

Re: [fw-wiz] DNS and Firewalls

Source: <http://www.derkeiler.com/Mailing-Lists/Firewall-Wizards/2003-02/0046.html>

From: Rob Payne (rns Payne@the-paynes.com)

Date: 02/20/03

From: Rob Payne <rns Payne@the-paynes.com>

To: tqbf@pobox.com

Date: Wed, 19 Feb 2003 23:15:25 -0500

On Sat, Feb 15, 2003 at 02:20:30PM -0800, tqbf@sockpuppet.org wrote:

> [arbitrary message clip for context]

>> Thomas, that comment is ridiculously specious. I asked if Tobias was
>> using nym-based security and then discussed why it is not practical.

> Rob, calling my comments ``specious'' doesn't make them
> specious. Neither does concocting straw-man arguments. Not only am
> I not stepping into this discussion to defend ``nym-based
> security'', but you're intentionally oversimplifying Bernstein's
> suggestion to make a fantasy argument even easier to win.

That is not what I was doing. I took Prof. Dan's proposal at his word, but I will get to that.

> Let me assume that you're responding to my message in good faith,
> and suggest that we're not going to come to a constructive
> resolution by ignoring each other's arguments.

That's true enough.

> I want to point out that ``DNSSEC requirements'' are not a credible
> reason to create hassles for firewall implementors. I think I have a
> good point in my favor: until [useful]*.COM is signed, EDNS0 and
> DNSSEC don't solve any real-world problems.

I don't care about [useful]*.com until the root zone is signed to have a verifiable chain of trust through com to [useful]*.com. EDNS0 solves real-world problems, as others have pointed out, and not handling it well (throwing away large fragmented packets between servers that have negotiated the large packet size through a clear channel) will break the ability of those servers to communicate.

Since this was a security-relevant list, I used two security-based (nym and dnssec) scenarios. They are not the only scenarios where EDNS is important. Why should heavily loaded servers have to switch

Firewall-Wizards: Re: [fw-wiz] DNS and Firewalls

to TCP to answer regular queries that can be answered without TCP. If reliability and service availability is not useful enough for vendors to at least look at this issue, then I am not going to change anyone's mind with anything that I have to say. I was under the impression that these were a few of the reasons for the firewalls.

> *You can say this is a chicken-and-egg problem because middleboxes are keeping DNSSEC from being deployed.*

I didn't say that, I said that it was going to become an issue. I thought it might be wise to get the firewalls fixed while the DNS changes are being hammered out.

> *Unfortunately, you'll have to contend with Vixie:
> ``it's impossible to know how many flag days we'll have before it's
> safe to burn ROMs... 2353 is already dead''.*

I have read the quote. Just because I've read it does not make me believe that it is true. As I said, previously, there are signed zones in use now. (I discussed these in previous messages.)

> *I think ``working code'' should come before attempts to build
> ``rough consensus''.*

I am not sure I understand that comment, or the inspiration for it. In some ways that would seem like starting construction without knowing if you were building a ship or a building.

> *You want to point out that DNSSEC is a more credible solution than
> ``nyms''. Fine: make a good-faith effort to take the idea of ``names
> are linked to keys directly'' to its logical conclusion. Saying ``we
> should all go back to a hosts file and copying it from machine to
> machine'' is obviously not a good-faith effort:*

My apologies, that comment came from the same email discussion with DJB.

> *it assumes a ``nym-based system'' is simply the idea that names
> embed links to their keys. No competent engineer would consider that
> a real proposal. I don't suggest you are incompetent.*

> *I haven't taken much time to think about ``nym-based security'' (my
> problem with DNSSEC ends at its presumptuousness and lack of real-world
> deployment, long before we get to alternative suggestions). But, let me
> tell you what I start thinking about when I think about when confronted
> with this problem: names change when keys need to change, and we make it
> easier to propagate name changes. We rely on systems whose keys don't
> change often to act as signposts to link to systems who do. Have you
> thought about any of this?*

Firewall-Wizards: Re: [fw-wiz] DNS and Firewalls

The scenario you describe is very similar to the one we have today. Root server ip addresses are included in the code for some DNS servers. But, unlike the addresses of root servers, that will only change when it is necessary for them to move to different owners or geographic locations, the security of a public key is a bit more tenuous. If one of the signposts is hacked down, herds of peasants can longer find their way to market.

In the first situation, the largest ISPs are working to keep things up and running. In the latter, a script kiddie takes down a system a bit more often than that. There are enterprises with tighter security, but many of those sign posts are local and easier to knock over. How does a lowly peasant (computer) know who to trust?

> *Of course, one of the reasons I haven't either is that we're talking about DNS names that look like ``rkjhf934f.sockpuppet.org". Don't you think that the author of the second-most popular open-source DNS server on the Internet understands this as well? Our normal assumptions about the role of DNS go out the window in this environment. Clearly everyone understands this.*

I don't know what he has thought of and what he hasn't. There are a lot of solutions to problems that are overlooked by engineering teams with only one member.

> *So what point are you trying to make, again? That people shouldn't mention Bernstein in discussions about DNS security?*

Why did you think this was about Bernstein at all? (Why did you change the subject of your message to make it about him?) No offense to any DNS implementor, but every one of them can be replaced. Would you have as much faith in djbdns if the person maintaining it was changed tomorrow? Software projects with a single author tend to have very serious problems when that author changes. Sometimes the project gets stronger, sometimes it does not but it is often a very bumpy ride.

-rob

firewall-wizards mailing list
firewall-wizards@honor.icsalabs.com
<http://honor.icsalabs.com/mailman/listinfo/firewall-wizards>

- application/pgp-signature attachment: [stored](#)