

DAILY KOS

DHS demand for DNS master key alarms nations

by **Deep Harm**

Sat Mar 31, 2007 at 04:03:53 PM PDT

Slashdot and **Cryptome** report that the U.S. Department of Homeland Security (DHS) is demanding the master key for the DNS root zone - a demand that has other nations alarmed. With the master key, DHS would have control over the Internet, as Slashdot describes, quoting an "anonymous reader."

The key will play an important role in the new DNSSEC security extension, because it will make spoofing IP-addresses impossible. By forcing the IANA [Internet Assigned Numbers Authority] to hand out a copy of the master key, the US government will be the only institution that is able to spoof IP addresses and be able to break into computers connected to the Internet without much effort.

The issue arose at Friday's meeting of the Internet Corporation for Assigned Names and Numbers (ICANN) in Lisbon, Portugal.

Deep Harm's diary :: ::

There is no indication yet that U.S. mainstream news media have reported on the DHS proposal. U.S. coverage of the ICANN meeting focused (predictably) on a proposal to create a domain specifically for **adult websites**. Cryptome cites a German news source, **Heisse Online**, which provides the following information.

The US Department of Homeland Security (DHS)...wants to have the key to sign the DNS root zone solidly in the hands of the US government. This ultimate master key would then allow authorities to track DNS Security Extensions (DNSSEC) all the way back to the servers that represent the name system's root zone on the Internet. The "key-signing key" signs the zone key, which is held by VeriSign. At the meeting of the Internet Corporation for Assigned Names and Numbers (ICANN) in Lisbon, Bernard Turcotte, president of the Canadian Internet Registration Authority (CIRA) drew everyone's attention to this proposal as a representative of the national top-level domain registries (ccTLDs).

At the ICANN meeting, Turcotte said that the managers of country registries were concerned about this proposal. When contacted by heise online, Turcotte said that the national registries had informed their governmental representatives about the DHS's plans. A representative of the EU Commission said that the matter is being discussed with EU member states. DNSSEC is seen as a necessary measure to keep the growing number of manipulations on the net under control. The DHS is itself sponsoring a campaign to support the implementation of DNSSEC. Three of the 13 operators currently work outside of the US, two of them in Europe. Lars-Johan Liman of the Swedish firm Autonomica, which operates the I root server, pointed out the possible political implications last year. Liman himself nominated ICANN as a possible candidate for the supervisory function.

When other nations are worried, Americans, too, should be concerned. The Bush administration has demonstrated that it is unable to wield power responsibly. Therefore, its demand for Internet control should be viewed as an opportunity to abuse its authority to control a medium that has played a critical role in holding it accountable.

Tags: [DHS](#), [Internet](#), [ICANN](#), [IANA](#), [DNS](#) (all tags)

[Permalink](#) | 32 comments

Comments: Expand Shrink Hide (Always) | Indented Flat (Always)

▼ **NO!!!!!!** (20+ / 0-)

Especially not Dumbya and his henchmen.

by [manwithnname](#) on [Sat Mar 31, 2007 at 04:03:41 PM PDT](#)

▼ **most incompetent and corrupt agency too** (10+ / 0-)

and Lieberman is in charge of oversight.

be very afraid.

by [fugue](#) on [Sat Mar 31, 2007 at 04:17:02 PM PDT](#)

[[Parent](#)]

▼ **and one of the most secretive n/t** (14+ / 0-)

Forewarned, forearmed; to be prepared is half the victory. ~ Cervantes

by [Deep Harm](#) on [Sat Mar 31, 2007 at 04:17:53 PM PDT](#)

[[Parent](#)]

▼ **It could be even worse** (5+ / 0-)

Once one Government has it, all the others will also. Some of those countrys would use it in more brutal ways than even our Government has yet to act. (debatable) This would total any concept of free speech on the Net that is left.

We cannot allow this to happen. Period

-8.63 -7.28 Molly Ivin : ".We want to find solutions other than killing people. Not in our name, not with our money, not with our children's blood."

by [OneCrankyDom](#) on [Sat Mar 31, 2007 at 06:04:45 PM PDT](#)

[[Parent](#)]

▼ **split of the net** (0 / 0)

The net wil pretty much break apart. Everybody will make their own protocol to protect their turf.

by [fugue](#) on [Sat Mar 31, 2007 at 06:43:09 PM PDT](#)

[[Parent](#)]

▼ **Hell they'll be selling it** (1+ / 0-)

on the "Free Market" to corporations and intelligence agencies the world over.

That they're doing so will be classified "top state secret."

Little known Constitutional fact: the phrase "executive privilege," does not exist anywhere in the Constitution! Justice Scalia...?

by [Jim P](#) on [Sat Mar 31, 2007 at 06:50:41 PM PDT](#)
[[Parent](#)]

▼ [ICANN](#) (8+ / 0-)

Why wouldn't ICANN supervise? Wouldn't that make the most sense?

by [susie dow](#) on [Sat Mar 31, 2007 at 04:06:29 PM PDT](#)

▼ [ICANN itself lacks accountability](#) (5+ / 0-)

See [ICANN Watch](#) website.

Forewarned, forearmed; to be prepared is half the victory. ~ Cervantes

by [Deep Harm](#) on [Sat Mar 31, 2007 at 05:23:54 PM PDT](#)

[[Parent](#)]

▼ [AGAIN NO!!!!](#) (8+ / 0-)

"Though the Mills of the Gods grind slowly, Yet they grind exceeding small."

by [Owillwoman](#) on [Sat Mar 31, 2007 at 04:15:01 PM PDT](#)

▼ [What does this mean?](#) (8+ / 0-)

Why would one country have an exclusive in this area of domain names and assignments? Isn't the international agreement of shared authority the reason the net traffic and versatility has grown?

What exactly does the DHS proposal regarding the "key" do to security or anonymity? Why should they get that power? The Fourth Amendment, search and seizure are no longer protected in the USA as are citizens rights so why should the other ICANN members reward a rogue government and a rogue agency?

"Someone has to be the first drop of rain" Taslima Nasrin

by [Pete Rock](#) on [Sat Mar 31, 2007 at 04:16:09 PM PDT](#)

▼ [Importance of secure DNS](#) (5+ / 0-)

See [Hackers Lauch Massive Attack on Internet DNS.](#)"

Forewarned, forearmed; to be prepared is half the victory. ~ Cervantes

by [Deep Harm](#) on [Sat Mar 31, 2007 at 05:01:36 PM PDT](#)

[[Parent](#)]

▼ [See ya later](#) (6+ / 0-)

I have to unplug my modem.

by [willb48](#) on [Sat Mar 31, 2007 at 04:19:29 PM PDT](#)

▼ **I never thought I'd write a GBCW.** (8+ / 0-)

Saying "I'm no techie" is a vast understatement, but from what I've read this sounds like "All of your tubes is belong to us." Is a "for Dummies" article about this anywhere?

"It does not require many words to speak the truth." -- Chief Joseph, native American leader (1840-1904)

by [highfive](#) on [Sat Mar 31, 2007 at 04:22:30 PM PDT](#)

▼ **I think you pretty well captured it** (10+ / 0-)

But, if you'd like to read more, I refer you to these sources: [DNS for Dummies](#), [DNS Root Name Servers Explained for Dummies](#), and just about everything you'd want to know about [DNSsec](#).

Forewarned, forearmed; to be prepared is half the victory. ~ Cervantes

by [Deep Harm](#) on [Sat Mar 31, 2007 at 04:51:36 PM PDT](#)
[[Parent](#)]

▼ **Thanks so much!** (1+ / 0-)

I'd like to know more.

"It does not require many words to speak the truth." -- Chief Joseph, native American leader (1840-1904)

by [highfive](#) on [Sat Mar 31, 2007 at 04:56:11 PM PDT](#)
[[Parent](#)]

▼ **The paper on DNS Cache Poisoning** (2+ / 0-)

is 404... interesting.

"My case is alter'd, I must work for my living." Moll Cut-Purse, The Roaring Girl - 1612, England's First Actress

by [theRoaringGirl](#) on [Sat Mar 31, 2007 at 05:16:36 PM PDT](#)
[[Parent](#)]

▼ **so does this mean** (0 / 0)

that agreement the UN agreed to last year to keep the DNS root name servers under US (ICANN) control is about to be kaput?

Quick! Man the Blogs!

by [HiBob](#) on [Sat Mar 31, 2007 at 06:07:04 PM PDT](#)
[[Parent](#)]

▼ **A slim, but silver lining** (8+ / 0-)

Not to be twisted, but hey, at least the bushies have pissed off enough of the rest of the world that these folks are going to tell DHS to pound salt.

Spare me - we may not have been able to stop this cabal from breaking our laws and discarding our right to privacy, but they'll be laughed back to the bat cave by the international community on this one.

rec'd

How many legs does a dog have if you call the tail a leg? Four; calling a tail a leg doesn't

make it a leg. (Abraham Lincoln)

by [Ninepatch](#) on [Sat Mar 31, 2007 at 04:32:47 PM PDT](#)

▼ **I so hope you are right.** (5+ / 0-)

"Though the Mills of the Gods grind slowly, Yet they grind exceeding small."

by [Owillwoman](#) on [Sat Mar 31, 2007 at 04:34:10 PM PDT](#)

[[Parent](#)]

▼ **and everyone in the US** (3+ / 0-)

will run their traffic through a proxy in Sweden. Excellent job, DHS.

Quick! Man the Blogs!

by [HiBob](#) on [Sat Mar 31, 2007 at 06:10:09 PM PDT](#)

[[Parent](#)]

▼ **Suggestions for top-level domain names** (11+ / 0-)

.CUM - Porn web sites

.CON - Religious web sites

.DUM - Bush family web sites

"When a true genius appears in this world, you may know him by this sign, that the dunces are all in confederacy against him." -- Jonathan Swift

by [Pope Bandar bin Turtle](#) on [Sat Mar 31, 2007 at 04:40:20 PM PDT](#)

▼ **Or see DHS proposal** (4+ / 0-)

...consolidate into one top-level domain, .gov.

[snark]

Forewarned, forearmed; to be prepared is half the victory. ~ Cervantes

by [Deep Harm](#) on [Sat Mar 31, 2007 at 05:09:30 PM PDT](#)

[[Parent](#)]

▼ **Or ...** (0 / 0)

.DIM?

"When a true genius appears in this world, you may know him by this sign, that the dunces are all in confederacy against him." -- Jonathan Swift

by [Pope Bandar bin Turtle](#) on [Sat Mar 31, 2007 at 10:17:32 PM PDT](#)

[[Parent](#)]

▼ **God, this is worse than when Clinton** (5+ / 0-)

wanted to mandate crypto chips that only the Gov't could have a master code to. Gotta beat this proposal back too!

by [kursk](#) on [Sat Mar 31, 2007 at 05:05:13 PM PDT](#)

▼ **Hmmm...** (0 / 0)

Wow. What an icky idea.

"Computer. End holographic program...Computer? Computer?"

by **kredwyn** on **Sat Mar 31, 2007 at 06:08:15 PM PDT**

▼ **It's all about fascism** (7+ / 0-)

Corporate control of everything that moves and doesn't move. That's the Bush agenda. Bastards.

by **EyeBall Kid** on **Sat Mar 31, 2007 at 06:48:28 PM PDT**

▼ **Very good catch, recommended** (6+ / 0-)

Raw Story's linked to this so hopefully it'll get the attention it deserves.

by **greatwhitebuffalo** on **Sat Mar 31, 2007 at 07:26:08 PM PDT**

▼ **Thank you for mentioning. n/t** (3+ / 0-)

Forewarned, forearmed; to be prepared is half the victory. ~ Cervantes

by **Deep Harm** on **Sat Mar 31, 2007 at 08:08:35 PM PDT**

[**Parent**]

▼ **Yep** (2+ / 0-)

I came here via their link.

This might be a first. I can't ever remember them linking directly to a diary before from the top stories area.

Perhaps it is a universal truth that the loss of liberty at home is to be charged to provisions against danger, real or pretended from abroad. ~J. Madison

by **wolverine 06** on **Sat Mar 31, 2007 at 09:50:08 PM PDT**

[**Parent**]

▼ **Me too.** (1+ / 0-)

I was surprised when it took me here. This sounds awful! It's quite confusing to me though. I hope somebody explains it in less technical terms. And I hope the MSM get wind of it. KEITH!! HELP!!

by **joodleboodle** on **Sun Apr 01, 2007 at 06:13:36 AM PDT**

[**Parent**]

▼ **great stuff** (0 / 0)

I love it when DKos talks high-tech.

Kelly w/a Y

by **the1bostongirl** on **Sun Apr 01, 2007 at 01:21:08 AM PDT**

▼ **WSIS** (2+ / 0-)

this partly explains why the u.s. was so adamant on keeping icann in u.s. hands at the world summit on the information society (wsis) back in tunis in november 2005...

visit my blog: [And, yes, I DO take it personally](#)

by [profmarcus](#) on [Sun Apr 01, 2007 at 06:18:33 AM PDT](#)

[Permalink](#) | [32 comments](#)



[Daily Kos homepage](#)

© Kos Media, LLC

Site content may be used for any purpose without explicit permission unless otherwise specified.

[Privacy Policy](#)

Powered by [Scoop](#).

[CDs](#)
[★ Reac](#)
[Advertise](#)
Classif
[Advertise](#)

I Supp
Bloggers'
[Support Blogge](#)

[Candidates](#)
[Blue Majority C](#)