys,

     one with a date signed of the middle of February and expiring the middle of March with the February and Feb/Mar root keys,

     one with the data signed of the beginning of March and expiring the end of March with the Feb/Mar and March root keys,

     etc.

During the first half of January, the data in the root zone with the above hypothetical key policy would be signed with the Dec/Jan and January keys. During the second half of January, it would be signed with the January and Jan/Feb keys. During the first half of February, it would be signed with the Jan/Feb and February keys. Etc.

The utmost security in the storage and use of the meta-root key is essential. The exact techniques are precautions to be used are beyond the scope of this document. Because of its special position, it may be best to continue with the same meta-root key for an extended period of time such as ten to fifteen years.

7. Security Considerations

The entirety of this document is concerned with operational considerations of public/private key pair DNS Security.

References

[RFC 1034] - P. Mockapetris, "Domain Names - Concepts and Facilities", STD 13, November 1987.

[RFC 1035] - P. Mockapetris, "Domain Names - Implementation and Specifications", STD 13, November 1987.

[RFC 1750] - D. Eastlake, S. Crocker, and J. Schiller, "Randomness Requirements for Security", December 1994.

[RFC 2065] - Donald Eastlake, Charles Kaufman, "Domain Name System Security Extensions", 01/03/1997.

[RFC 2137] - Donald Eastlake, "Secure Domain Name System Dynamic Update", 04/21/1997.

draft-ietf-dnssec-secext2-*.txt - D. Eastlake, "Domain Name System Security Extensions".

[RSA FAQ] - RSADSI Frequently Asked Questions periodic posting.

Author's Address

Donald E. Eastlake 3rd
CyberCash, Inc.
318 Acton Street
Carlisle, MA 01741 USA

Telephone: +1 978-287-4877
             +1 703-620-4200 (main office, Reston, Virginia, USA)
fax: +1 978-371-7148
email: dee@cybercash.com

Expiration and File Name

This draft expires September 1998.

Its file name is draft-ietf-dnssec-secops-01.txt.