Network Working Group
INTERNET-DRAFT

Martin Hamilton
Jon Knight
Loughborough University
March 1998

Distributing control of the Domain Name System

draft-hamilton-fix-dns-00.txt

Status of This Memo

Abstract

This proposal outlines a way in which the Internet community may be able to route around the legal and political issues associated with control of the Domain Name System. We suggest a new mechanism for the distribution of domain name information, based on strong cryptographic authentication. In this new system, anyone is free to "publish" domain name information, with control over whether or not it is accepted left to the local site DNS server administrators.

1. Problem definition

The Domain Name System is theoretically an extension to the basic Internet infrastructure - simply resolving requests to look up "domain name" tokens and returning Internet Protocol addresses and related information [1,2]. In practice it is treated as essential by the vast majority of Internet users, and control of the DNS is a legal and political Hot Potato.

There appear to be two general problems with control of the DNS :-

* Clashes over who has the right to a particular domain name, e.g. should Apple Computer, Inc. have an inalienable right to the apple.com domain name ?

* Clashes over the hierarchical authority structure which is used to delegate portions of the Internet domain namespace to particular domain name serveres.

This proposal does not address the first point directly, though it may be of some indirect benefit in this area. The second point is at the heart of this proposal.

2. Proposed solution

The Usenet News system incorporates a "control" mechanism, which is used for the creation and deletion of "newsgroups" (conferences). Anyone is free to create or delete a newsgroup, but in practice most Usenet servers will only act on control messages from a very small number of originators - at the discretion of their administrators. Usenet has recently added strong cryptographic authentication for control messages, using PGP [3].

We propose that this model should be adopted for the distribution of Domain Name information.

We anticipate that some minor changes would be necessary to DNS server software (e.g. BIND) to take account of this new model of DNS propagation. No changes would be needed at the resolver level, as moving to this new system would be transparent to end users. Usenet News would be an excellent mechanism for the distribution of DNS related control messages - though not a timely one. For this reason we assume that most use of this system would be for the distribution of new top level domain information, which could be expected to change infrequently.

The exact level of control which is given to a particular identity would, of necessity, vary from site to site. Some sites might choose

to act on control messages from particular people (e.g. Jon Postel or Paul Vixie :-) for arbitrary second and third level domains - at their discretion.

3. Security considerations

Use of strong cryptographic authentication such as PGP is essential for the correct operation of this system. Compromised cryptographic protocols (e.g. using 40 bit keys, or escrowed private keys) would not be appropriate, since these weaknesses are now well known outside the cryptological community - e.g. in the print and broadcast media.

It is essential that stringent measures are taken to protect the private keys which are used to sign the control messages. As a bare minimum these should be stored on computers which are not connected to a network, with messages and signatures being transported via floppy disk. We envisage that a code of conduct would rapidly emerge if this proposal is successful.

The trust model for this system is very simple :-

* Implementations should discard control messages which have not been cryptographically signed.

* Control messages with invalid signatures may be logged, but should not be acted upon - even if they come from a trusted originator.

* Control messages which have a valid signature from a trusted originator but do not fall into their access control list of permitted operations may be logged, but should not be acted upon.

In addition, implementors should take care to avoid the normal security problems - e.g. avoid allocating fixed size buffers, check for buffer overruns. Checking for unusual behaviour would also be advisable, e.g. attempts to change large amounts of domain name information in a short space of time may indicate that the originator's private key has been compromised.

4. References

[1] P.V. Mockapetris. "Domain names - implementation and specification", RFC 1035, 1987.

[2] P.V. Mockapetris. "Domain names - concepts and facilities", RFC 1034, 1987.

[3] David Lawrence et al - pgpcontrol.
<URL:ftp://ftp.isc.org/pub/pgpcontrol>

5. Authors' address

Martin Hamilton, Jon Knight
Department of Computer Studies
Loughborough University of Technology
Leics. LE11 3TU, UK

Email: m.t.hamilton@lut.ac.uk
j.p.knight@lut.ac.uk

This Internet Draft expires September 1998.